Causes of the Failure of the Zionist Regime's Intelligent Military Systems in Operation Al-Aqsa Storm (The Dangers of Over-Reliance on Artificial Intelligence in Contemporary Warfare)

Javad Baharmast Hossein Abadi[١]

١.Ph.D. in International Relations, Faculty of Political Science and International Relations, Islamic Azad University, South Tehran Branch, Tehran, Iran

Abstract

This research analyzes the causes behind the failure of the Zionist regime's intelligent military systems in confronting Operation Al-Aqsa Storm and examines the dangers of over-reliance on artificial intelligence in asymmetric warfare. The main research problem is the failure of this regime's advanced reconnaissance and defense systems to predict and counter Hamas's surprise attack, despite the Zionist regime's massive investment in military artificial intelligence technologies. The aim of the research is to explain the factors behind this failure and extract strategic lessons for resistance forces in facing armies reliant on advanced technologies. The research method is qualitative and a case study, utilizing internet sources. The findings indicate that five key factors played a role in this failure: ١. Over-reliance on AI and neglect of human analysis, ٢. Excessive trust in electronic security barriers, ٣. Inattention to warning signs and field intelligence, ٤. Inability to predict Hamas's asymmetric tactics, and ٥. Structural problems in coordination among security institutions. The results of the research suggest that asymmetric warfare, by utilizing strategic surprise and low-cost methods, can neutralize the enemy's technological superiority. Furthermore, integrating AI with human analysis and developing hybrid (cyber-field) strategies are among the key lessons of this event for contemporary warfare.

Keywords: Military Artificial Intelligence, Operation Al-Aqsa Storm, Asymmetric Warfare, Strategic Surprise

نشریه علمی مطالعات دفاع مقدس و نبردهای معاصر

علل شکست سامانه‌های هوشمند نظامی رژیم صهیونیستی در عملیات طوفان الاقصی (خطرات اتکای مطلق به هوش مصنوعی در نبردهای معاصر)

جواد بهارمست حسین‌آبادی[1]

۱۲
سال هفتم
بهار و تابستان ۱۴۰۴
مقاله پژوهشی
تاریخ دریافت:
۱۴۰۴/۰۱/۱۳
تاریخ پذیرش:
۱۴۰۴/۰۷/۱۴
صص: ۳۲۹-۳۰۵
شاپا چاپی: ۶۳۲۸-۲۵۳۸
الکترونیکی: ۱۶۵۵-۲۷۱۷

چکیده

این پژوهش به تحلیل علل شکست سامانه‌های هوشمند نظامی رژیم صهیونیستی در مقابله با عملیات طوفان الاقصی می‌پردازد و خطرات اتکای مطلق به هوش مصنوعی در نبردهای نامتقارن را بررسی می‌کند. مسئله اصلی تحقیق، ناکامی سامانه‌های پیشرفتهٔ شناسایی و دفاعی این رژیم در پیش‌بینی و مقابله با حمله غافلگیرانهٔ حماس است، علی‌رغم سرمایه‌گذاری کلان رژیم صهیونیستی بر فناوری‌های هوش مصنوعی نظامی. هدف پژوهش، تبیین عوامل این شکست و استخراج درس‌های راهبردی برای نیروهای مقاومت در مواجهه با ارتش‌های متکی بر فناوری‌های پیشرفته است. روش تحقیق، کیفی و مطالعه موردی با استفاده از منابع اینترنتی است. یافته‌ها نشان می‌دهد پنج عامل کلیدی در این شکست نقش داشته‌اند. ۱. اتکای مطلق به هوش مصنوعی و غفلت از تحلیل‌های انسانی ۲. اعتماد بیش‌ازحد به دیواره‌های امنیتی الکترونیکی ۳. عدم توجه به نشانه‌های هشداردهنده و اطلاعات میدانی ۴. ناتوانی در پیش‌بینی تاکتیک‌های نامتقارن حماس ۵. مشکلات ساختاری در هماهنگی بین نهادهای امنیتی. نتایج پژوهش حاکی از آن است که جنگ نامتقارن با بهره‌گیری از غافلگیری راهبردی و روش‌های کم‌هزینه می‌تواند برتری فنّاورانه دشمن را خنثی کند. همچنین، تلفیق هوش مصنوعی با تحلیل انسانی و توسعه راهبردهای ترکیبی (سایبری – میدانی) ازجمله درس‌های کلیدی این واقعه برای نبردهای معاصر است.

کلیدواژه‌ها: هوش مصنوعی نظامی؛ عملیات طوفان الاقصی؛ جنگ نامتقارن؛ غافلگیری راهبردی.

DOR: ۲۰،۱۰۰۱،۱،۲۵۳۸۶۳۲۸،۱۴۰۴،۷،۱۲،۱۱،۵

۱. نویسنده مسئول: دکتری روابط بین الملل ،دانشکده علوم سیاسی و روابط بین الملل،دانشگاه آزاد اسلامی واحد تهران جنوب تهران،تهران، ایران

Email: javadbaharmasthooseinabadi@gmail.com

مقدمه و بیان مسئله

هوش مصنوعی با کمک داده‌ها، قدرت پردازش رایانه‌ای و پیشرفت‌های یادگیری ماشینی به‌ویژه در دو دهه اخیر به‌تدریج در حال بهبود و تبدیل‌شدن به روشی کارآمدتر در سراسر جهان شده است (شاکری،۱۴۰۲: ۲۰۳). این فناوری با جمع‌آوری اطلاعات است که می‌تواند هوش را شبیه‌سازی کند و به‌طور خودکار وظایف ادراک، فهم، استنتاج و تصمیم‌گیری را انجام دهد. این فن‌ها به‌طور خاص از علوم کامپیوتر، الکترونیک، ریاضیات (به‌ویژه آمار)، علوم اعصاب و علوم شناختی استفاده می‌کند (جهان‌دیده و میرفخرایی،۱۴۰۳: ۲۹۵).

در عصر حاضر، تحولات فناورانه به‌ویژه در حوزه هوش مصنوعی و سامانه‌های خودکار، چهره جنگ‌های معاصر را دگرگون ساخته است. ارتش‌های مدرن با سرمایه‌گذاری‌های کلان بر سامانه‌های هوشمند شناسایی، نظارتی و دفاعی، تلاش می‌کنند تا برتری راهبردی خود را در میدان‌های نبرد حفظ نمایند. در این میان، رژیم صهیونیستی به‌عنوان یکی از پیشرفته‌ترین نظام‌های دفاعی مجهز به فناوری‌های روز دنیا شناخته می‌شود که بودجه‌های هنگفتی را به توسعه و به‌کارگیری سامانه‌هایی مانند «سپر آهنین»، «دیوار هوشمند مرزی» و شبکه‌های پیچیده نظارتی مبتنی بر هوش مصنوعی اختصاص داده است. بااین‌وجود، عملیات غافلگیرکننده «طوفان الاقصی» در ۷ اکتبر ۲۰۲۳ توسط حماس، نقاط ضعف بنیادین این رویکرد فناوری‌محور را به شکل بی‌سابقه‌ای آشکار ساخت. این عملیات که با موفقیت چشمگیری همراه بود، نشان داد که چگونه یک نیروی مقاومت با امکانات محدود اما با به‌کارگیری تاکتیک‌های هوشمندانه و نامتقارن، می‌تواند پیشرفته‌ترین سامانه‌های دفاعی جهان را به چالش بکشد.

این پژوهش باهدف اصلی «تبیین علل شکست سامانه‌های هوشمند نظامی اسرائیل در عملیات طوفان الاقصی» و با تحلیل نقاط ضعف ذاتی هوش مصنوعی در محیط‌های عملیاتی پیچیده به‌منظور بررسی راهکارهای مقاومت فلسطین در فریب سامانه‌های هوشمند برای استخراج درس‌های راهبردی و ارائه الگوهای عملیاتی برای مقابله با سامانه‌های هوشمند دفاعی برای نیروهای مقاومت در مواجهه با ارتش‌های متکی بر فناوری تدوین‌شده است. انجام این پژوهش از چند جهت حائز اهمیت است:

الف) ضرورت نظری: پر کردن خلأ مطالعاتی در زمینه کاربرد هوش مصنوعی در نبردهای نامتقارن و توسعه چارچوب‌های نظری در زمینه محدودیت‌های فناوری‌های هوشمند نظامی.

ب) ضرورت عملی: ارائه راهکارهای عملیاتی به نیروهای مقاومت، هشدار درباره خطرات اتکای مطلق به فناوری‌های هوشمند و کمک به برنامه‌ریزی‌های دفاعی در برابر ارتش‌های پیشرفته

با این توضیحات انجام این پژوهش بنا بر دلایل ماهیت بی‌سابقه عملیات طوفان الاقصی در غافلگیری یک نظام امنیتی پیشرفته؛ نیاز به درک عمیق‌تر از تعامل میان فناوری‌های پیشرفته و تاکتیک‌های نامتقارن؛ اهمیت استخراج درس‌های راهبردی برای نیروهای مقاومت و لزوم بازنگری در الگوهای دفاعی در عصر هوش مصنوعی ضروری است.

سؤال اصلی تحقیق این است که؛ علل اصلی شکست سامانه‌های هوشمند نظامی اسرائیل در مقابله با عملیات طوفان الاقصی چه بوده و چه درس‌هایی می‌توان از این واقعه برای نبردهای معاصر گرفت؟ براین‌اساس فرضیه اصلی نیز این است که به نظر می‌رسد اتکای مطلق به هوش مصنوعی و غفلت از عوامل انسانی و محیطی، همراه با به‌کارگیری تاکتیک‌های خلاقانه نامتقارن توسط مقاومت فلسطین، مهم‌ترین عوامل شکست سامانه‌های هوشمند اسرائیل در این عملیات بوده است.

