نشریه علمی آفاق اطلاعات

پالانتیر، لوتِم : سلاح فناورانه غرب در خدمت ماشین کشتار رژیم صهیونیستی

محمدعلی عابدی[1]

۶
سال دوم
تابستان ۱۴۰۴
مقاله پژوهشی
تاریخ دریافت:
۱۴۰۴/۰۶/۰۳
تاریخ پذیرش:
۱۴۰۴/۰۶/۲۳
صص: ۴۰-۱۱

چکیده

در عصر تسلط داده‌ها و ابزارهای هوش مصنوعی، همگرایی شرکت‌های فناوری غربی با ساختارهای امنیتی ـ نظامی اسرائیل، نحوه‌ی گردآوری، تحلیل و کاربرد اطلاعات در میدان‌های نبرد را بازتعریف کرده است. این مقاله با هدف تحلیل نقش شرکت پالانتیر و واحد فناوری لوتِم در تقویت ظرفیت‌های هدف‌یابی، جنگ الکترونیک و عملیات سایبری رژیم غاصب صهیونیستی و بررسی نقش تسهیل‌گران ابری مانند گوگل و مایکروسافت انجام شده است. روش تحقیق، تحلیل کیفی اسناد رسمی، گزارش‌های معتبر بین‌المللی و منابع رسانه‌ای و پژوهشی است. یافته‌ها نشان می‌دهد پالانتیر از طریق پلتفرم‌های تحلیلیِ چندمنبعه، تحلیل گراف و مدل‌های یادگیری ماشین، فرایند تولید فهرست‌های هدف و هشداردهی لحظه‌ای را سرعت و خودکارسازی می‌کند؛ در مقابل، لوتِم با یکپارچه‌سازی این ابزارها و بهره‌گیری از زیرساخت‌های ابری، نقش عملیاتی‌کننده و تسهیل‌گر در جنگ اطلاعاتی و عملیات قابل اتکا را ایفا می‌کند. در عین حال، توسعه‌ی این پیوستگی فناوری ـ نظامی پیامدهای مهم اخلاقی، حقوق بشری و حقوقی (شامل شفافیت الگوریتمی، مسئولیت‌پذیری در تصمیم‌های مرگبار و خطرات افزایش خودمختاری سامانه‌ها) را به همراه دارد. مقاله در پایان پیشنهاد می‌کند که برای کاهش مخاطرات، چارچوب‌های نظارتی جامع، مکانیزم‌های ارزیابی مستقل و محدودیت‌های کاربردی برای سامانه‌های تصمیم‌یار نظامی تدوین و اجرا شوند.

کلیدواژه‌ها: پالانتیر، لوتِم، هوش مصنوعی، هدف‌یابی نظامی، جنگ سایبری.

---

۱ .دانشجوی دکتری مهندسی برق، مخابرات سیستم دانشگاه علوم تحقیقات تهران.

۱. مقدمه و بیان مسئله

ظهور فناوری‌های هوش مصنوعی و کلان داده، تحولی بنیادین در عرصه‌های نظامی و امنیتی به‌وجود آورده است [۱]. رژیم غاصب صهیونیستی به‌عنوان یکی از پیشرفته‌ترین کشورها در حوزه فناوری‌های امنیتی؛ از سیستم‌های مبتنی بر هوش مصنوعی، شرکت‌های تحلیلی مانند: پالانتیر[1]بهره می‌برد. پالانتیر تکنولوژیز، شرکتی آمریکایی که در دِنور مستقراست؛ از سال‌های گذشته در زمینه‌ی تحلیل داده‌های پیچیده و هوشمند فعالیت می‌کند. که با همکاری نهادهای امنیتی و نظامی آمریکا، تجارب گسترده‌ای در طراحی الگوریتم‌های هدف‌گیری و پشتیبانی تصمیم نظامی کسب کرده است [۲]. در سال ۲۰۲۴، پالانتیر قراردادی راهبردی با وزارت دفاع اسراییل امضا کرد. تا فناوری‌های هوشمند خود را برای استفاده در عملیات نظامی، تحلیل داده‌های جاسوسی، و نظارت بر تهدیدها فراهم کند. این فناوری‌ها به حوزه عملیات میدان نبرد نفوذ کرد و به فرمانده‌ها امکان تصمیم‌گیری سریع،دقیق ومبتنی برداده‌های ترکیبی می‌دهند[۱-۳]. واحد لوتم:یکی از پیشرفته‌ترین نیروهای سایبری و الکترونیک جهان است. که نقش حیاتی برای امنیت سایبری اسراییل در جنگ مدرن دارد. این واحد؛ ترکیبی از هک، جنگ الکترونیک و عملیات اطلاعاتی است. که در جبهه‌های نامرئی جنگ علیه دشمنان اسراییل فعالیت می‌کند. با این حال، قدرت این واحد، نگرانی‌هایی درباره‌ی اخلاق و حقوق بشر ایجاد کرده است. واحد فناوری لوتم: به‌عنوان یکی از زیرمجموعه‌های کلیدی نیروی دفاعی اسراییل، با بهره‌گیری از فناوری‌های پالانتیر و زیرساخت‌های ابری گوگل و مایکروسافت، مسئول تحلیل داده‌های اطلاعاتی و اجرای عملیات سایبری است [۴-۵]. این واحد در تسهیل هدف‌گیری دقیق و واکنش‌های سریع در محیط‌های پرتنش منطقه‌ای، نقش حیاتی دارد.

1. PALANTIR

۲. پالانتیر؛ شرکت تحلیل‌گر داده‌های امنیتی و نظامی

پالانتیر تکنولوژیز[1]یک شرکت نرم‌افزاری آمریکایی تخصصی در زمینه تحلیل داده‌های کلان[2] است. که در سال ۲۰۰۳ توسط پیتر تیل[3] بنیانگذار پِی‌پال و چند تن دیگر تأسیس شد. نام این شرکت از "پالانتیر" در ارباب حلقه‌ها گرفته شده است؛کره‌های بلورینی که امکان دیدن رویدادهای دوردست را فراهم می‌کردند. پالانتیر، با توسعه سامانه‌های پیشرفته همچون Gotham و پلتفرم Palantir Artificial Intelligence Platform، امکان هم‌زمان‌سازی و تحلیل داده‌های متنوع از منابع مختلف را فراهم می‌کند [۶-۷]. این داده‌ها شامل اطلاعات ماهواره‌ای، داده‌های پهپادی،حرکات نیروهای زمینی،ارتباطات سیگنالی واطلاعات میدانی است. الگوریتم‌های یادگیری عمیق و مدل‌های هوش مصنوعی پالانتیر قادرهستند، تا اهداف بالقوه را خودکار کشف و اولویت‌بندی نمایند [۸-۹]. در زمینه‌ی هدف‌گیری، فناوری پالانتیر با بهره‌برداری از مدل‌های پیشرفته، فهرست‌های هدف را به سرعت تولید و تحویل نیروهای دفاعی اسراییل می‌دهد. به دلیل سرعت بسیار بالای پردازش و دقت الگوریتم‌ها،این فهرست‌ها، امکان واکنش سریع در عملیات‌های تهاجمی و تدافعی را می‌دهند. سیستم‌های هوش مصنوعی پالانتیر حتی به تولید هشدارهای لحظه‌ای درباره‌ی تحرکات تهدیدآمیز می‌پردازند. که موجب افزایش سطح هوشیاری عملیاتی می‌شود [۱] ,[۴].

پالانتیر همچنین سیستم هوش مصنوعی پیشرفته‌ای به‌نام TITAN[4]در حال توسعه دارد که با پوشش داده‌های فضایی، هوایی و زمینی و پیشرفت‌های یادگیری ماشین، انتظار می‌رود تحولی عظیم در مدیریت عملیات نظامی ایجاد کند [۱]. محصولات اصلی این شرکت، پالانتیر گوتهام[5] پالانتیر فاندری[6] پالانتیر آپولو[7]هستند. که در ادامه به پالانتیر گوتهام پرداخته شده است [۱۰].