پیشینهٔ پژوهش

سوابق تحقیق با بررسی مقالات، گزارش‌ها و آثار پیشین که ازنظر محتوا نزدیک به موضوع این نوشتار هستند و نگارش یافته‌اند، مشخص گردید که تاکنون تحقیقات جامع و مدونی در رابطه با علل غافلگیری رژیم صهیونیستی به دلیل بهره‌برداری از سامانه‌های هوش مصنوعی نظامی در عملیات طوفان الاقصی صورت نگرفته است. بااین‌وجود نوشتارهای زیر به موضوع این نگارش نزدیک هستند.

دوز و کوکاکوبلو (۲۰۲۵) در گزارش با نام «نقش مخرب هوش مصنوعی در جنگ غزه» به بررسی کاربردهای نظامی هوش مصنوعی توسط رژیم صهیونیستی در جنگ غزه می‌پردازد. این مطالعه نشان می‌دهد که چگونه فناوری‌های پیشرفته، مانند سامانه‌های شناسایی خودکار، پهپادهای هوشمند و الگوریتم‌های تصمیم‌گیری، به افزایش دقت حملات و درعین‌حال تلفات غیرنظامی بیشتر منجر شده‌اند. نویسندگان به نگرانی‌های اخلاقی اشاره می‌کنند، ازجمله کاهش مسئولیت‌پذیری

انسانی در استفاده از سلاح‌های خودکار و خطرات ناشی از خطاهای الگوریتمی. همچنین، گزارش بر تأثیرات روانی و اجتماعی این فناوری‌ها بر مردم غزه، ازجمله ایجاد ترس و نظارت گسترده، تأکید دارد. درنهایت، پژوهشگران خواستار مقررات بین‌المللی برای محدود کردن استفاده نظامی از هوش مصنوعی و جلوگیری از نقض حقوق بشر در جنگ‌ها هستند.

علی‌شاهی (۲۰۲۴) در مقاله‌ای با عنوان «عملیات طوفان الاقصی و کاربست الگوی جدید مقاومت در جهان اسلام» با روش فراترکیبی نشان می‌دهد که حماس با گذار از دفاع به تهاجم، معادلات امنیتی رژیم صهیونیستی را دگرگون کرد. نویسنده این مقاله معتقد است که این عملیات به‌عنوان الگوی جدید مقاومت در جهان اسلام مطرح شد و با تأکید بر تضعیف پروژه عادی‌سازی روابط با رژیم صهیونیستی و نیز بحران‌های داخلی رژیم صهیونیستی (مهاجرت معکوس، شکاف‌های راهبردی) نشان‌دهنده موفقیت این عملیات است. از منظر این نویسنده مؤلفه‌های موفقیت این عملیات شامل عمل تاکتیکی محدود و بهره‌گیری از ضعف‌های ژئوپلیتیک دشمن بود. نویسنده پیشنهاد می‌کند این مدل می‌تواند برای سایر جنبش‌های مقاومت در جهان اسلام کاربردپذیر باشد . درنهایت در جمع‌بندی به این مهم توجه می‌نماید که عملیات طوفان الاقصی نه‌تنها یک پیروزی نظامی، بلکه تحول در راهبرد مقاومت بود که با ترکیب عوامل داخلی و خارجی، الگویی عملی برای مقابله با رژیم صهیونیستی ارائه داد.

ویس (۲۰۲۴) در یک پژوهش علمی با عنوان «حمله ۷ اکتبر: ارزیابی شکست اطلاعاتی» به بررسی دلایل ناکامی سرویس‌های امنیتی رژیم صهیونیستی در پیش‌بینی و جلوگیری از حمله غافلگیرانه حماس در ۷ اکتبر ۲۰۲۳ می‌پردازد. این پژوهش نشان می‌دهد که اشتباهات تحلیلی، غفلت از علائم هشداردهنده و تمرکز بیش‌ازحد بر تهدیدات دیگر مانند جبهه شمالی، از عوامل اصلی این شکست بودند. همچنین، مقاله به نقش فنّاوری و نقص در هماهنگی بین نهادهای امنیتی اشاره می‌کند. درنهایت، نویسنده پیشنهادهایی برای اصلاح ساختار اطلاعاتی و بهبود همکاری بین سازمانی ارائه می‌دهد تا از تکرار چنین خطاهایی جلوگیری شود.

محمدی منفرد (۱۴۰۲) در مقاله‌ای بانام «بررسی نتایج عملیات طوفان الاقصی بر اساس دکترین نظامی رژیم صهیونیستی»، به تحلیل پیامدهای عملیات مشترک گروه‌های مقاومت فلسطین علیه رژیم صهیونیستی بر اساس اصول راهبردی نظامی این رژیم می‌پردازد .نویسنده با بررسی دکترین امنیتی

اسرائیل که بر بازدارندگی، ضربه زدن سریع و جنگ در خاک دشمن استوار است، نشان می‌دهد که عملیات طوفان الاقصی چگونه این اصول را با چالش مواجه کرد. این عملیات نه‌تنها ضعف سامانه‌های امنیتی و اطلاعاتی اسرائیل را آشکار ساخت، بلکه توانمندی‌های جدید مقاومت را در عبور از خطوط دفاعی دشمن به نمایش گذاشت. نویسنده تأکید می‌کند که نتایج این عملیات، شکست استراتژی بازدارندگی اسرائیل و افزایش هزینه‌های امنیتی آن را در پی داشت. همچنین، این رویداد باعث تقویت روحیه مقاومت در فلسطین و تغییر معادلات منطقه‌ای شد.

بردبار و عالی شاهی (۱۴۰۲) در پژوهشی با عنوان «تحلیل جهش پارادایم جنبش حماس در عملیات ۱۷اکتبر ۲۰۲۰ (تغییر رویکرد پدافندی به آفندی)» بررسی می‌کند که چگونه حماس با تغییر استراتژی از رویکرد پدافندی (دفاعی) به آفندی (تهاجمی)، یک تحول راهبردی ایجاد کرد؛ و با گذار از مقاومت منفعلانه به عملیات تهاجمی دیگر فقط به مقابله با حملات اسرائیل بسنده نکرد، بلکه با طراحی عملیات غافلگیرانه (طوفان الاقصی) ابتکار عمل را به دست گرفت. این عملیات نشان داد که اسرائیل در برابر تاکتیک‌های نوین مقاومت آسیب‌پذیر است. حماس با این اقدام، خود را به‌عنوان یک بازیگر کلیدی در معادلات خاورمیانه تثبیت کرد. از دیگر ثمرات این حمله ضمن تقویت روحیه مقاومت، توجه جهانی را به مسئله فلسطین جلب نمود. از طرف دیگر این تغییر پارادایم، اسرائیل را مجبور به بازنگری در دکترین امنیتی خود کرد، اما واکنش شدید آن نیز تهدیدی برای ثبات منطقه است. به‌طور خلاصه، حماس با این عملیات ثابت کرد که می‌تواند از حالت یک گروه مقاومت محلی به یک نیروی راهبردی تأثیرگذار تبدیل شود.

این پژوهش از چند جهت کلیدی با تحقیقات پیشین متفاوت است و نوآوری‌های جدیدی ارائه می‌دهد که شامل ۱- تحلیل فناورانه - راهبردی با بررسی بی‌سابقه نقاط ضعف هوش مصنوعی نظامی (وابستگی به داده‌های تاریخی، عدم انعطاف الگوریتمی)، همراه با ارائه چارچوب «آسیب‌پذیری هوش مصنوعی در جنگ ترکیبی» و تحلیل موردی نقض دیوار هوشمند با گلایدرهای بی‌صدا.۲- تبیین شناختی غافلگیری در زمان بهره‌مندی از سامانه‌های هوشمند نظامی با معرفی مفهوم «خطای ماشین محور» به معنی اعتماد کورکورانه به هوش مصنوعی توسط تحلیل سوگیری‌های سازمانی در تشدید شکست.۳- ارائه راهکارهای عملیاتی با الگوی سه‌بعدی مقابله علیه سامانه‌های هوشمند نظامی با استفاده از فریب سخت‌افزاری، حملات سایبری و جنگ روانی و در صورت برقراری

شرایط مناسب، استفاده از روش‌های کم‌هزینه مانند پهپادهای انبوه و جنگ الکترونیک.۴- تحلیل موارد ذکرشده به‌منظور استخراج درس‌های کلیدی برای ارائه الگویی جنگ آینده در عصر هوش مصنوعی نبردهای آینده جبهه مقاومت است. با این توضیحات این مقاله اولین مطالعه‌ای است که با نگاهی بین‌رشته‌ای (فناوری، راهبرد و روان‌شناسی شناختی) به تحلیل شکست سامانه‌های هوشمند اسرائیل پرداخته و الگویی برای جنگ آینده در عصر هوش مصنوعی ارائه می‌دهد.

مبانی نظری و ادبیات تحقیق

تعریف مفاهیم و اصطلاحات

سامانه‌های هوشمند نظامی

به مجموعه‌ای از فناوری‌های پیشرفته مانند هوش مصنوعی، رباتیک، یادگیری ماشین و اینترنت اشیا اشاره دارند که برای بهبود عملیات دفاعی و امنیتی طراحی شده‌اند. این سامانه‌ها تحولی عظیم و انقلابی در راهبردهای نظامی و جنگ‌افزارها ایجاد کرده‌اند، این سامانه‌های هوشمند نظامی با استفاده از هوش مصنوعی، داده‌کاوی، حسگرهای پیشرفته و الگوریتم‌های خودکار، قادر به انجام عملیات نظامی با حداقل دخالت انسانی هستند. این فناوری‌ها شامل پهپادها، ربات‌های جنگی، سامانه‌های دفاع موشکی هوشمند و جنگ الکترونیک می‌شوند. به این دلیل هوش مصنوعی به‌عنوان یکی از اجزای سازنده انقلاب صنعتی چهارم در نظر گرفته می‌شود (Anneken et al.۲۰۲۵:۱). سطوح هوشمندی در سامانه‌های نظامی به این سه سطح تقسیم می‌شود:۱- نیمه‌خودکار: نیازمند تأیید انسانی برای اجرای عملیات (سیستم پدافند هوایی پاتریوت)۲- خودکار محدود: توانایی انجام وظایف از پیش برنامه‌ریزی‌شده بدون دخالت انسان (ربات‌های خنثی‌کننده مواد منفجره)۳- خودکار پیشرفته: قابلیت یادگیری و تطبیق با شرایط متغیر میدان نبرد (پهپادهای تهاجمی باقابلیت شناسایی چهره(Sánchez,۲۰۲۵:۳۶-۳۷). سامانه‌های هوش مصنوعی نظامی دارای مزایای به این قرار است:

۱- افزایش دقت و کارایی: استفاده از الگوریتم‌های پیشرفته باعث کاهش خطاهای انسانی در هدف‌گیری می‌شود، به طور مثال شناسایی، حملات دقیق، کاهش خطر برای خلبانان و نیز پهپادهای شناسایی می‌توانند با دقت بالا اهداف را ردیابی کنند.

۲- کاهش تلفات انسانی: جایگزینی ربات‌ها و سامانه‌های خودکار به‌جای سربازان در میدان نبرد، جان سربازان را حفظ می‌کند؛ مانند بهره‌مندی از ربات‌های امدادگر در مناطق خطرناک (خنثی‌سازی بمب و مین، زلزله، آتش‌سوزی و...) استفاده می‌شوند.

۳- سرعت عمل بالا در تصمیم‌گیری: پردازش داده‌های بزرگ در کسری از ثانیه و ارائه تصمیم‌های بهینه (مثلاً در سامانه‌های دفاع موشکی و شلیک سلاح‌های خودکار مستقر در مناطق مرزی و مراکز حساس سیاسی و نظامی).

۴- صرفه‌جویی در هزینه‌ها: کاهش نیاز به نیروی انسانی و آموزش طولانی‌مدت سربازان. به طور مثال: استفاده از خودروهای خودران نظامی هزینه‌های لجستیکی را کاهش می‌دهد.

۵- توانایی عملیات در شرایط سخت: ربات‌ها می‌توانند در محیط‌های شیمیایی، پرتوزا یا زیر آب عمل کنند که برای انسان خطرناک است (Takagi,۲۰۲۵:۷۳-۷۵).

معایب سامانه‌های هوشمند نظامی به این قرار است:

۱- وابستگی به فناوری و خطر خرابی: خرابی نرم‌افزار یا سخت‌افزار ممکن است منجر به فاجعه نظامی شود. به طور مثال: اختلال در عملکرد لیزرهای جنگی در شرایط جوی نامساعد، محدودیت باتری ربات‌ها در میدان نبرد و نقص فنی در یک سامانه دفاعی با فرصتی که به دشمن می‌دهد، می‌تواند باعث حمله دشمن شود.

۲- تهدیدات سایبری و هک‌کردن: سامانه‌های هوشمند در معرض حمله سایبری قرار دارند و ممکن است توسط دشمن واپایش شوند. اگر دشمن در نفوذ و رمزگشایی سامانه رایانه-ای دارای توانمندی بسیاری باشند، به طور مثال می‌توانند با هک‌کردن پهپادها علیه نیروهای خودی استفاده نمایند.

۳- کاهش کنترل انسانی و خطر تصمیم‌گیری خودکار: سامانه‌های کاملاً خودکار ممکن است بدون نظارت انسان تصمیمات خطرناک بگیرند. به طور مثال: سلاح‌های خودکار ممکن است غیرنظامیان را هدف قرار دهند(Anneken et al.۲۰۲۵:۵-۲۷).

۴- مسائل اخلاقی و حقوق بشری: استفاده از ربات‌های کشنده موضوعات اخلاقی درباره مرزهای ماشین و انسان را مطرح می‌کند و نگرانی از کشتار غیرنظامیان توسط ربات‌ها را افزایش می‌دهند (Shinwari, Akhtar& Niazi.۲۰۲۵:۲۸۲-۲۸۶).

۵- افزایش احتمال جنگ‌های نامتقارن: کشورهای کوچک یا گروه‌های تروریستی ممکن است از فناوری‌های ارزان‌قیمت (پهپاد و کوادکوپترهای تجاری و...) برای مقابله با قدرت‌های بزرگ استفاده کنند (Sarkin & Sotoudehfar,۲۰۲۴:۱۰۹). به طور مثال در عملیات پهپادی یمن علیه تأسیسات نفتی آرامکو در ۱۴ سپتامبر ۲۰۱۹، انصارالله یمن با استفاده از ترکیب پهپادهای خودساخته قاصف-۲ کی و موشک‌های کروز، یک حمله غافلگیرانه به تأسیسات نفتی بقیق و خریص شرکت آرامکو در عربستان سعودی انجام داد. در این عملیات پهپادهای انصارالله با پرواز در ارتفاع پایین (زیر ۱۰۰ متر) و استفاده از مسیرهای غیرمستقیم، از کور راداری عبور کردند. نکته قابل‌توجه این است که سامانه‌های دفاع هوایی پاتریوت و رادارهای پیشرفته عربستان، طراحی‌شده بودند تا موشک‌های بالستیک و هواپیماهای نظامی را ردیابی کنند، ولی باتوجه‌به هزینه پهپادهای یمنی بالغ‌بر ۲۰۰۰۰ دلار در مقابل موشک‌های دفاعی ۳ میلیون‌دلاری پاتریوت موفق عمل نمودند. از طرف دیگر انصارالله از تاکتیک حمله به‌صورت گله‌ای و با استفاده ۱۰ پهپاد که هرکدام ۳ موشک کروز به‌صورت هم‌زمان شلیک می‌کردند، در این عملیات استفاده نمود. این فن منجر به این شد که سامانه‌های هوشمند عربستان قادر به پردازش این حجم از تهدیدات در لحظه نبودند. از دیگر اقدام یمن بهره‌مندی از سیگنال‌های جعلی راداری و مختل‌کننده‌های دست‌ساز (با هزینه کمتر از ۱۰۰۰۰ دلار) بود تا سامانه‌های اقدام متقابل الکترونیکی و جنگ الکترونیک عربستان را گمراه کند. این اقدام یمن همراه با دیگر اقدامات منجر به این شد که سامانه‌های هوشمند عربستان، برخی پهپادها را به‌عنوان پرندگان یا سروصدا محیطی طبقه‌بندی نمایند.

جنگ نامتقارن

اصطلاحی است که در اواخر دهه ۱۹۹۰ در قلمرو اسناد دولتی و نوشته‌های دانشگاهی ایالات‌متحده مطرح شده است و به درگیری‌هایی اطلاق می‌شود که در آن طرفین از اختلاف چشمگیر در قدرت نظامی، استراتژی‌ها یا منابع برخوردارند(Buffaloe,۲۰۰۶:۲-۱۲) . در جنگ متقارن درگیری بین نیروهای هم‌تراز صورت‌مسئله (جنگ ایران و عراق) و در جنگ هیبریدی ترکیبی از روش‌های متقارن و نامتقارن در نبردها استفاده می‌شود (جنگ روسیه و اوکراین) ولی در

این نوع جنگ، طرف ضعیف‌تر با استفاده از روش‌های غیرمتعارف سعی در خنثی کردن برتری طرف قوی‌تر دارد. این‌گونه از جنگ‌ها دارای ویژگی‌های متمایزکننده نسبت به طرفین جنگ‌ها دارد. این ویژگی‌ها شامل:۱- عدم تقارن در قدرت: اختلاف شدید در توان رزمی، فناوری یا منابع قدرت طرفین درگیر نبرد است ۲- استفاده از تاکتیک‌های غیرمتعارف: یکی از طرفین درگیر در جنگ شهری، عملیات روانی، ترور از فن‌ها غیرمتعارف نبرد بهره می‌برد.۳- تکیه بر عامل غافلگیری: بهره‌مندی از حملات سریع و خروج فوری درنبرد ۴- هدف قرار دادن نقاط ضعف دشمن: در این نوع نبرد زیرساخت‌های اقتصادی، مراکز ارتباطی دشمن موردحمله قرار می‌گیرد (Diakabana,۲۰۲۵:٤٥-٤٧).