1. Palantir Technologies
2. Big Data
3. Peter Thiel
4.Tactical Intelligence Targeting Access Node
5. Gotham
6. Foundry
۷. □□□□□□

۱-۲. پالانتیر گوتهام

پالانتیر گوتهام : یکی از قدرتمندترین پلتفرم‌های نرم‌افزاری در جهان برای تحلیل داده‌های امنیتی و نظامی است. نام گوتهام از شهر گوتهام در دنیای بتمن الهام گرفته شده‌است. که نمادی از یک محیط پر از تهدیدهای امنیتی است. این سیستم به سازمان‌های اطلاعاتی، نظامی و امنیتی کمک می‌کند تا داده‌های کلان را پردازش کنند، الگوهای پنهان را شناسایی نمایند و تصمیم‌گیری‌های استراتژیک را بهبود بخشند. گوتهام به صورت ویژه در اختیار نهادهای امنیتی اسراییل، سازمان سیا[1] اف.بی.آی[2] و پنتاگون قرار می‌گیرد [۱۱]. ویژگی‌های کلیدی پالانتیر گوتهام به‌ترتیب زیر می‌باشند:

۲-۱-۱. تحلیل گراف داده‌ها[3]

توانایی ترسیم روابط پیچیده بین افراد، سازمان‌ها، مکان‌ها و رویدادها (شناسایی شبکه‌های هدف با نمایش ارتباطات بین اعضا) و ردیابی جریان مالی هدف در ویژگی تحلیل گراف داده‌ها جای می‌گیرد.

۱-۲-۲. یکپارچه‌سازی چندمنبعی داده‌ها

یکپارچه سازی چندمنبعی داده‌ها، شامل ترکیب داده‌های مخابراتی، مالی، ماهواره‌ای، رسانه‌های اجتماعی و پایگاه‌های اطلاعاتی دولتی (ارتباط دادن یک تماس تلفنی مشکوک به یک تراکنش بانکی غیرعادی) و تطبیق تصاویر ماهواره‌ای با گزارش‌های میدانی هست.

۳-۱-۲. هوش مصنوعی و یادگیری ماشین[4]

تشخیص الگوهای رفتاری (شناسایی فعالیت‌های غیرعادی در یک منطقه)، پیش‌بینی تهدیدات بر اساس داده‌های تاریخی و تحلیل خودکار محتوای متنی (مانند ایمیل‌ها، پیام‌های رمزنگاری‌شده)، این دسته را شامل می‌شود.

---

1. CIA
2. FBI
3. Graph Analytics
1. Artificial Intelligence and Machine Learning

۴-۱-۲. نقشه‌برداری پویا[۱]

- نمایش داده‌ها روی نقشه‌های سه‌بعدی تعاملی (ردیابی حرکت وسایل نقلیه مشکوک در زمان واقعی).
- شبیه‌سازی عملیات نظامی قبل از اجرا.

۵-۱-۲. سیستم هشدار زودهنگام[۲]

شناسایی ناهنجاری‌هاᵌر جریان داده‌ها (مثال: هشدار دربارهی افزایش غیرعادی ارتباطات در یک منطقه نظامی) و تشخیص تلاش برای نفوذ سایبری، سیستم هشدار زودهنگام را شامل می‌شود.

۲-۲. کاربردهای گوتهام در اسرائیل

۱-۲-۲. امنیت داخلی (شین بت)[۴]

در ردیابی فعالیت‌های فلسطینی‌ها در کرانه باختری و نوار غزه، شناسایی اهداف از طریق تحلیل ارتباطات تلفنی و مالی و پیشگیری از حملات انتحاری با شناسایی الگوهای رفتاری مشکوک، به این قسمت کمک می‌کند [۱۲].

۲-۲-۲. نیروی دفاعی اسرائیل[۵]

هدف‌یابی دقیق در عملیات‌های هوایی (مثلاً در نوار غزه)، تحلیل اطلاعات میدان نبرد برای تصمیم‌گیری سریع و ردیابی موشک‌ها و تونل‌های حماس در نیروی دفاعی اسرائیل کمک می‌کند.

---

۲. Dynamic Geospatial Mapping

3. Early Warning System
4. Anomaly Detection
5. Shin Bet
1. IDF

۳-۲-۲. جنگ سایبری (واحد ۸۲۰۰[1])

شناسایی حمله‌های سایبری به زیرساخت‌های حیاتی اسرائیل، نظارت بر ارتباطات هدف (مانند نیروهای محور مقاومت: حماس، حزب‌الله، حشدالشعبی و ایران) و تحلیل کمپین‌های تبلیغاتی هدف در شبکه‌های اجتماعی، مواردی است؛که گوتهام در جنگ سایبری به اسرائیل کمک می‌کند [۱۳].

۴-۲-۲. مرزهای امنیتی

مدیریت داده‌های مرزی در گذرگاه‌هایی مانند: اریحا و رفح، تشخیص جعل مدارک با استفاده از هوش مصنوعی و پیش‌بینی تلاش‌های نفوذ از طریق مرزها از جمله خدماتی است که پالانتیر به اسرائیل ارائه می‌دهد.

۲-۳. کاربردهای نظامی و امنیتی پالانتیر در اسرائیل

پالانتیر در پروژه‌های امنیت ملی برای تحلیل داده‌های تروریستی، پیش‌بینی حملات احتمالی و ردیابی شبکه‌های حماس و حزب‌الله استفاده مشارکت فعال دارد. همچنین اسراییل از محصولات این شرکت در همکاری با سازمان‌های اسراییلی از جمله شین بت (سرویس امنیت داخلی)، موساد (سرویس اطلاعات خارجی) و نیروهای دفاعی اسرائیل[2] برای تحلیل اطلاعات امنیتی، هماهنگی عملیات نظامی و مدیریت بحران استفاده می‌کند. در کاربردهای مرزی نیز از جمله مدیریت داده‌های گذرگاه‌های مرزی، شناسایی الگوهای عبور غیرقانونی و تحلیل ویدیوهای نظارتی با هوش مصنوعی به‌کار گرفته می‌شود [۸], [۱۴].

۲-۴. فناوری‌های کلیدی پالانتیر

موتور تحلیل گراف[3] با توانایی نمایش روابط پیچیده بین افراد، مکان‌ها و رویدادها (مانند ترسیم شبکه‌های مدنظر با هزاران گره ارتباطی)، یادگیری ماشین پیشرفته با الگوریتم‌های پیش‌بینی‌کننده رفتار و سیستم‌های تشخیص الگو در داده‌های نامرتبط،

1. Unit 8200
2. IDF
3. Graph Analytics

پردازش زبان طبیعی[1] با تحلیل محتوای ارتباطات الکترونیکی و شناسایی کلمات کلیدی و مفاهیم پنهان، سیستم‌های جغرافیایی-فضایی با تلفیق داده‌های ماهواره‌ای با اطلاعات زمین و نقشه‌برداری سه‌بعدی از مناطق عملیاتی از جمله فناوری‌های مورد استفاده در شرکت پالانتیر است[۱۵].

۲-۵. همکاری‌های استراتژیک پالانتیر در اسرائیل

خطاهای تحلیلی از جمله احتمال شناسایی نادرست افراد[2] خطر تصمیم‌گیری‌های اشتباه بر اساس داده‌های ناقص و کاربردهای نظامی در کشتار غیرنظامیان و قتل عام مردم بی‌گناه غزه از جمله ایرادات محصولات این شرکت است که متاسفانه با آگاهی کامل در اختیار اسرائیل قرار می‌گیرد. در ادامه به برخی از کاربردهای پالانتیر در اسرائیل پرداخته شده است [۱۶].

۲-۵-۱. همکاری با ارتش اسرائیل (IDF)

- پروژه "سپر آهنین دیجیتال" برای دفاع سایبری
- سیستم مدیریت اطلاعات میدان نبرد.

۲-۵-۲. همکاری با صنایع دفاعی

- مشارکت با رافائل[3] در پروژه‌های امنیتی
- همکاری با صنایع هوای اسرائیل[4]

۲-۵-۳. مراکز تحقیقاتی

- تأسیس آزمایشگاه‌های مشترک در دانشگاه‌های تل‌آویو و تخنیون
- سرمایه‌گذاری در استارت‌آپ‌های امنیتی اسراییلی.

1. NLP
2. False Positives
3.RAFAEL
4. IAI

۲-۶. آینده پالانتیر در اسراییل

آینده پالانتیر گوتهام را می‌توان در ادغام با فناوری‌های Real-Time Intelligence (مانند پهپادها و ربات‌های شناسایی)، بهبود مدل‌های پیش‌بینی حملات هدف با هوش مصنوعی پیشرفته، گسترش همکاری با متحدان اسراییل (مانند آمریکا و امارات)، خودکارسازی بیشتر و ادغام با فناوری‌های جنگ پیش‌بینی کرد. متاسفانه این قدرت تحلیلی فوق‌العاده در اختیار رژیم غاصب قرار گرفته که هیچ محدودیتی برای گریز از اخلاق، حریم خصوصی و سوءاستفاده نمی‌شناسد [۱۷-۱۸].

۲-۶-۱. توسعه سیستم‌های خودمختار

- ادغام بیشتر با پهپادها و ربات‌های نظامی
- سیستم‌های شناسایی هدف خودکار

۲-۶-۲.جنگ سایبری

- توسعه ابزارهای دفاع و حمله سایبری،
- شناسایی تهدیدات سایبری در زمان واقعی.

۲-۶-۳. هوش مصنوعی پیشرفته

- مدل‌های پیش‌بینی کننده با دقت بالاتر،
- سیستم‌های تصمیم‌گیری مستقل.

۳. واحد فناوری لوتم: پلی تکنولوژیک میان هوش مصنوعی و عملیات نظامی

واحد لوتم (با نام رسمی "לוטם" - לוטם"ם، مخففLohamah Telelogit Meuhedet به‌معنای "جنگ اطلاعاتی تخصصی") زیرمجموعه‌ای از دسته‌ی ارتباطات و سایبر (C4I Corps) در نیروی دفاعی اسرائیل (IDF) است که مسئول جنگ الکترونیک، امنیت سایبری و عملیات ارتباطات پیشرفته می‌باشد. این واحد ترکیبی از تخصص‌های فناوری اطلاعات، هکینگ قانونی و جنگ الکترونیک است که نقش کلیدی در حفاظت از زیرساخت‌های دیجیتال اسرائیل و حمله به سیستم‌های دشمنان ایفا می‌کند. بر اساس اسناد فاش‌شده توسط ادوارد اسنودن، لوتم در رده‌بندی

جهانی جنگ سایبری در کنار واحد ۸۲۰۰ اسراییل و سازمان NSA آمریکا قرار می‌گیرد [۱۲]. لوتم؛ ادغام‌کننده الگوریتم‌های پالانتیر با زیرساخت‌های ابری گوگل و مایکروسافت است که پردازش بلادرنگ را برای اطلاعات گسترده و متنوع فراهم می‌آورد و اقدامات نظامی را دقیق‌تر و به‌موقع‌تر می‌کند [۱۳]. این واحد با بهره‌گیری از فناوری‌های مذکور، عملیات خود را در مناطق بحران‌خیز مانند غزه با دقت بالا هدایت می‌کند و سهم بزرگی در قابلیت‌های هدف‌گیری دقیق و مدیریت اطلاعات جنگی دارد. در واقع، لوتِم مسئول استفاده عملیاتی از تحلیل‌های پالانتیر و گردآوری اطلاعات حساس به‌منظور تصمیم‌گیری‌های تاکتیکی است[۱] , [۱۷].

۳-۱. ماموریت‌ها و وظایف اصلی لوتِم

۱-۱-۳. جنگ سایبری[۱]

دفاع از شبکه‌های نظامی و دولتی اسراییل در برابر حملات سایبری، حمله به سیستم‌های هدف(مانند حماس، حزب‌الله و ایران) برای مختل کردن ارتباطات یا جمع‌آوری اطلاعات و نفوذ به سرورها و شبکه‌های هدف برای شناسایی تهدیدهای پیش از وقوع، از جمله وظایف جنگ سایبری در واحد فناوری لوتم است.

۲-۱-۳. جنگ الکترونیک[۲]

از ماموریت‌های این بخش می‌توان به شنود و مختل کردن ارتباطات رادیویی و ماهواره‌ای هدف، جلوگیری از هدایت موشک‌ها و پهپادهای با استفاده از سیستم‌های اخلالگر[۳] و فریب سیستم‌های راداری هدف با ایجاد سیگنال‌های جعلی اشاره کرد.

۱. Cyber Warfare
۲. Electronic Warfare (EW)
3. Jammers

۳-۱-۳. عملیات اطلاعات سیگنالی[1]

استراق‌سمع ارتباطات دشمن (مکالمات رادیویی، ترافیک اینترنتی)، تحلیل داده‌های مخابراتی برای شناسایی اهداف نظامی و همکاری با واحد ۸۲۰۰ (واحد اطلاعات سایبری اسرائیل) در عملیات‌های مشترک در عملیات سیگنت می‌گنجد [۱۹].

۴-۱-۳.پشتیبانی از عملیات ویژه

تأمین ارتباطات امن برای نیروهای ویژه، هدایت پهپادهای جاسوسی و سیستم‌های نظارتی پیشرفته و پشتیبانی فنی در عملیات‌های ضدتروریستی از وظایف لوتم در پشتیبانی از عملیات ویژه است.

۳-۲. ساختار و سازماندهی لوتِم

وابسته به دسته C4I (ارتباطات، کامپیوتر، سایبر و اطلاعات) در IDF، همکاری نزدیک با واحد ۸۲۰۰ (هوش سایبری)، واحد ۸۱۰۰ (توسعه فناوری‌های اطلاعاتی)، شین بت[2] موساد در عملیات امنیتی و پرسنل آن متشکل از متخصصان سایبری، مهندسان الکترونیک و هکرهای آموزش‌دیده هستند [۲۰].

۳-۳. فناوری‌های مورد استفاده لوتِم

سیستم‌های جنگ الکترونیک پیشرفته (مانند سکوی Scorpius برای اخلال در ارتباطات دشمن)، ابزارهای نفوذ سایبری (شبیه به پلتفرم‌های پالانتیر و NSO Group)، شبکه‌های ارتباطی رمزنگاری‌شده برای عملیات محرمانه و هوش مصنوعی و یادگیری ماشین برای تحلیل ترافیک مخابراتی از جمله فناوری‌های مورد استفاده در لوتِم است [۲۱].

4. SIGINT
1. Shin Bet

۴. نقش گوگل و مایکروسافت در پشتیبانی فناورانه از لوتِم[۱]

گوگل و مایکروسافت نقشی اساسی در تامین زیرساخت‌های ابری و فناوری‌های هوش مصنوعی برای واحد لوتم دارند. گوگل با ارائه مدل‌های زبانی هوش مصنوعی نظیر Gemini و خدمات گسترده ابری و مایکروسافت با زیرساخت قدرتمند Azure، امکان تحلیل و پردازش سریع داده‌ها را در سامانه‌های حساس امنیتی و نظامی فراهم می‌کنند [۶], [۱۳].

۲. این بخش، برگرفته شده از گزارش «هوش مصنوعی در خدمت ماشین کشتار اسراییل» معاونت تحقیقات و جهاد خودکفائی س.ا.س می‌باشد.



شکل ۱. سربازهای نیروی دفاعی اسراییل که در کنفرانس مرکز تحقیق و توسعه مایکروسافت اسراییل شرکت کرده‌اند. این عکس از سوی واحد فناوری لوتم (تحت فرماندهی اداره خدمات کامپیوتری ارتش اسرائیل) در دوم آگوست ۲۰۲۳ به اشتراک گذاشته شد. این تصویر کنفرانسی را با حضور حدود ۱۵۰ سرباز اسرائیلی نشان می‌دهد که توسط بخش شاهار از واحد لوتم برگزار شده است. بخشی از نشانِ مایکروسافت در سمت چپ تصویر قابل **مشاهده است**. عنوان اسلاید نمایش داده شده "۱۰ فرمان دیجیتال" است. کوته‌نوشت RTFM در دومین فرمان یا دستورالعمل این اسلاید درج شده نوشته شده است که به Read The Fucking Manual اشاره دارد: کتابچه‌ی راهنمای لعنتی را بخوانید! (این عبارت نوعی اصطلاح غیررسمی و طنزآمیز است که به افراد توصیه می‌کند پیش از پرسیدن سوال یا درخواست کمک، دستورالعمل یا راهنما را به دقت مطالعه کنند).