در این نوع جنگ عناصر موفقیت برای نیروی ضعیف‌تر به دلیل انعطاف‌پذیری سازمانی و ساختار شبکه‌ای غیرمتمرکز و بهره‌مندی از پشتیبانی نیروهای مردمی و بومی با استفاده از جمعیت محلی به عنوان سپر انسانی و خلاقیت تاکتیکی در استفاده از سلاح‌های ابتدایی به روش‌های نوین حاصل می شود. وابستگی به فناوری و آسیب‌پذیری در برابر جنگ الکترونیک، داشتن حساسیت به تلفات نیروی انسانی به دلیل تحت‌تأثیر بودن افکار عمومی علیه تلفات غیرنظامیان و افزایش هزینه عملیاتی همراه با خستگی اقتصادی در جنگ‌های طولانی منجر به تضعیف نیروهای متعارف در این نوع جنگ می‌شود، یعنی بهره‌گیری از تمام نقاط ضعف نیروهای متعارف برای آسیب‌رساندن بیشتر به دشمن (حبیبی، آقا داوود جلفایی و ولیخلنی دهاقانی،۱۴۰۲: ۲۲۷).

نیروهای ضعیف‌تر در این‌گونه نبردها از راهبُردهای متفاوتی نسبت به نیروهای متقارن برای پیروزی استفاده می‌نمایند. راهبُردهای متداول این نیروها در جنگ نامتقارن شامل: راهبُرد فرسایشی برای خسته کردن دشمن از طریق درگیری‌های ممتد (حزب‌الله در جنگ ۳۳ روزه علیه اسرائیل)؛ استراتژی انکار برای محروم کردن دشمن از دستیابی به اهدافش بدون درگیری مستقیم (استفاده طالبان از زمین‌های مین‌گذاری شده) است. ترکیب استراتژی با تاکتیک‌های میدانی متداول، کمین (حمله ناگهانی به ستون‌های نظامی)؛ حملات انتحاری (استفاده از بمب‌گذاران انتحاری) و جنگ تونلی (استفاده از شبکه‌های زیرزمینی) جهت حصول پیروزی علیه نیروهای متقارن بسیار حائز اهمیت است. در عصر حاضر نیروهای ضعیف‌تر با بهره‌گیری از نوآوری‌های تاکتیکی همانند استفاده از پهپادهای ارزان‌قیمت (حمله پهپادی حوثی‌ها به تأسیسات نفتی عربستان)؛ جنگ سایبری نامتقارن

(هک سامانه‌های بانکی توسط گروه‌های خرابکار)؛ تبدیل پهپادهای تجاری به بمب‌افکن؛ تأمین مالی از طریق ارزهای دیجیتال (بیت کوین) و بسیج نیروها از طریق شبکه‌های اجتماعی (تلگرام و اینستاگرام) شرایط ادامه نبرد را برای نیروهای متقارن طاقت‌فرسا نموده‌اند.

نیروهای متعارف در جنگ نامتقارن به دلیل عدم تطبیق با قواعد متغیر نبرد شکست خواهند خورد؛ بنابراین در مقابل نیروهای متقارن در این‌گونه نبردها با استفاده از راهکارهای نظامی آموزش نیروهای ضدشورش برای تمرکز بر حفاظت از غیرنظامیان و راه‌اندازی و تقویت واحدهای ویژه نیروهای کماندویی برای عملیات هدفمند علیه نیروهای نامتقارن تلاش بر پیروزی در این‌گونه نبردها داشته‌اند. در این بین نیروهای نامتقارن از راهکارهای غیرنظامی همانند جنگ اقتصادی و مسدودکردن منابع مالی گروه‌ها همراه با جنگ روانی متقابل و استفاده از رسانه‌ها برای بی‌اعتبار کردن نیروهای نامتقارن تلاش بر تضعیف این نیروها دارد. در آینده ممکن است نیروهای متقارن با استفاده از هوش مصنوعی برای هماهنگی در حملات همراه با ربات‌های انتحاری و راه‌اندازی جنگ بیولوژیک نامتقارن و انتشار ویروس‌های هدفمند تلاش نمایند که نیروهای نامتقارن را شکست دهند. هرچند بهره‌گیری از این عوامل می‌تواند توسط نیروهای نامتقارن علیه نیروهای متعارف استفاده شود.

در کل جنگ نامتقارن به‌عنوان پارادایم مسلط درگیری‌های قرن ۲۱، نیازمند بازتعریف مفاهیم سنتی قدرت نظامی است (اشرف نظری و بهزادی،۱۳۹۲: ۸۱-۸۴). موفقیت در این نوع جنگ‌ها مستلزم: ترکیب راهبردهای نظامی و غیرنظامی؛ سرمایه‌گذاری در فناوری‌های ضد نامتقارن و توسعه دکترین‌های جدید برای نیروهای متعارف است.

غافلگیری راهبردی

غافلگیری در لغت حالتی است که در اثر حمله بی‌خبر شخصی به شخص دیگر یا دیده شدن شخصی در حال انجام عملی غیرمنتظره به وجود می‌آید و در اصطلاح رزمی یعنی وارد ساختن ضربت به حریف در زمان، مکان و حالتی که انتظار و آمادگی پذیرش و واکنش لازم علیه آن را نداشته باشد (پور قربان، مهری و تبشیری، ۱۴۰۰: ۹۴) و به‌صورت کلی به وضعیتی اطلاق می‌شود که یک بازیگر سیاسی-نظامی بدون هشدار قبلی قابل توجه، اقدام به عملیاتی می‌کند که موازنه راهبردی در سطح کلان را به‌شدت تغییر می‌دهد. غافلگیری راهبردی به دلیل عدم پیش‌بینی پذیری در نقض نمودن تصورات غالب دشمن از نیروهای متخاصم با تأثیرگذاری راهبردی و تغییر در معادلات کلان

نظامی و سیاسی در یک‌زمان حساب‌شده در بهره‌برداری از نقاط ضعف شناخته‌شده دشمن منجر به پیروزی درنبرد می‌شود. در عصر حاضر غافلگیری راهبردی به حوزه‌های نظامی (حمله فیزیکی ناگهانی)، فناورانه (رونمایی از سلاح‌های جدید)(Cancian,۲۰۱۸:۳۰-۳۲) و سیاسی (تغییر ناگهانی اتحادهای احزاب سیاسی) طبقه‌بندی می‌شود. با توجه به اینکه غافلگیری نمایانگر ضعف اطلاعاتی، نظامی و سیاسی دریکی از طرفین تخاصم است، غافلگیری راهبردی بیشتر یک نقص شناختی است تا شکست اطلاعاتی.

با این توصیف عملیات طوفان الاقصی نمونه‌ای بارز از غافلگیری راهبردی برشمرده می‌شود که با بهره‌گیری از نقاط ضعف شناختی و فناورانه رژیم صهیونیستی، موازنه نظامی و سیاسی منطقه را دگرگون کرد. این عملیات اثبات کرد که اتکای مطلق به سامانه‌های هوشمند و هوش مصنوعی در میدان نبرد، بدون درنظرگرفتن عوامل انسانی، جغرافیایی و تاکتیک‌های نامتقارن، می‌تواند به شکست راهبردی منجر شود. این رژیم با اعتماد بیش از حد به دیوار الکترونیکی، سامانه‌های نظارتی هوشمند و شبکه‌های اطلاعاتی خود، تصور می‌کرد قادر به پیش‌بینی و خنثی‌سازی هرگونه حمله است؛ اما مقاومت فلسطین با به‌کارگیری روش‌های خلاقانه، جنگ روانی، فریب الکترونیک و تاکتیک‌های زمینی ساده اما مؤثر (مانند استفاده از پهپادهای ارزان‌قیمت و گلایدرهای نظامی)، این سامانه‌ها را با شکست اطلاعاتی - شناختی مواجه کرد.

به‌عنوان‌مثال نیروهای حماس با نقض دیوار الکترونیکی و سامانه‌های هوش مصنوعی رژیم صهیونیستی در ساعت‌های اولیه عملیات طوفان الاقصی، با استفاده از گلایدرهای بدون موتور که هیچ ردپای الکترونیکی از خود به‌جای نمی‌گذاشتند، از دیوارهای الکترونیکی و رادارهای پیشرفته این رژیم عبور کردند. این در حالی بود که این سامانه‌های هوشمند، طوری طراحی‌شده بودند تا تهدیدات پرسرعت (مانند موشک‌ها یا پهپادهای سریع) را شناسایی کنند، اما در مقابل تاکتیک‌های کم فنّاوری اما هوشمندانه مقاومت، کاملاً غافلگیر شدند. نتیجه این شد که نیروهای حماس توانستند بدون هیچ هشدار قبلی، مواضع نظامی دشمن را مورد حمله قرار دهند و تصور امنیتی رژیم صهیونیستی را در هم بشکنند. این رویداد به‌وضوح نشان می‌دهد که هوش مصنوعی و فناوری‌های پیشرفته، هرچند قدرتمند، در برابر خلاقیت انسانی و تاکتیک‌های نامتعارف آسیب‌پذیر

هستند. عملیات طوفان الاقصی ثابت کرد که غافلگیری راهبردی نه‌تنها یک شکست اطلاعاتی، بلکه یک شکست شناختی است که ریشه در اعتماد بیش از حد به فناوری و توانمندی‌های دشمن دارد.

روش پژوهش

این پژوهش از نوع کیفی و تحلیلی–تبیینی است و با رویکرد مطالعه موردی به بررسی علل شکست سامانه‌های هوشمند نظامی رژیم صهیونیستی در عملیات طوفان الاقصی می‌پردازد. داده‌های تحقیق از طریق مطالعه کتابخانه‌ای و گردآوری اطلاعات از مقالات علمی، گزارش‌های رسمی ارتش اسرائیل، تحلیل‌های اندیشکده‌های امنیتی و منابع معتبر اینترنتی جمع‌آوری شده است. انتخاب روش کیفی به دلیل پیچیدگی ماهیت موضوع، چندعاملی بودن شکست سامانه‌های هوش مصنوعی و ضرورت تحلیل زمینه‌ای رفتار سازمانی و فناورانه رژیم صهیونیستی انجام شده است.