همکاری این شرکت‌ها با لوتم و پالانتیر باعث ارتقاء چشم‌گیر قابلیت‌های عملیات نظامی شده است. درحالی‌که گزارش‌های رسانه‌های ایالات متحده عمدتاً بر روی فعالیت‌های واحد ۸۲۰۰ اسراییل متمرکز بوده است، شرکت‌های بزرگ فناوری مانند مایکروسافت و گوگل سال‌ها از واحد فناوری نظامی لوتِم در ارتش اسراییل پشتیبانی کرده‌اند.

فرمانده سابق واحد فناوری نظامی لوتِم، ژنرال اومرداگان[1] در مصاحبه‌ای با نشریه اسراییلی Tech12 در آوریل ۲۰۲۳ بیان کرد: «تلاش‌های سازمان تحت رهبری او برای ایجاد یک مدل زبانی بزرگ مشابه ChatGPT که برای انتخاب اهداف نظامی بر اساس دستورات زبان طبیعی طراحی شده باشد، هنوز در مراحل اولیه است». داگان هم‌چنین از این‌که واحد لوتِم تحت‌الشعاع واحد ۸۲۰۰ قرار گرفته، گلایه کرد. از واحد ۸۲۰۰ اغلب به‌عنوان نسخه کوچک‌تری از آژانس امنیت ملی ایالات متحده یاد می‌شود. داگان اظهار داشت: «دو نوع برندسازی مرسوم وجود دارد: اول اینکه شما به اندازه ارزش واقعی خود برند یا شناخته می‌شوید و نوع دوم این‌گونه است که شما بیشتر از ارزش واقعی خود برند یا شناخته می‌شوید». لوتِم نوع سومی را ابداع کرده است. این نوع از برندسازی زمانی اتفاق می‌افتد که شما کمتر از ارزش واقعی خود برند یا شناخته می‌شوید [۲۲].

حضور لوتم در دسته سوم، تا حد زیادی توضیح می‌دهد که چرا رابطه چندین‌ساله میان سربازان لوتِم با مایکروسافت و گوگل تا حد زیادی از توجه روزنامه‌نگاران دور مانده است. لوتِم به‌عنوان یک سازمان چتری[2] تشکیل شده است، تا واحد اصلی محاسبات نیروهای دفاعی اسراییل[3] که به‌نام مامرام[4] شناخته می‌شود، را در خود جای دهد. لوتِم همچنین به مرور زمان به پایگاه و مرکزی برای فعالیت سایر واحدها و بخش‌ها تبدیل شده است، از جمله: بخش «سیگما»[5] برای عملیاتی کردن ابزارهای تحلیل داده‌های تجاری شاخه توسعه نرم‌افزار «ماتزفن»[6] مدرسه علوم کامپیوتر

1. Omer Dagan
2. Umbrella Organization
3. The Original Computing Unit of The Israel Defense Forces
4. Mamram
5. Sigma
6. Matzpen

«بسماچ»[1] و بخش نیروی انسانی و لجستیک «شاحار».[2] (ژنرال اوزی موسکوویچ بین سال‌های ۲۰۱۱ تا ۲۰۱۶ اداره‌ی خدمات کامپیوتری[3] را به‌عنوان سازمان بالادستی لوتم فرماندهی می‌کرد. موسکوویچ توسط شرکت اوراکل[4] اجیر شد تا علیه قرارداد رایانش ابری پروژه نیمبوس، به ارزش تقریبی ۱,۲ میلیارد دلار، که بین گوگل، آمازون و دولت اسراییل منعقد شده بود، لابی‌گری کند [۲۳].

روزنامه جروزالم پست در ماه فوریه ۲۰۲۴ مصاحبه‌ای با اعضای لوتم انجام داد. در این گفتگو، یک سرهنگ ناشناس که با حرف «S» از او از او یاد شده، ادعا کرد: «پیشرفت‌های فناورانه در لوتم که نتیجه محاصره مداوم غزه توسط اسراییل است، به یک تغییر اساسی منجر شده است». وی گفت: «سرعت هدف‌گیری دیجیتال به‌حدی رسیده که ارتش اکنون می‌تواند اهداف جدید را در لحظه و به‌طور آنی سریع‌تر از انجام فرآیند حذف اهداف قدیمی، اضافه کند». (به‌عبارت دیگر، سرعت اضافه کردن اهداف جدید اکنون بیشتر از سرعت حذف یا نابودی اهداف قدیمی است). ماه بعد، لس رابرتز، اپیدمیولوژیست دانشگاه کلمبیا مقاله‌ای را در مجله تایم با عنوان «داده‌ها و تحقیقات علمی به وضوح نشان می‌دهند که بیش از ۳۰،۰۰۰ نفر در غزه کشته شده‌اند» منتشر کرد که در آن خاطرنشان شده بود که کشته‌شدگان «عمدتاً زنان و کودکان» بوده‌اند [۲۴].

ژنرال داگان پیش از پایان فرماندهی خود در لوتم در کنفرانس «فناوری اطلاعات در خدمت ارتش اسراییل»[5] در تاریخ ۱۸ ژوئیه ۲۰۲۲ شرکت کرد و سخنرانی را با عنوان «تحلیل‌ها و تصمیم‌گیری عملیاتی مبتنی بر اطلاعات» ارائه نمود. یائل گروسمن[6] (فرمانده وقت مامرام) و تالی کاسپی[7] (فرمانده وقت بخش شاحار) و همچنین تالیا گازیت[8] (فرمانده سابق مامرام) از جمله سایر

---

۱. Basmach School for Computer Science
1. The Shachar Personnel And Logistics Unit
2. The Computer Services Directorate
3. Oracle
4. IT for IDF conference
5. Yael Grossman
6. Tali Caspi
7. Talya Gazit

سخنرانان این کنفرانس بودند. یکی از مدیران اجرایی شرکت Ness Technologies وقت خود را صرف بررسی و صحبت درباره تاریخچه ۶۳ ساله مامرام نمود.

گوگل کلود با حمایت مالی سنگین خود از این رویداد امکان حضور و سخنرانی را برای یکی از مدیرانش به‌دست آورد. این مدیر (آساف لو[1]) دارای تجربه کاری قابل‌توجهی، هم در واحد ۸۲۰۰ و هم در شرکت اوراکل بوده است. آساف لِو (مدیر گروه مهندسان پشتیبانی از مشتری گوگل کلود) پیش از این حدود دو سال به‌عنوان سرپرست گروه زیرساخت‌های اپلیکیشن[2] در واحد ۸۲۰۰ خدمت کرده و پس از آن به مدت سیزده سال در شرکت اوراکل فعالیت کرده بود. همچنین تامیر هایمن فرمانده سابق آمان دیدگاه‌های خود را در مورد ماهیت تحول دیجیتال ارائه داد [۲۵].

در نوامبر سال ۲۰۲۲، بخش فرماندهی و کنترل[3] اداره خدمات کامپیوتریِ فرماندهی مرکزی ارتش اسراییل که مسئولیت مناطق کرانه باختری را بر عهده دارد، تصاویری از سربازان خود را که در اجلاس Google Israel Cloud در تاریخ نهم نوامبر ۲۰۲۲ شرکت کرده بودند، منتشر کرد و این حضور را به‌عنوان بخشی از روند مدرن‌سازی فرماندهی توصیف نمود. ترجمه انگلیسی یک پست عبری در یک حساب لینکدین اینگونه است: «ما در کنفرانس گوگل کلود بودیم!! چهارشنبه گذشته، نمایندگانی از بخش دیجیتال واحد (فناوری اطلاعات و ارتباطات) فرماندهی مرکزی در اجلاس گوگل کلود اسراییل شرکت کردند. این بخشی از تلاش‌های گسترده برای پیاده‌سازی سامانه‌های فنی جدید و ترویج تحول دیجیتال در فرماندهی مرکزی است.»

1. Asaf Lev
2. Unit 8200's application infrastructure team
۳. C4I

به‌معنای فرماندهی کنترل ارتباطات کامپیوتر و اطلاعات است.



شکل ۲. حضور سربازان نیروهای دفاعی اسرائیل در دفاتر گوگل کلود اسرائیل برای شرکت در اجلاس Google IL Cloud در تاریخ ۹ نوامبر ۲۰۲۲. – بوعاز مائوز – مدیر گوگل اسرائیل – سخنرانی اصلی آن رویداد بود.

چندین پست اخیر از حساب لینکدین متعلق به واحد C4I فرماندهی مرکزی، ساخت یک پایگاه داده امنیتی مشترک با پلیس اسرائیل را در آستانه ماه رمضان، که در نهم آوریل به پایان رسید تبلیغ کرده‌اند. سخنگوی ارتش اسرائیل، ایال کوهن[1] همچنین به نقش واحد C4I در ردیابی شاباحیم[2] اشاره کرده است. علاوه بر رابطه گوگل با بخش C4I در فرماندهی مرکزی ارتش اسرائیل، رئیس بخش عمومی و دفاعی گوگل در اسرائیل[3] شای مور[4] نیروی پلیس اسرائیل بسیار سودآورتر بوده است در ۲۹ فوریه اعلام کرد که گوگل در قالب یک پروژه با پلیس اسرائیل همکاری کرده است. برخلاف همکاری گوگل با پلیس، رابطه مایکروسافت با. مایکروسافت یک قرارداد سه ساله به ارزش تقریبی ۴,۲ میلیون دلار با پلیس اسرائیل منعقد کرده است که از ژانویه ۲۰۲۳ آغاز شده است. در کنفرانس «فناوری اطلاعات در خدمت ارتش اسرائیل» در سال ۲۰۲۳، لورا بوازیز[5] از مهندسان

1.Eyal Cohen
2.Shabahim
این واژه در عبری به فلسطینی‌هایی اشاره دارد که به‌طور غیرقانونی از کرانه باختری به اسرائیل وارد می‌شوند.
۳. The Company's Head of Public Sector & Defense in ISRAEL
4. Shay Mor
5. Laura Bouaziz

خدمات به مشتریان گوگل کلود اسرائیل که جایگزین آساف لِو شده بود سخنرانی کرد. موضوع سخنرانی او بیشتر با موضوع «چت.جی.پی.تی تهاجمی» فرمانده سابق[1] لوتِم، داگان، هم‌خوانی داشت و به بررسی استفاده‌های نظامی از هوش مصنوعی مولد گوگل پرداخت. بوازیز حتی تصویری از این سخنرانی را به‌عنوان عکس بالای صفحه در حساب لینکدین خود قرار داده است. پیش از پیوستن به گوگل در اوایل سال ۲۰۲۲، خانم بوازیز حدود چهار سال را صرف توسعه سامانه‌های یادگیری ماشین برای صنایع هوافضای اسرائیل کرده بود. به‌تازگی وبسایت The Intercept گزارشی منتشر کرده که نشان می‌دهد صنایع هوافضای اسرائیل بر اساس قراردادهای خود ملزم به خرید خدمات ابری از گوگل یا آمازون در قالب پروژه نیمبوس[2] هستند [۲۴], [۲۶-۲۷].

یکی از موارد دستور جلسه رویداد سال ۲۰۲۳ به این شکل ترجمه می‌شود: «عملیات مراکز محاسبات داخلی، ابرها و ... کار هیبریدی به‌عنوان بخشی از مناقصه نیمبوس و ارزیابی‌ها برای مناقصه

۱.Offensive Chatgpt -

این مفهوم به کاربردهای تهاجمی هوش مصنوعی مولد مانند ChatGPT در زمینه‌های نظامی و امنیتی اشاره دارد. در اینجا offensive تهاجمی به معنای استفاده از فناوری‌های هوش مصنوعی برای انجام عملیات‌های تهاجمی است که می‌تواند شامل اقداماتی مانند حملات سایبری جنگ اطلاعاتی تولید محتوا برای نفوذ روانی با تبلیغات و یا دیگر مواردی باشد که به‌طور فعال در عملیات نظامی و امنیتی برای حمله با مقابله با دشمن به‌کار می‌رود.

۲Project Nimbus–پروژه نیمبوس، یک پروژه مرتبط با رایانش ابری دولت ا سرائیل و نیروهای دفاعی آن ا ست. در آوریل ۲۰۲۱، وزارت امور مالی ا سرائیل اعلام کرد که موافقت نامه‌ای برای ارائه «راه‌حل ابری جامع برای دولت و سازمان دفاعی» به امضاء رسیده است. طبق این موافقت‌نامه شرکت‌ها مزرعه‌های ابری محلی ایجاد خواهند کرد که اطلاعات را در مرزهای ا سرائیل با رعایت د ستورالعمل‌های امنیتی دقیقی نگه می‌دارند. گرچه ماموریت خاص پروژه نیمبوس هنوز فاش ن شده ا ست، اما ابزارهای هوش مصنوعی سکوی ابری گوگل می‌توانند به نیروهای نظامی و خدمات امنیتی اسرائیل قابلیت‌هایی مانند تشخیص چهره، دسته‌بندی خودکار تصاویر، پیگیری اشیاء و تحلیل احساس را بدهند. ابزارهایی که پیشتر توسط سازمان مرز و مراقبت آمریکا برای نظارت مرزی استفاده شده‌اند. پروژه نیمبوس چهار فاز برنامه‌ریزی شده دارد، اول، خرید و ساخت زیرساخت ابری؛ دوم، تدوین سیاست دولتی برای انتقال؛ سوم، انتقال به زیرساخت ابری و چهارم، اجرا و بهینه‌سازی عملیات ابری. طبق قرارداد ۱.۲ میلیارد دلاری، شرکت‌های فناوری گوگل (Google Cloud Platform) و آمازون (Amazon Web Services) برای ارائه خدمات محا سبات ابری شامل هوش م صنوعی و یادگیری ما شین، به نهادهای دولتی ا سرائیل انتخاب شدند.

ابر ایمن – سِریوس» طبق گزارشی که گلوبس[1] رسانه خبری اسرائیلی – در سال ۲۰۲۱ منتشر کرد و شامل مصاحبه‌ای با فرمانده وقت لوتِم، داگان بود، سِریوس امن‌تر از نیمبوس است که توسط ارتش اسرائیل استفاده می‌شود.

بائل گروسمن، فرمانده سابق مامرام، در سال ۲۰۲۳ مجدداً برای سخنرانی در «کنفرانس فناوری اطلاعات در خدمت ارتش اسرائیل» دعوت شد، البته این بار در جایگاه جدید خود به عنوان فرمانده واحد لوتم. همتای هایمن در این زمینه می‌توانست بنی گانتز، وزیر دفاع سابق باشد. هشت سال پیش، گانتز جایزه‌ای را به آونر زیو[2] فرمانده وقت شاخه متسین لوتم، بابت توسعه ابزار ترکیب داده‌ها[3] به‌نام گوی کریستالی[4] اعطا کرد. گوی کریستالی برای پشتیبانی از عملیات تیغه ی حفاظتی[5] یا همان جنگ غزه در سال ۲۰۱۴ استفاده شده بود. سایر ابزارهای ترکیب داده‌ای که توسط بخش ماتزین توسعه یافته‌اند، از نظر حساسیت و محرمانه بودن آنقدر مهم هستند که نمی‌توان درباره آن‌ها صحبت کرد یا اطلاعات عمومی ارائه داد [۲۸].