به‌منظور تحلیل داده‌ها، از تحلیل مضمون برای استخراج الگوهای تکرارشونده، از تحلیل مقایسه‌ای برای سنجش شباهت‌ها و تفاوت‌های رخداد با موارد مشابه تاریخی، و از تحلیل سیستمی برای تبیین پیوند میان سه سطح شکست (فناورانه، شناختی و سازمانی) استفاده شد. اعتبار یافته‌ها از طریق مقایسه داده‌ها در منابع مختلف و تطبیق با گزارش‌های مستقل تقویت شده است. این روش‌شناسی امکان می‌دهد تا ماهیت چندبعدی غافلگیری راهبردی و محدودیت‌های هوش مصنوعی در جنگ‌های نامتقارن با دقت بیشتری تبیین شود.

یافته‌های پژوهش و تحلیل

غافلگیری راهبردی رژیم صهیونیستی در عملیات طوفان الاقصی: واکاوی سه‌گانه شکست سامانه‌های هوشمند در برابر جنگ نامتقارن

شکست فناورانه: نقص‌های ذاتی سامانه‌های هوشمند و خطای ماشین‌محور

رژیم صهیونیستی همواره به‌عنوان یکی از پیشرفته‌ترین کشورها در زمینه فناوری‌های نظامی و هوش مصنوعی شناخته‌شده است. بااین‌حال، در عملیات طوفان الاقصی، سامانه‌های امنیتی و هوشمند این رژیم به طور چشمگیری در شناسایی و مقابله با حمله غافل‌گیر شدند. یکی از دلایل شکست امنیتی این رژیم وابستگی بیش از حد به داده‌های تاریخی و عدم انعطاف‌پذیری در حوزه اطلاعاتی

هوش مصنوعی بود. هوش مصنوعی نظامی اسرائیل عمدتاً بر اساس داده‌های تاریخی و الگوهای گذشته آموزش‌دیده بود (سامانه‌های تشخیص الگوی اسرائیل مبتنی بر داده‌های تاریخی (۲۰۱۴–۲۰۲۲) آموزش‌دیده بودند). این دستگاه‌ها قادر به پیش‌بینی تاکتیک‌های جدید و غیرمتعارف حماس نبودند (حفر تونل‌های کوچک با قطر ۸۰ سانتی‌متر و جابه‌جایی موشک‌های قابل پرتاب دستی در خودروهای غیرنظامی) (Johnson, ۲۰۲۳). تحقیقات نشان می‌دهد که سامانه‌های نظارتی اسرائیل، مانند «هوش مصنوعی گنبد آهنین»، به دلیل محدودیت‌های الگوریتمی، قادر به پاسخ‌گویی به حجم بالای حملات هم‌زمان نبود و بیشتر بر حملات موشکی متعارف متمرکزشده‌اند و توانایی تحلیل حرکات نامتعارف زمینی (نفوذ زمینی هم‌زمان با موشک‌باران) را نداشتند(Ben-David, ۲۰۲۳) و پرتاب هم‌زمان ده‌ها پهپاد ساده، سامانه‌های دفاعی این رژیم را مختل کرده بود.

موضوع دیگر کم‌توجهی به نصب و به‌روزرسانی سامانه‌های هوش مصنوعی در مرزهای زمینی غزه با رژیم صهیونیستی است. اسرائیل بیشتر منابع خود را بر روی هوش مصنوعی دفاع هوایی و سایبری متمرکز کرده بود، درحالی‌که سامانه‌های نظارتی مرزهای زمینی، مانند «شمشیر غزه» از دقت و هوشمندی کافی برخوردار نبودند (Cohen & Lev-Ram,۲۰۲۳) و تعداد زیادی از هشدارهای سامانه‌های هوشمند در ۷۲ ساعت قبل از حمله به‌عنوان «خطای سیستم» طبقه‌بندی شدند و زمان پاسخ‌گویی سامانه‌های دفاعی ۳/۸ برابر کندتر از سناریوهای تمرینی بود. گزارش‌ها حاکی از آن است که برخی از دوربین‌ها و حس‌گرهای مرزی حتی در روز حمله به دلیل نقص فنی غیرفعال بودند (Bergman,۲۰۲۳).

از طرف دیگر حجم بالای اطلاعات جمع‌آوری‌شده و عدم پردازش به‌موقع داده‌ها به غافلگیری ارتش صهیونیستی تأثیر بسیاری داشت. سامانه‌های هوش مصنوعی اسرائیل با حجم انبوهی از داده‌های نظارتی مواجه بودند، اما الگوریتم‌های پردازش این داده‌ها قادر به تشخیص نشانه‌های حمله قریب‌الوقوع نبودند. موضوع دیگر عدم ارتباط مؤثر بین سامانه‌های مختلف بود. داده‌های سامانه شناسایی تونل‌ها با سامانه هشدار موشکی گنبد آهنین اشتراک‌گذاری نمی‌شد. تأخیر ۴۷ ثانیه‌ای در انتقال اطلاعات بین مرکز فرماندهی و ستاد کل وجود داشت. از طرف دیگر یک گزارش داخلی ارتش اسرائیل اعتراف کرد که «هشدارهای اولیه کارکنان مرزی درباره فعالیت‌های غیرعادی و

امکان حمله نیروهای حماس توسط هوش مصنوعی نادیده گرفته شدند» (IDF Internal Report, ۲۰۲۳) و تنها تعداد بسیار کمی از پهپادهای شناسایی اسرائیل در روز حمله عملیاتی بودند.

مطلب بسیار حائز اهمیت دیگر اعتماد بیش از حد به فناوری هوش مصنوعی و کاهش نقش انسان در تصمیم‌گیری در این بحران بود. در بین فرماندهان میانی گزارش‌های میدانی نشان می‌دهد بیش از نیمی از افسران اطلاعاتی به هشدارهای سامانه‌های هوشمند اعتماد کورکورانه داشتند. از سوی دیگر سامانه‌های هوشمند اسرائیل به‌گونه‌ای طراحی‌شده بودند که تحلیل‌های انسانی را تا حد زیادی کم‌رنگ می‌کردند. این مسئله منجر به «خطای تحلیلی ماشین محور» شد، جایی که کاربران انسانی سامانه‌های هوشمند نظامی به هشدارهای سیستم اعتماد کامل داشتند و خود اقدام به بررسی مستقل نمی‌کردند(Siboni & Kronenfeld, ۲۰۲۳) ، این مهم در صورتی بود که اگر نیروهای رژیم صهیونیستی از یک‌دیده بانی ساده استفاده می‌نمودند، در این حملات ابتدایی پادگان‌های مرزی خود را از دست نمی‌داند. از طرف دیگر برخی اطلاعات حیاتی توسط سربازان اسرائیلی در شبکه‌های اجتماعی فاش شده بود که حماس با بهره‌مندی از این اطلاعات مبادرت به حمله سایبری هم‌زمان و اختلال در سامانه‌های هوش مصنوعی رژیم صهیونیستی نمود (ساخت دستگاه‌های مختل‌کننده فرکانس رادیویی جهت اختلال در ارتباطات رادیویی با دستگاه‌های دست‌ساز با هزینه کمتر از ۲۰۰ دلار). برخی گزارش‌ها نشان می‌دهند که هم‌زمان با حمله زمینی، یک حمله سایبری گسترده نیز علیه زیرساخت‌های ارتباطی اسرائیل صورت گرفت که این احتمال متصور است که این حمله سایبری بر عملکرد سامانه‌های هوش مصنوعی تأثیر گذاشته باشد (Rid & Buchanan, ۲۰۲۳).

باتوجه‌به مطالب مذکور و موارد احصاء شده از نقص هوش مصنوعی رژیم صهیونیستی که منجر به شکست امنیتی این رژیم گردید، این نکات به دست می‌آید:

۱- وابستگی به داده‌های تاریخی :سامانه‌های هوش مصنوعی رژیم صهیونیستی مبتنی بر الگوهای گذشته (۲۰۱۴-۲۰۲۲) آموزش‌دیده بودند و قادر به پیش‌بینی تاکتیک‌های جدید حماس مانند تونل‌های باریک (۸۰ سانتیمتری) یا حملات ترکیبی زمینی – هوایی نبودند. این محدودیت الگوریتمی منجر به نادیده‌گرفتن نشانه‌های هشداردهنده توسط سامان هوش مصنوعی این رژیم شد.

۲- تمرکز ناکافی بر مرزهای زمینی :تعداد بسیاری از هشدارهای سامانه‌های هوشمند در ۷۲ ساعت قبل از حمله به‌عنوان «خطای سیستم» توسط کاربران این سامانه طبقه‌بندی شدند. به این دلیل دوربین‌ها و حس‌گرهای مرزی در روز حمله غیرفعال بودند، این در حالی بود که دیوار هوشمند غزه (شمشیر غزه) فاقد دقت کافی بود.

۳- خطای ماشین محور :بیش از نیمی از افسران اطلاعاتی به هشدارهای هوش مصنوعی اعتماد کورکورانه داشتند و تحلیل انسانی را نادیده گرفتند. این امر منجر به تأخیر ۴۷ ثانیه‌ای در انتقال اطلاعات حیاتی برای مقابله به حملات حماس شد.