1. Globes
2. Avner Ziv
3. Data Fusion Tool
4. Crystal Ball
5. Operation Protective Edge



شکل ۳- لورا بوازیز، مهندس خدمات مشتریان گوگل کلود اسرائیل، در حال سخنرانی درباره کاربردهای نظامی محصولات هوش مصنوعی مولد گوگل در کنفرانس «فناوری اطلاعات در خدمت ارتش اسرائیل» در تاریخ ۲۸ ژوئن ۲۰۲۳- وزیر دفاع سابق اسرائیل گانتز نیز از جمله سخنرانان این رویداد بوده است.

حدود یک ماه بعد، در دوم آگوست، حساب لینکدین واحد لوتِم تصویری از یک سالن پر از سربازان ارتش اسرائیل را منتشر کرد که در کنفرانسی در یکی از پردیسهای مایکروسافت در اسرائیل شرکت کرده بودند. این کنفرانس توسط واحد لجستیک شاحار در واحد لوتِم برگزار شده بود. عنوان اسلاید نمایش داده شده « ۱۰ فرمان دیجیتال» است. کوته نوشت RTFM در دومین فرمان یا دستورالعمل این اسلاید درج شده نوشته شده است که به Read The Fucking Manual اشاره دارد. کتابچه‌ی راهنمای لعنتی را بخوانید!

این رویداد سومین کنفرانس سالانه توسعه‌دهندگان لوتِم بود که حدود ۱۵۰ سرباز، افسر و مشاور از بخش‌های مختلف توسعه‌ی ارتش اسرائیل در آن شرکت داشتند. این کنفرانس شامل سخنرانی و

گفتگوهای حرفه‌ای در خصوص کوبرنیتس گوگل[1] ری اکت متا[2] دفاع سایبری[3] آزمایش[4] مدیریت دانش[5] و نوآوری بود. در توضیحات حساب لینکدین این واحد نوشته شده است: «پلتفرم دیجیتال ارتش به‌عنوان زیرساختی عمل می‌کند که بر اساس آن ده‌ها سامانه‌ی مختلف در ارتش اسرائیل ایجاد و پیاده‌سازی شده‌اند. این سامانه‌ها به‌صورت روزانه به نیروهای عادی و ذخیره ارتش خدمات می‌دهند. هم‌چنین این پلتفرم چهار ارائه‌دهنده‌ی خدمات ابری عمومی را به یک شبکه مشترک متصل می‌کند» [۲۹].

یکی از توسعه‌دهندگان وابسته به لوتم، ایدان فیشمن[6] خاطر نشان کرد که گوگل میزبان توسعه‌دهندگان در کنفرانس‌های سالانه پیشین به سرپرستی بخش شاحار لوتم، بوده است. یکی از توسعه‌دهندگان فول استک[7] لوتم، لیراز گانون[8] تجربه حضور خود را در رویداد هکاتون[9] که تقریباً

---

۱. [Google's] Kubernetes

2. [Meta's] React
3. Cyber Defense
۴. Testing

5. Knowledge Management
6. Idan Fishman
۷. Full stack

به کسی گفته می شود که هم در بخش Frontend و هم در بخش Backend توانایی تو سعه دا شته با شد. تو سعه‌دهندگان فول اســـتک قادرند کل چرخه توســـعه نرم افزار را مدیریت کنند. از طراحی رابط کاربری گرفته تا مدیریت پایگاه داده و پیاده‌سازی منطق کسب‌وکار.

8. Liraz Ganon
9. Hackathon

هکاتون رویدادی اســـت که در آن برنامه‌نویســـان رایانه و افراد دیگری که درگیر توســـعه نرم‌افزار هســـتند، از جمله طراحان گرافیکی، طراحان واســـط کاربری و مدیران پروژه گرد هم می‌آیند و در توســـعه پروژه‌های نرم‌افزاری و گاهی ســـخت‌افزاری با یکدیگر همکاری می‌کنند. هکاتون‌ها معمولاً بین یک روز تا یک هفته به طول می‌انجامند. برخی از هکاتون‌ها تنها برای اهداف اجتماعی و آموز شی هستند. هر چند که در اکثر موارد، هدف هکاتون‌ها ایجاد نرم‌افزارهای مفید و قابل استفاده است. هکاتون ها معمولاً بر روی هدف خا صی تمرکز دارند که می‌تواند شامل یک زبان برنامه‌نویسی مورد ا ستفاده، یک سیستم‌عامل، یک برنامه کاربردی، یک رابط برنامه‌نویسی نرم‌افزار، مو ضوع و گروه جمعیت شناختی برنامه‌نویسان با شد. در برخی موارد دیگر، محدودیتی بر نوع نرم‌افزاری که قرار ا ست ایجاد شود وجود ندارد. واژه «هکاتون» یک واژه مرکب ا ست که از تلفیق دو واژه «هک» و «ماراتون» حا صل شده ا ست. کلمه «هک» در این واژه به‌معنای «بازیگو شی»، «ماجراجویی»، برنامه‌نوی سی اکت شافی است و با کلمه هک که در امنیت رایانه استفاده می‌شود، متفاوت است. به‌نظر می‌رسد که این واژه هم توسط توسعه‌دهندگان اوپن بی‌اس‌دی و هم توسط تیم بازاریابی سان مایکرو سیستمز به شکل مستقل ایجاد شده با شد که هر دو اولین بار در سال

در اوایل آگوست ۲۰۲۳ در کمپ مایکروسافت در هرتزلیا برگزار شد، به اشتراک گذاشته است. او در این هکاتون از پلتفرم محاسبات ابری آژور مایکروسافت برای آزمایش چندین فناوری مرتبط با هوش مصنوعی استفاده کرده است، از جمله GPT 3.5، کتابخانه‌ی پایتون مدل‌های زبانی بزرگ LangChainو Azure AI Search.

با توجه به این‌که ایدان فیشمن در لینکدین خود به تسلطش در کار با AWS وAzure و Google Cloud اشاره کرده است، می‌توان فرض کرد که این سرویس‌ها بخشی از چهار «ابر عمومی» هستند که در زیر ساخت مشترک ارتش اسرائیل گنجانده شده‌اند (و احتمالاً شرکت اوراکل چهارمین ارائه‌دهنده خدمات ابری است که در این زیرساخت بکارگیری شده است، زیرا اوراکل نیز یکی از بزرگترین شرکت‌های ارائه‌دهنده خدمات ابری است.).

حدود دو هفته قبل از کنفرانس توسعه‌دهندگان مایکروسافت، در روز یکشنبه ۱۶ ژوئیه ۲۰۲۳، انجمن دانش‌آموختگان مامرام کنفرانسی را در دانشگاه بن گوریون در نقب با عنوان «هوش مصنوعی، هوش مصنوعی مولد و کارزارهای دیجیتالی آینده ارتش اسرائیل»[1]برگزار کرد. سخنرانان این رویداد شامل مدیر معماری راهکارهای انویدیا[2]در اسرائیل اوفیر زمیر[3]، دانشمند ارشد مرکز تحقیق و توسعه مایکروسافت در اسرائیل تومر سایمون[4] فرمانده لوتم، پائل گروسمن و مافوق

۱۹۹۹ مورد استفاده قرار گرفتند. اولین استفاده شناخته‌شده از این کلمه توسط اوپن بی‌اس‌دی، اشاره به رویدادی دارد که توسعه‌دهندگان اوپن بی‌اس‌دی در چهارم ژوئیه ۱۹۹۴ در شهر کلگری کانادا برای توسعه یک نرم‌افزار رمزنگاری گرد هم جمع شدند. این گردهمایی، به‌خاطر پرهیز کردن از مشکلات قانونی که از مقررات صدور نرم‌افزارهای رمزنگاری در ایالات متحده ناشی می‌شدند، صورت گرفت. در مورد شرکت سان، استفاده از این واژه اشاره به رویدادی در کنفرانس جاواوان از ۱۵ ژوئیه تا ۱۹ ژوئیه سال ۱۹۹۹ دارد. در این رویداد، جان گیج (John Gage) از شرکت‌کنندگان دعوت کرد که برنامه‌ای به زبان جاوا برای پالم ۵ بنویسند که با استفاده از درگاه مادون قرمز، با دیگر کاربران پالم ارتباط برقرار کرده و آن را در اینترنت به ثبت برسانند. این رویداد هکاتون لقب گرفت.