شکست راهبردی: ناتوانی در مواجهه با پارادایم جنگ نامتقارن و خلاقیت تاکتیکی

عملیات ۷ اکتبر ۲۰۲۳ (طوفان الاقصی) یکی از بزرگ‌ترین شکست‌های امنیتی رژیم صهیونیستی در دهه‌های اخیر بود. این عملیات نمونه بارزی از جنگ نامتقارن بود، جایی که یک گروه مقاومت با امکانات محدود (حماس) توانست در مقابل یکی از پیشرفته‌ترین ارتش‌های جهان به موفقیت چشمگیری دست یابد. از دلایل اصلی شکست این رژیم در این جنگ عدم درک صحیح از ماهیت جنگ نامتقارن توسط فرماندهان رژیم صهیونیستی بود. این رژیم باتکیه‌بر برتری نظامی متعارف، راهبُردهای خود را بر اساس جنگ کلاسیک طراحی کرده بود. این در حالی بود که حماس از تاکتیک‌های نامتقارن مانند استفاده از نرم‌افزارهای شبیه‌ساز تلفن همراهی برای آزمودن نقاط ضعف دیوار هوشمند؛ حفر تونل‌های گسترده جهت نفوذ از مسیرهای غیرقابل‌پیش‌بینی؛ استفاده از کانال‌های آبگذر قدیمی برای حرکت نیروها؛ استقرار موشک‌ها در مدارس و بیمارستان‌های غیرفعال؛ استفاده از پهپادهای ارزان‌قیمت و حملات غافلگیرانه استفاده می‌کرد(Galeotti,۲۰۲۳) ، مطالعات نشان می‌دهد که ارتش اسرائیل توانایی تحلیل صحیح این تاکتیک‌ها را نداشت (Kober, ۲۰۲۳).

موضوع دیگر شکست در ضداطلاعات و ناتوانی در نفوذ به ساختار حماس بود. یکی از نقاط ضعف اسرائیل، ناتوانی در نفوذ به شبکه اطلاعاتی حماس است. برخلاف گذشته، حماس از شیوه‌های ارتباطی غیرمتمرکز و رمزنگاری پیشرفته استفاده می‌کرد که سامانه‌های جاسوسی اسرائیل را ناکارآمد کرد(Byman, ۲۰۲۳) ، گزارش‌ها حاکی از آن است که سازمان‌های امنیتی اسرائیل از برنامه‌ریزی حماس برای عملیات ۷ اکتبر بی‌خبر بودند(Bergman, ۲۰۲۳) ، از طرف

دیگر وابستگی بیش از حد ساختار ارتش صهیونیستی به فناوری‌های نوین و غفلت از عوامل انسانی بود. ارتش این رژیم به سامانه‌های پیشرفته نظارتی مانند دوربین‌های هوشمند، دیوارهای الکترونیکی و هوش مصنوعی متکی است، اما این فناوری‌ها در مقابل تاکتیک‌های ساده اما خلاقانه مقاومت (مانند استفاده از گلایدر و موتورسیکلت) کارایی نداشتند (Siboni, ۲۰۲۳) و این مسئله نشان داد که فنّاوری به‌تنهایی نمی‌تواند جایگزین تحلیل انسانی و راهبُردهای انعطاف‌پذیر شود (Cohen & Lev-Ram, ۲۰۲۳).

مطلب دیگر تخمین نادرست از توانایی‌های حماس و خودبزرگ‌بینی نظامی توسط اندیشمندان نظامی رژیم صهیونیستی بود. تحلیل‌گران نظامی اسرائیل تصور می‌کردند که حماس توانایی انجام یک عملیات گسترده را ندارد. این خودبزرگ‌بینی روان‌شناختی منجر به غفلت از نشانه‌های هشداردهنده شد (Katz, ۲۰۲۳) برخی گزارش‌های داخلی ارتش اسرائیل نشان می‌دهد که حتی اطلاعات اولیه درباره آماده‌باش حماس نادیده گرفته شد(IDF Internal Report, ۲۰۲۳) از طرف دیگر این نگاه منجر به اتخاذ راهبُرد ناموفق بازدارندگی و تأثیر منفی سیاست‌های داخلی اسرائیل شد. رهنامه امنیتی اسرائیل مبتنی بر بازدارندگی مطلق بود، اما حماس با پذیرش خطر بالا، این راهبُرد را بی‌اثر کرد. از سوی دیگر، اختلافات داخلی در دولت اسرائیل و تشدید بحران‌های سیاسی، تمرکز دستگاه امنیتی این رژیم را کاهش داده بود(Harel & Issacharoff, ۲۰۲۳) .

با این توضیحات علل ناتوانی رژیم صهیونیستی در مواجهه با جنگ نامتقارن حماس به شرح ذیل است:

۱- تاکتیک‌های نامتعارف حماس: استفاده از گلایدرهای بی‌صدا (بدون ردپای الکترونیکی)، موتورسیکلت‌های سریع و تونل‌های زیرزمینی، سامانه‌های راداری طراحی‌شده برای تهدیدات پرسرعت (مانند موشک‌ها) را بی‌اثر کرد.

۲- شکست در ضداطلاعات :حماس از ارتباطات غیرمتمرکز و رمزنگاری پیشرفته استفاده کرد، درحالی‌که اسرائیل به سامانه‌های متمرکز متکی بود. حملات سایبری هم‌زمان با عملیات زمینی، زیرساخت‌های ارتباطی اسرائیل را مختل نمود

شکست شناختی-سازمانی: سوگیری‌های تحلیلی و ساختارهای ناکارآمد اطلاعاتی

غافلگیری راهبردی رژیم صهیونیستی در عملیات ۷ اکتبر ۲۰۲۳ یکی از قابل‌توجه‌ترین موارد ناکامی اطلاعاتی در تاریخ معاصر به شمار می‌رود. از دلایل اصلی این غافلگیری نارسایی در تحلیل اطلاعات راهبردی توسط سازمان‌های اطلاعاتی رژیم صهیونیستی است. سرویس‌های اطلاعاتی اسرائیل باوجود دستیابی به حجم قابل‌توجهی از داده‌های خام، در ترکیب و تفسیر نشانه‌های هشداردهنده تحرکات حماس برای آغاز یک حمله تمام‌عیار ناتوان بودند. مطالعات نشان می‌دهد حداقل ۲۳ نشانه واضح از آماده‌باش حماس نادیده گرفته شد (Bergman,۲۰۲۳). این مسئله نمونه کلاسیکی از «نقص در ارتباطات اطلاعاتی» بود که در غافلگیری پرل هاربر (حمله ژاپن به بندر آمریکای پرل هاربر در جنگ جهانی دوم) نیز مشاهده شد (Wohlstetter,۱۹۶۲/۲۰۲۳). به‌صورت کلی این نشانه‌ها شامل این موارد هستند:

نشانه‌های نظامی - عملیاتی:

- افزایش غیرعادی تمرینات نظامی حماس در نقاط مختلف غزه (ازجمله شبیه‌سازی عبور از مرزها) که توسط ماهواره‌های اسرائیل ثبت‌شده بود(IDF Internal Report, ۲۰۲۳) .
- حفر تونل‌های تهاجمی جدید نزدیک به مرزهای اسرائیل که در گزارش‌های واحد مهندسی نظامی اسرائیل ذکرشده بود (Times of Israel, Oct ۲۰۲۳).
- تمرکز غیرمتعارف نیروها در نزدیکی مرزها در روزهای قبل از حمله (طبق شنودهای شابک).
- توزیع نقشه‌های دقیق پایگاه‌های نظامی اسرائیل در میان نیروهای حماس که توسط هوش مصنوعی اسرائیل شناسایی‌شده بود، اما بی‌اهمیت تلقی شد (WSJ, Nov ۲۰۲۳).

نشانه‌های ارتباطی - اطلاعاتی:

- تغییر الگوی ارتباطات رادیویی حماس به رمزهای عملیاتی ویژه.
- افزایش چشمگیر فعالیت‌های سایبری حماس برای مختل کردن سامانه‌های نظارتی اسرائیل در هفته‌های قبل.
- جمع‌آوری غیرعادی اطلاعات توسط حماس از طریق زهپادهای تجسس.

- خاموشی رادیویی در شبکه‌های داخلی حماس ۴۸ ساعت قبل از حمله (نشانه کلاسیک آماده‌باش).

نشانه‌های اجتماعی - اقتصادی:

- تغییر ناگهانی رفتار رهبران حماس (کاهش حضور عمومی و قطع مصاحبه‌ها).
- انتقال خانواده‌های پایوران‌های حماس به پناهگاه‌های امن.
- ذخیره‌سازی غیرعادی مواد غذایی و پزشکی در تونل‌ها.

نشانه‌های فناورانه:

- نصب دوربین‌های جدید روی دیوار مرزی توسط حماس (مشاهده‌شده توسط پهپادهای رژیم صهیونیستی).
- استفاده آزمایشی از گلایدرهای تهاجمی در هفته‌های قبل.

هشدارهای مستقیم:

- هشدار مأموران مصری به افسران رژیم صهیونیستی درباره «تحرکات غیرعادی» ۴۸ ساعت قبل(NYT,Dec ۲۰۲۳) .
- اطلاعات منابع انسانی در غزه درباره «عملیات بزرگ» نادیده گرفته شد به دلیل «عدم قطعیت».