1. AI & GEN Al and the IDF's next digital campaign
2. Director for Solutions Architecture
3. Ofir Zamir
4. Tomer Simon

مستقیم او، رئیس اداره خدمات کامپیوتری اِران نیو[1] بودند. یک ماه پیش از کنفرانس، ژنرال نیو به روزنامه جروزالم پست گفته بود: «برآورد من این است که در آینده ای نزدیک، تمامی جنبه‌های جنگ تحت تأثیر اطلاعات تولید شده به‌وسیله‌ی هوش مصنوعی مولد قرار خواهد گرفت» [۲۴].



شکل ۴- حضور فرمانده‌ی واحد لوتم، ژنرال پائل گروسمن و فرمانده اداره خدمات کامپیوتری، ژنرال اران نیو، در کنفرانس ۱۶ ژوئیه ۲۰۲۳ در دانشگاه بن‌گوریون نقب در شهر بئرشیع با موضوع «هوش مصنوعی، هوش مصنوعی مولد و کارزار دیجیتال آینده‌ی ارتش اسرائیل»

همکاری گوگل با واحد لوتِم و اجزای مرتبط با C4I در فرماندهی‌های منطقه‌ای ارتش اسرائیل، به‌جای همکاری مستقیم با سازمان‌های حساس‌تری مانند واحد ۸۲۰۰، به‌طور کلی با ادعای دیرینه‌ی این شرکت همخوانی دارد. گوگل مدت‌ها تأکید کرده است که فعالیت‌هایش به‌سمت پروژه‌های بسیار حساس با طبقه‌بندی‌شده نظامی که به تسلیحات با خدمات اطلاعاتی مربوط می‌شود، سوق نمی‌یابد. (به‌عبارت دیگر، گوگل ترجیح می‌دهد با بخش‌هایی همکاری کند که به‌طور مستقیم با اطلاعات حساس و طبقه‌بندی‌شده یا توسعه سلاح‌ها سروکار ندارند، بلکه بیشتر در زمینه فناوری‌های

1. Eran Niv

رایانه‌ای و اطلاعاتی کلی عمل می‌کنند). نوریت کوهن اینگر[1] فرمانده سابق بخش «سیگما»[2] در واحد لوتم پس از بازنشستگی وارد بخش خصوصی شده است. او به‌طور همزمان هم به عنوان منتور در برنامه Google for Startups[3] فعالیت می‌کند و هم به‌عنوان قائم‌مقام رئیس شرکت اسرائیلی ActiveFence که در حوزه «اعتماد و ایمنی»[4] فعالیت دارد، مشغول به کار شده است. درحالی‌که به شغل بعدی او به عنوان یک مدیر اجرایی در حوزه فناوری اشاره ای نشد، اظهارات نوریت کوهن اینگر در مقاله‌ای که در ماه نوامبر در روزنامه لس‌آنجلس تایمز منتشر شده است، نقل شده‌اند. این مقاله درباره نقش شرکت‌های فناوری آمریکایی در بمباران مداوم غزه بوده و در آن به سخنان او در زمان رهبری بخش سیگما اشاره شده است [۱۹], [۲۳].

1. Nurit Cohen Inger

۲.این واحد مسئولیت تطبیق و استفاده از ابزارها و نرم‌افزارهای تحلیل داده‌های تجاری برای پاسخگویی به نیازهای عملیاتی نظامی را داشته است. به‌عبارت دیگر Sigma تلاش دارد تا از ابزارها و فناوری‌های تحلیل داده که در محیط‌های تجاری استفاده می‌شوند، برای کاربردهای نظامی به‌کار گرفته شود.

۳. یک برنامه جهانی است که توسط گوگل ایجاد شده تا از استارتاپ‌ها در سراسر جهان حمایت کند. هدف اصلی این برنامه کمک به بنیانگذاران استارتاپ‌ها برای رشد و توسعه کسب و کارهای خود از طریق دسترسی به منابع گوگل، مشاوره فنی برنامه‌های آموزشی و فرصت‌های شبکه سازی است. این برنامه تلاش می‌کند تا به استارتاپ‌ها ابزارهایی را که برای موفقیت نیاز دارند، ارائه دهد. از جمله منابع فناوری پشتیبانی فنی و آموزش‌هایی که بر اساس نیازهای استارتاپ‌ها طراحی شده‌اند.

4. Trust and Safety



شکل ۵- (تصویر سمت چپ) سرهنگ دوم نوریت کوهن اینگر در لباس نظامی به‌عنوان فرمانده بخش «سیگما» و (تصویر راست) کوهن اینگر به‌عنوان مربی در برنامه Google for Startups. تصویر سمت چپ توسط ارتش اسرائیل منتشر شده و تصویر سمت راست توسط کوهن اینگر از طریق لینکدین به اشتراک گذاشته شده است.

دیوید ایگناتیوس[1] ستون‌نویس شناخته‌شده واشنگتن پست، مقاله‌ای منتشر کرده است که در آن موفقیت اولیه اوکراین در مقابله با روسیه در فوریه ۲۰۲۲ به‌طور عمده به شرکت پالانتیر نسبت داده شده است. به واسطه‌ی این مقاله مهم، این گمانه‌زنی به‌طور گسترده مطرح شده است که این شرکت اکنون ممکن است در تهاجم اسرائیل به غزه نیز نقشی مشابه داشته باشد؛ به‌ویژه در زمینه پشتیبانی از سامانه‌های هدف‌یابی این گمانه‌زنی‌ها پس از برگزاری جلسه هیئت مدیره پالانتیر در اوایل ژانویه در تل‌آویو و سپس اعلام همکاری استراتژیک با وزارت دفاع اسرائیل تقویت شد.

با این حال، وب‌سایت خبری اسرائیلی Globes در اواخر ژانویه گزارش داد که گرچه پالانتیر با وزارت دفاع اسرائیل قراردادی را امضا کرده و از نظر لجستیکی و منابع انسانی به آن کمک می‌کند، اما واحد ۸۲۰۰ ارتش اسرائیل و سرویس امنیت داخلی، شین بت، از همکاری با این شرکت خودداری کرده‌اند. (این مطلب حاکی از این است که احتمالاً این نهادها یا از فناوری‌های دیگری استفاده می‌کنند یا توجیه خاصی برای عدم همکاری با پالانتیر دارند.) با این وجود، هفته‌نامه

1. David Ignatius

آمریکایی The Nation در ۱۲ آوریل ۲۰۲۴ گزارش داد که پالانتیر در حال تغذیه سامانه‌های هدف‌یابی[1] اسرائیل است. به‌نظر می‌رسد با توجه به این گزارش، اگرچه آمان (یگان ۸۲۰۰) تصمیم گرفته با پالانتیر همکاری نکند، اما این تصمیم در کلِ سیستم دفاعی اسرائیل اهمیت چندانی نداشته یا اثرگذار نبوده است. به‌عبارت دیگر، بر خلاف نظر آمان، سایر بخش‌های دفاعی اسرائیل از پالانتیر استقبال کرده و با این شرکت همکاری می‌کنند [۲۴], [۲۶].