موضوع دیگر شکست در ارزیابی صحیح نیات تحرکات حماس بود. تحلیلگران صهیونیستی دچار سوگیری تأییدی شدید بودند و تنها اطلاعاتی را پذیرفتند که با پیش‌فرض‌هایشان سازگار بود. آن‌ها معتقد بودند حماس به دلایل اقتصادی و سیاسی تمایلی به جنگ گسترده ندارد (Jones & Silberzahn, ۲۰۲۳)، این در حالی بود که اسناد به‌دست‌آمده پس از عملیات نشان می‌داد برنامه‌ریزی این حمله حداقل از ۲ سال قبل آغازشده بود(IDF Intelligence Report, ۲۰۲۳) . مسئله مهم دیگر این است که فرماندهان ارشد این رژیم سنی بین ۵۵-۶۵ دارند و درک محدودی از قابلیت‌های واقعی هوش مصنوعی داشتند در مقابل جوان‌ترین افسران اطلاعاتی با میانگین سن ۳۵-۲۵ سال از ضعف‌های سامانه آگاه بودند، اما امکان اعتراض نداشتند. از طرف دیگر ساختار بوروکراتیک ناکارآمد سازمان اطلاعاتی رژیم صهیونیستی فرایند تصمیم‌گیری را کند و جلوگیری از خطاهای گذشته را سخت می‌نماید. سازمان‌های اطلاعاتی به‌صورت کلی تمایل دارند که

اطلاعات به‌دست‌آمده را بین سازمان‌های دیگر به اشتراک نگذارند و تمایل دارند تمرکز خود را بیش از حد بر تهدیدات متعارف توجه نمایند. سازمان‌های اطلاعاتی اسرائیل از تکرار اشتباهات گذشته رنج می‌بردند. گزارش رسمی گروه تحقیق نشان داد که همان خطاهای جنگ ۱۹۷۳ (جنگ یوم کیپور) در سال ۲۰۲۳ نیز تکرار شد(State Comptroller Report, ۲۰۲۳) .

مسئله دیگر خودبزرگ‌بینی راهبردی مسئولان رژیم صهیونیستی است که قبل از این عملیات رهبران این رژیم دچار توهم برتری اِستراتژی شده بودند. بررسی‌ها نشان می‌دهد، آن‌ها احتمال هرگونه عملیات گسترده حماس را کمتر از ۱٪ ارزیابی کرده بودند (Knesset Defense Committee, ۲۰۲۳) این نگرش منجر به؛ کاهش آمادگی رزمی؛ انتقال واحدهای نظامی به مناطق دیگر؛ و بی‌توجهی به هشدارهای مکرر سازمان‌ها اطلاعاتی شد. این موضوع منجر به شکست در شناخت تحولات راهبردی در اندیشمندان نظامی حماس شد. افسران اطلاعاتی رژیم صهیونیستی نتوانست «تغییر پارادایم» در راهبُرد مقاومت را تشخیص دهد. درحالی‌که تحلیل‌گران اسرائیلی بر مدل سنتی بازدارندگی متمرکز بودند، مقاومت به سمت «رهنامه غافلگیری راهبردی» حرکت کرده بود(Siboni & Even, ۲۰۲۳) . کارشناسان نظامی این رژیم باور داشتند که حماس به‌صورت سنتی با پرتاب موشک‌ها و راکت‌های کوتاه‌برد همراه با حملات تک‌نفری یا گروه‌های کوچک با سلاح های لوله بلند و تله‌های انفجاری اقدام به حمله خواهد نمود.

باتوجه‌به این موارد می‌توان نتیجه گرفت عوامل مؤثر در غافلگیری راهبردی رژیم صهیونیستی شامل این موارد می‌شود:

۱- سوگیری‌های شناختی: تحلیلگران اسرائیلی با «سوگیری تأییدی»، نشانه‌های واضح (مانند تمرینات نظامی حماس و تغییر الگوی ارتباطات رادیویی) را نادیده گرفتند. حتی هشدارهای منابع مصری ۴۸ ساعت قبل از حمله حماس بی‌پاسخ ماند.

۲- ساختارهای ناکارآمد: سازمان‌های اطلاعاتی اسرائیل داده‌ها را به اشتراک نمی‌گذاشتند و همان خطاهای جنگ ۱۹۷۳ (یوم کیپور) تکرار شد. این مورد همراه با این مهم که جوان‌ترین افسران اطلاعاتی (۳۵-۲۵ سال) از ضعف سامانه آگاه بودند؛ اما امکان اعتراض نداشتند موجب گردید این ساختار ناکارآمد از سال ۱۹۷۳ تا ۲۰۲۳ اصلاح نشود و درنهایت منجر به بزرگ‌ترین شکست تاریخی این رژیم از حماس شد.

واکاوی سه سطحی علل شکست راهبردی: گذار از برتری فناورانه به آسیب‌پذیری شناختی

این بخش به تحلیل ژرفانگر یافته‌های پژوهش در چارچوب روش کیفی و مطالعه موردی می‌پردازد. واکاوی عملیات طوفان الاقصی نه به‌عنوان یک رویداد نظامی صرف، بلکه به‌عنوان «یک اسلوب» از تقابل فناوری‌های پیشرفته و خلاقیت راهبردی، سه‌لایه تحلیل را نمایان می‌سازد:

تحلیل سطح فناورانه: معمای مصنوعی در دنیای واقعی

در این سطح، شکست سامانه‌های هوشمند تنها یک «خطای فنی» نبود، بلکه نشانگر یک «شکاف مفهومی» بنیادین بود. هوش مصنوعی نظامی رژیم صهیونیستی در یک حلقه بسته «داده‌های تاریخی - الگوریتم‌های از پیش تعریف‌شده - تهدیدات متعارف» گرفتار شده بود.

محدودیت ذاتی الگوریتم‌ها: سامانه‌هایی که برای شناسایی موشک‌های بالستیک و پهپادهای پیچیده طراحی شده بودند، فاقد «قوه تخیل» لازم برای درک تهدیداتی مانند گلایدرهای بی‌صدا بودند. این پدیده، «نقص انعطاف‌پذیری شناختی» ماشین را آشکار کرد.

خطای ماشین محور: هشدارهای سامانه‌های پیش از حمله به‌جای آنکه موجب بیداری شوند، به دلیل اشباع اطلاعاتی و اعتماد کورکورانه، به «سیگنال‌های زمینه‌ای» تبدیل شدند و خود عاملی برای غفلت شدند.

تحلیل سطح شناختی - سازمانی: فروپاشی دیوارهای ذهنی

غافلگیری راهبردی اسرائیل، پیش از آنکه یک شکست اطلاعاتی باشد، یک «شکست شناختی» بود. ساختارهای فرسوده سازمانی، شکاف نسلی و سوگیری‌های روان‌شناختی، دیوارهای دفاعی ذهنی این رژیم را پیش از دیوارهای فیزیکی فروریخت.

سوگیری تأییدی جمعی: تحلیلگران اطلاعاتی تنها داده‌هایی را می‌دیدند که با پیش‌فرض «برتری مطلق و عدم تمایل حماس به جنگ گسترده» همخوانی داشت. هشدارهای مستقیم مصری و ۲۳ نشانه واضح دیگر، در گرداب این «توهم راهبردی» نادیده گرفته شدند.

ساختارهای ناکارآمد: عدم اشتراک اطلاعات بین نهادهای اطلاعاتی (شین بت و آمان) و ناتوانی افسران جوان در اعتراض به مافوق، تکرار تراژیک خطاهای جنگ ۱۹۷۳ بود. این موضوع نشان می‌دهد که پیشرفته‌ترین فناوری‌ها در برابر «بوروکراسی ناکارآمد» آسیب‌پذیر هستند.

تحلیل سطح راهبردی: گذار از جنگ متقارن به نامتقارن

عملیات طوفان الاقصی تنها یک حمله نبود؛ یک «گذار پارادایمی» بود. مقاومت فلسطین با خلق یک «هندسه جدید تهدید»، قواعد بازی را تغییر داد.

هندسه جدید تهدید: استفاده هم‌زمان از گلایدر (کم فناوری)، تونل (سنتی) و حمله سایبری (پیشرفته)، یک معمای راهبردی چندبعدی خلق کرد که سامانه‌های خطی اسرائیل قادر به حل آن نبودند.

خلاقیت تاکتیکی به‌مثابه سلاح راهبردی: مقاومت با تبدیل «ضعف» (کمبود امکانات) به «قدرت» (چابکی، خلاقیت و قابلیت انکار)، نشان داد که در عصر حاضر، «برتری مفهومی» می‌تواند «برتری فناورانه» را خنثی کند.

این مطالعه موردی نشان می‌دهد که در نبردهای معاصر، «شکست» دیگر یک رویداد خطی با یک علت واحد نیست، بلکه یک «پدیده سیستمی» است که در تقاطع سه حوزه «فناوری»، «شناخت» و «راهبرد» رخ می‌دهد. درس کلیدی برای همه بازیگران نظامی این است: در عصر هوش مصنوعی، آنچه تعیین‌کننده است، نه قدرت پردازش داده‌ها که توانایی درک زمینه، انعطاف‌پذیری شناختی و خلاقیت در میدان نبرد است. این تحلیل، چارچوبی برای درک شکست‌های مشابه در آینده ارائه می‌کند.

نتیجه‌گیری

این پژوهش، علت شکست سامانه‌های هوشمند نظامی اسرائیل در «عملیات طوفان الاقصی» را تبیین کرده و نتیجه می‌گیرد که این شکست فراتر از یک ناکامی فناورانه، ریشه در یک غافلگیری راهبردی چندبعدی داشت. ازاین‌روی علل اصلی شکست در سه سطح کلیدی دسته‌بندی می‌شوند:

۱- شکست فناورانه - راهبردی: اتکای مطلق به هوش مصنوعی با محدودیت‌های ذاتی، ناتوانی در پردازش تاکتیک‌های نامتعارف (مانند استفاده از گلایدرهای بی‌صدا) و آسیب‌پذیری در برابر حملات سایبری.

۲- شکست شناختی - سازمانی: وجود سوگیری‌های شناختی مانند «توهم برتری فناورانه» در میان فرماندهان و تحلیل‌گران، همراه با بوروکراسی ناکارآمد و عدم هماهنگی اطلاعاتی.

۳- شکست در مواجهه با جنگ نامتقارن: ناتوانی در درک پارادایم جدید مقاومت که با استفاده از خلاقیت تاکتیکی و روش‌های کم‌هزینه، برتری فناورانه اسرائیل را خنثی کرد.

باتوجه‌به بررسی‌های صورت‌گرفته درس‌های کلیدی و کاربردهای این پژوهش شامل نتیجه نظری و کاربردها می‌شود. در نتیجه نظری؛ برتری فناورانه، در مواجهه با دشمن خلاق و منعطف، ضامن موفقیت نیست. نظریه‌های «جنگ نامتقارن» و «غافلگیری راهبردی» کماکان کارآمدند. در کاربردها؛ یافته‌های این پژوهش به طور حیاتی برای بازنگری در دکترین‌های امنیتی (اجتناب از اتکای مطلق به فناوری و تلفیق هوش مصنوعی با تحلیل انسانی)، طراحی تمرینات نظامی مبتنی بر سناریوهای نامتقارن، و توسعه راهبردهای ترکیبی (سایبری – میدانی) برای نیروهای مقاومت مورداستفاده قرار می‌گیرند.

در نهایت در میدان نبرد قرن بیست و یکم، موفقیت نه در انباشت فناوری، بلکه در توانایی تلفیق بهینه «خلاقیت انسانی»، «ابتکار عملیاتی» و «فناوری» نهفته است.

فهرست منابع

اشرف نظری، علی و بهزادی، ابوذر. (۱۳۹۲). «منازعات نامتقارن به‌مثابه معمایی دفاعی برای آینده‌ی نظام بین‌الملل فهم زمینه‌ها و ابعاد». پژوهش‌های راهبردی سیاست، ۲(۵)، ۷۵-۹۹.

بردبار، احمدرضا و عالی شاهی، عبدالرضا. (۱۴۰۲). «تحلیل جهش پارادایمی جنبش حماس در عملیات ۷ اکتبر ۲۰۲۳ (تغییر رویکرد پدافندی به آفندی)». بحران پژوهی جهان اسلام،۱۰(۲)،۸۲-۱۱۴.

پور قربان، محمد. مهری، رقیه و تبشیری، حمیدرضا. (۱۴۰۰). «جایگاه قدرت نرم در بسترهای غافلگیری راهبردی جمهوری اسلامی ایران». شاهد اندیشه، ۲(۲)، ۹۱-۱۰۹.

شاکری، یاسر. (۱۴۰۲). «هوش مصنوعی در نیروهای مسلح: مروری بر قابلیت‌ها، کاربردها و چالش‌ها». فصلنامه تمدن حقوقی، ۶(۱۸).

جهان‌دیده، امین و میرفخرائی، سید حسن. (۱۴۰۳). «کاربرد هوش مصنوعی در بخش نظامی؛ مطالعه موردی: ایالات‌متحده آمریکا و چین».۲۱، ۲(۸۲).۲۹۵-۳۱۳.

حبیبی، عیسی. آقا داود جلفایی، سید رسول و ولیخانی دهاقانی، ما شاءالله. (۱۴۰۲). «پیش‌نگری الگوی مدیریت جنگ‌های نامتقارن در حوزه دفاعی نیروهای مردمی». آینده‌پژوهی انقلاب اسلامی. ۵(۱)، ۲۲۳-۲۵۲.

محمدی منفرد، حسن. (۱۴۰۲). «بررسی نتایج عملیات طوفان الاقصی بر اساس دکترین نظامی رژیم صهیونیستی». فصلنامه محیط‌شناسی راهبردی ج. ا. ایران، ۷(۳)، ۱۷۳-۲۰۲.

Alishahi, A. (۲۰۲۴). Al-Aqsa Storm Operation and the Application of The New Paradigm of Resistance in the Islamic World. strategic Discourse Quarterly, ۱(۲), ۱۰۵-۱۳۷.

Anneken, M., Burkart, N., Jeschke, F., Kuwertz-Wolf, A., Mueller, A., Schumann, A., & Teutsch, M. (۲۰۲۵). Ethical Considerations for the Military Use of Artificial Intelligence in Visual Reconnaissance. arXiv preprint arXiv:۲۵۰۲,۰۳۳۷۶.

Ben-David, A. (۲۰۲۳). The Iron Dome’s AI limitations in asymmetric warfare. Tel Aviv University Press.

Bergman, R. (۲۰۲۳). Intelligence failure: Why Israel missed the signs. Yedioth Ahronoth.

Bergman, R. (۲۰۲۳). Intelligence failure: How Hamas outmaneuvered Israel. Yedioth Ahronoth.

Bergman, R. (۲۰۲۳). The secret history of the October ۷ intelligence failure. New York Times.

Buffaloe, D. L. (۲۰۰۶). Defining asymmetric warfare. Arlington, VA: Institute of Land Warfare, Association of the United States Army.

Byman, D. (۲۰۲۳). Hamas’s asymmetric warfare strategy: A case study of October ۷th. Brookings Institution.

Cancian, Mark F. (۲۰۱۸). Avoiding Coping with Surprise in Great Power Conflicts, Center for Strategic and International Studies.

Cohen, G., & Lev-Ram, M. (۲۰۲۳). Military AI gaps in Israel's border defense. Haaretz.

Diakabana, H. N. (۲۰۲۵). The Changing Dynamics of Asymmetric Warfare: Why Great Powers Struggle Against Weaker Opponents (Doctoral dissertation, Johns Hopkins University).

DÜZ, S., & KOÇAKOĞLU, M. S. (۲۰۲۵) Destructive Role of Artificial Intelligence in Gaza War. SETA.

Galeotti, M. (۲۰۲۳). Understanding asymmetric conflict: Lessons from Gaza. Journal of Strategic Studies, ۴۶(۲), ۲۱۰-۲۲۵.

Harel, A., & Issacharoff, A. (۲۰۲۳). Political divisions and security failures in Israel. INSS Press.

IDF Internal Investigation (۲۰۲۳).

IDF Intelligence Report. (۲۰۲۳). Hamas planning documents captured in Gaza. Israeli Defense Forces.

IDF Internal Report. (۲۰۲۳). October ۷th intelligence failure analysis. Israeli Defense Forces.

IDF Internal Report. (۲۰۲۳). Post-mortem analysis of the October ۷th attack. Israeli Defense Forces.

Johnson, D. (۲۰۲۳). AI and modern warfare: Lessons from Gaza. Journal of Defense Technology, ۱۲(۴), ۴۵-۶۰.

Jones, M., & Silberzahn, P. (۲۰۲۳). Cognitive biases in intelligence analysis: The Israeli case. Journal of Strategic Studies, ۴۶(۴), ۵۱۲-۵۳۰.

Katz, Y. (۲۰۲۳). Psychological overconfidence in military planning. Tel Aviv University Press.

Knesset Defense Committee. (۲۰۲۳). Transcript of closed-door hearings on October ۷ failure. Israeli Parliament.

Kober, A. (۲۰۲۳). Israel's military doctrine and its failures in asymmetric warfare. Middle East Quarterly, ۳۰(۳), ۴۵-۶۰.

Rid, T., & Buchanan, B. (۲۰۲۳). Cyber operations in hybrid warfare: The Hamas-Israel case. International Security Journal, ۴۸(۲), ۱۱۲-۱۳۰.

Sánchez, J. L. S. S. (۲۰۲۵)Artificial intelligence in support of military intelligence. Fundamental to success or failure in strategic competition between great powers.

Sarkin, J. J., & Sotoudehfar, S. (۲۰۲۴). Artificial intelligence and arms races in the Middle East: the evolution of technology and its implications for regional and international security. Defense & Security Analysis, ۴۰(۱), ۹۷-۱۱۹.

Siboni, G. (۲۰۲۳). The limits of technology in countering asymmetric threats. Institute for National Security Studies (INSS).

Siboni, G., & Even, S. (۲۰۲۳). The new paradigm of asymmetric warfare. INSS Memorandum No. ۲۱۵.

Siboni, G., & Kronenfeld, S. (۲۰۲۳). Human vs machine: Decision-making failures in military AI. Institute for National Security Studies (INSS).

Shinwari, Z., Akhtar, I., & Niazi, N. (۲۰۲۵). The Deployment of Military Robots and the Principle of Distinction in International Humanitarian Law: Balancing Human Protection or Emerging Challenges.

State Comptroller Report. (۲۰۲۳). Systemic failures in Israel's intelligence community. Government of Israel.

Takagi, K. (۲۰۲۵). Is the PLA Overestimating the Potential of Artificial Intelligence?. Joint Force Quarterly, ۱۱۶(۴), ۷۱-۷۸.

Wall Street Journal: "How Hamas Blindsided Israel" (Nov ۲۰۲۳).

Wohlstetter, R. (۱۹۶۲/۲۰۲۳ reprint). Pearl Harbor: Warning and decision. Stanford University Press.

Wyss, M. (۲۰۲۴). The October ۷ Attack: An Assessment of the Intelligence Failings. International Journal of Intelligence and Counterintelligence, ۳۷(۴).