خانم بوعزیز، نماینده گوگل کلود اسرائیل در کنفرانس« فناوری اطلاعات در خدمت ارتش اسرائیل» در سال ۲۰۲۳ در مصاحبه‌ای با وبگاه اسراییلی People and Computers در ۱۹ فوریه ۲۰۲۴ اعلام کرد که مدل زبانی بزرگ جمینای گوگل[2] از زبان عبری پشتیبانی می‌کند و به شرکت‌ها توصیه کرد که از طریق پلتفرم Vertex Al مدل جمینای را آزمایش و بررسی کنند. تقریباً دو سال پیش، مدیر عامل گوگل کلود، توماس کوریان[3]- که پیش‌تر یکی از مدیران اجرایی شرکت اوراکل بود- اعلام کرد که Vertex Al با Palantir تلفیق شده است. (این سخن کوریان به این مطلب اشاره دارد که Vertex AI به‌عنوان یک پلتفرم هوش مصنوعی که با هدف توسعه آموزش و بکارگیری مدل‌های یادگیری ماشین از سوی گوگل طراحی شده است، با فناوری‌ها و ابزارهای پالانتیر به هم متصل شده است). ژنرال گابی پورتنوی[4] فرمانده سابق واحد ۹۹۰۵ و مدیرکل اداره ملی سایبری اسراییل[6] در یکی از معدود مطالب‌اش در حساب لینکدین خود، جلسه هیئت مدیره

---

۱. Targeting Systems

2. Google's 'Gemini' large language model (LLM)

3. Thomas Kurian

4. Gaby Portnoy

۵.این واحد که زیر نظر اطلاعات ارتش اسرائیل اداره می شود، مسئول جمع‌آوری اطلاعات بصری است. این اطلاعات شامل داده‌های جغرافیایی می‌شود که از ماهواره‌ها و هواپیماها به‌دست می‌آید. نقشه برداری و تفسیر اطلاعات جمع‌آوری شده برای نیروهای نظامی و تصمیم‌گیران از جمله سایر ماموریت‌های این واحد محسوب می‌شود. بنابر گزارش روزنامه اسرائیلی جروزالم پست، ۵۸ درصد از کارکنان این واحد را زنان تشکیل می‌دهند.

٦The Israel National Cyber Directorate

پالانتیر در تل‌آویو را منتشر کرده است. (این مطلب به‌نوعی ارتباط نزدیک بین پالانتیر و نخبگان امنیتی اسرائیل از جمله افرادی مثل گابی پورتنوی را نشان می‌دهد) [۲۸].

حدود ۵۰ نفر از کارکنان گوگل در آوریل ۲۰۲۴ به‌علت اعتراض به حمایت گوگل از ارتش اسرائیل در جریان نسل‌کشی مداوم در غزه اخراج شدند. روز سه‌شنبه، ده‌ها نفر از این کارکنان، شکایتی را از طریق هیئت ملی روابط کار[1] ثبت کرده و مدعی شدند که حق فعالیت جمعی محافظت شده[2] آن‌ها نقض شده است. این درحالی است که گزارش‌ها حاکی از آن است که یوسی ماتیاس[3] بنیان‌گذار مرکز تحقیق و توسعه گوگل در اسرائیل به سمت ریاست کل تحقیقات گوگل ارتقاء یافته است.

۵. ملاحظات اخلاقی و حقوقی

به‌رغم مزایای فراوان فناوری‌های هوشمند، کاربرد آن‌ها در تصمیمات نظامی، از جمله هدف‌گیری و حملات هوایی، بحث‌های جدی اخلاقی و حقوق بشری را به‌خصوص درخصوص تلفات غیرنظامیان و از همه مهم‌تر قرار گرفتن این فناوری ها در دست حیوان‌های انسان‌نما از جنس رژیم غاصب صهیونی، برانگیخته است [۷], [۱۸-۱۹]. نگرانی‌ها درباره شفافیت عملکرد الگوریتم‌های هدف‌گیری، استقلال تصمیم نهایی اپراتورهای انسانی، و مسئولیت قراردادن فناوری در چارچوب قوانین بین‌المللی در صورت اهمیت!، از جمله مسائل مهمی هستند که نیازمند نظارت و پاسخگویی مستمرند [۸], [۲۰].

1. National Labor Relations Board
2. Protected Concerted Activity
3. Yossi Matias

۶. نتیجه‌گیری

پالانتیر به‌عنوان یکی از پیشرفته‌ترین پلتفرم‌های تحلیل داده در جهان، نقش حیاتی در معماری امنیتی اسرائیل ایفا می‌کند. با قابلیت‌های منحصربه‌فرد در پردازش داده‌های کلان و شناسایی الگوهای پیچیده، این سیستم به ابزاری استراتژیک برای سازمان‌های امنیتی و نظامی تبدیل شده است. توسعه آینده پالانتیر در اسرائیل احتمالاً بر افزایش سطح خودمختاری سیستم‌ها، ادغام عمیق‌تر با فناوری‌های جنگ سایبری و بهبود قابلیت‌های پیش‌بینی‌کننده متمرکز خواهد بود. هم چنین واحد لوتم، به‌عنوان الگوی جنگ سایبری مدرن، نمونه‌ای بی‌نظیر از ادغام عمیق فناوری‌های دیجیتال و عملیات نظامی است. با ترکیب هوش مصنوعی، جنگ الکترونیک و عملیات اطلاعاتی، این واحد مرزهای جنگ مدرن را بازتعریف می‌کند و هنگامی‌که غول‌های فناوری هم از هیچ کمکی به این رژیم کودک‌کش دریغ نمی‌کنند، اینجا هست که فناوری روی خطرناک خود را نشان می‌دهد. قدرت این سیستم‌ها نگرانی‌های جدی درباره تعادل بین امنیت و آزادی‌های مدنی ایجاد کرده است که نیازمند تنظیم چارچوب‌های اخلاقی و حقوقی دقیق است.

منابع:

1. Truthout, "Organizers Are Demanding Palantir Drop Contracts With ICE and Israeli Military," Aug. 2025.
2. Business & Human Rights Resource Centre, "Palantir allegedly enables Israel's AI targeting in Gaza," Apr. 2024.
3. SNN.ir, "Israel’s Lotem Unit & Military AI," Apr. 2025.
4. Asriran, "Google and Microsoft support Israeli military AI," May 2025.
5. Khatebazar.ir, "Technologies in Israeli operations," ۲۰۲۵.
6. Economic Times, "Palantir's AI is helping pick targets in war zones, "Jul. 2025.
7. Palantir Blog, "Ethical AI in Defense Decision Support Systems, "Nov. 2024.
8. Khabarfoori, "How technology giants applied AI in warfare," Feb. 2024.
9. Gerdab.ir, "Artificial Intelligence Palantir proposes military strategies," Apr. 2023.
10. Ahrominvest, "Palantir Technologies: Creator of data-driven future, "Aug. 2025.
11. Truthout, "Palantir’s AI platform and Israeli military," Aug. 2025.
12. Business & Human Rights Resource Centre, "Palantir supplying Israel with AI tools," Jan. 2024.
13. CNBC, "Palantir lands $10 billion Army software and data contract, "Aug. 2025.
14. Al Jazeera, "UN report lists companies complicit in Israel's ‘genocide’," Jul. 2025.
15. Amnesty International, "Israel/OPT: States must act now to halt Israel’s military takeover," Aug. 2025.
16. IEMed, "The Israeli Military's Use of AI in Gaza," Mar. 2025.
17. "PALANTIR and National Security", Data Analysis Review, 2023.
18. Clarke, R. A. "Cyber War: The Next Threat to National Security". HarperCollins, 2019.
19. Rid, T. Active Measures:" The Secret History of Disinformation and Political Warfare". Farrar, Straus and Giroux, 2020.

20. IDF Technical Reports. "Quantum-Resistant Cryptography in Military Systems". C4I Directorate, 2022.
21. Journal of Cybersecurity. "AI-Powered Cyber Operations: The Case of Unit Lotem". Oxford Academic, 2023.
22. "AI in Military Applications", Israel Defense Journal, 2023.
23. "LAVENDER": The Next Generation Surveillance System", TechSecurity Magazine, 2022.
24. "PALANTIR and National Security", Data Analysis Review, 2023.
25. Clarke, R. A. "Cyber War: The Next Threat to National Security". HarperCollins, 2019.
26. Rid, T. "Active Measures: The Secret History of Disinformation and Political Warfare". Farrar, Straus and Giroux, 2020.
27. IDF Technical Reports "Quantum-Resistant Cryptography in Military Systems". C4I Directorate, 2022.
28. Journal of Cybersecurity "AI-Powered Cyber Operations: The Case of Unit Lotem*. Oxford Academic, 2023.
29. "AI in Military Applications", Israel Defense Journal, 2023.