بسم‌الله‌الرحمن‌الرحیم

والحمدلله القاصم الجبارین

تبدیل تهدیدها به فرصت‌ها یکی از اهداف اصلی مقاومت است. فهمیدن این فرصتی که در دل تهدیدها نهفته است، نیاز به مطالعاتی علمی، روش‌مند و در عین‌حال هدفمند و با دغدغه دارد. مطالعاتی ساختاریافته که به دنبال رسیدن به هدفی مشخص در میدان باشد، از پرداختن بیش از اندازه به کلیات و تحلیل‌های بدون مستندات دقیق اجتناب کند، محدودیت‌های میدانی را بشناسد و از اطناب آکادمیک اجتناب کند. اندیشکده قرار تلاش دارد این نیاز حیاتی جبهه مقاومت را برطرف سازد و به محلی برای همگرایی مطالعات ساختاریافته و هدفمند در زمینه مقاومت و استعمار در منطقه غرب آسیا تبدیل شود.

بررسی نقش فناوری‌های جاسوسی در امنیت رژیم صهیونیستی

تحلیل پارادیم‌محور از صنعت جاسوس‌افزار اسرائیل

فهرست مطالب

نکات مهم:

- برآورد شده که سود سالانه صنعت فناوری جاسوسی اسرائیل در سال حداقل ۳ میلیارد دلار است.
- بیش از ۷۰ کشور از فناوری‌های اسرائیلی استفاده کرده‌اند.
- جاسوس‌افزار پگاسوس از ۵۰ هزار تلفن همراه جاسوسی کرده است.
- چهار شرکت اسرائیلی در لیست سیاه تجاری آمریکا و کشورهای اروپایی قرار دارند (NSO, Candiru, Cytrox, Intellexa)
- با این‌حال کشورهای غربی مشتری محصولات مشابه اسرائیلی هستند (به‌طور مثال آمریکا با Verint و Cellebrite قراردادهای متعدد دارد و پلیس بریتانیا مشتری اصلی Briefcam است).
- عمده مشتریان شرکت Candiru کشورهای خلیج فارس بودند و Corsight AI نیز بازار آمریکای لاتین را هدف قرار داده است.
- صنعت جاسوس‌افزار اسرائیل نشان‌دهنده تغییر پارادیم در سیاست‌های کلان رژیم صهیونیستی است. اسرائیل با اتکا به توسعه فناوری‌های پیشرفته و عرضه آنها به دولت‌ها و نهادهای امنیتی در جهان، خود را به شریکی غیرقابل حذف برای دولت‌های غربی تبدیل کرده است.
- صنعت جاسوس‌افزار رژیم صهیونیستی، تنها یک واکنش منفعلانه به تهدیدات امنیتی نیست، بلکه یک استراتژی فعال برای تثبیت قدرت رژیم است.

.

مقدمه

رژیم صهیونیستی امروزه به‌عنوان یکی از اصلی‌ترین تولیدکنندگان و صادرکنندگان فناوری جاسوسی در جهان شناخته می‌شود. این صنعت، که عمدتاً توسط سربازان سابق یگان ۸۲۰۰ ارتش اسرائیل راه‌اندازی شده، به یک صنعت چند میلیارد دلاری تبدیل شده و شرکت‌هایی مانند NSO Group، Cellebrite، Cognyte، Candiru و Corsight AI ، ابزارهای پیشرفته‌ای تولید کرده‌اند که قادر به نفوذ به تلفن‌های هوشمند، شنود ارتباطات، تشخیص چهره، ردیابی مکان و استخراج داده‌های حذف‌شده هستند.

این فناوری‌ها در ابتدا بر روی مردم فلسطین آزمایش شده و سپس به دولت‌ها و نهادهای امنیتی غربی - از جمله آمریکا، انگلیس، فرانسه و کانادا- فروخته شده‌اند. فروش این ابزارها نه تنها منبع درآمد چشمگیری برای اسرائیل است، بلکه نقش کلیدی در تقویت سیستم‌های نظارتی جهانی و نقض گسترده حقوق بشر ایفا می‌کند.

صادرات فناوری‌های جاسوسی روی دیگر اشغالگری و نسل‌کشی رژیم صهیونیستی است. در این گزارش اندیشکده قرار تلاش می‌کند تمام اطلاعات موجود درباره این صنعت جاسوس‌افزار را به شکل موردی بررسی کند و تحلیلی پارادیمی و شبکه‌محور از صنعت جاسوس‌افزار ارائه کند.

این پژوهش به بررسی نظام‌مند صنعت جاسوس‌افزارهای رژیم صهیونیستی می‌پردازد و آن را نه به‌عنوان یک پدیده فناورانه بی‌روح، بلکه به‌عنوان یک شبکه سیاسی-نظامی-اقتصادی می‌نگرد که در آن فناوری به ابزاری برای تداوم اشغال، نظارت گسترده و صادرات قدرت تبدیل شده است.

فناوری جاسوسی که توسط جاسوسان سابق اسرائیلی ساخته می‌شود، امروزه به یک صنعت مهم تبدیل شده است که مشتریان اصلی آن دولت‌ها و نهادهای نظامی و انتظامی کشورهای غربی هستند.

فناوری جاسوسی کاربردهای مختلف و ظرفیت‌های مختلفی دارد. از نرم‌افزارهای تشخیص چهره و صدا گرفته تا فناوری شنود و نفوذ، ابزارهای ردیابی مکان فرد و روش‌هایی برای استخراج داده از تلفن‌های همراه و سایر دستگاه ها. این فناوری توسط برنامه‌نویسانی ایجاد شده که برنامه‌هایشان را بر روی مردم فلسطین آزمایش کردند و از این طریق سلطه و برقراری نظام آپارتاید علیه مردم بی‌گناه فلسطین را امکان‌پذیر کردند. تاکنون تنها تعداد اندکی از رسوایی‌های افشاشده از سوی این جاسوس‌افزارهای اسرائیلی در رسانه‌های عمومی مطرح شده‌اند که در این گزارش تلاش می‌کنیم همه این موارد را جمع‌آوری و بررسی کنیم و اهمیت مسئله را نشان دهیم.

مبانی نظری

مبانی نظری این پژوهش بر سه محور استوار است. نخست، نظریه نظام نظارتی میشل فوکو[1] که در آن قدرت نه از طریق سرکوب آشکار، بلکه از طریق نظارت مستمر و محاسبه‌پذیر کردن افراد تحقق می‌یابد. دوم، مفهوم جامعه کنترل از ژیل دولوز که پس از عصر «نهادهای بسته» مانند زندان و مدرسه، وارد عصر «نهادهای باز» شده‌ایم که در آن نظارت به صورت پیوسته، دیجیتال و شبکه‌ای انجام می‌شود[2].

[1] Foucault, M. (1977). Discipline and Punish: The Birth of the Prison. Pantheon Books.
[2] Deleuze, G. (1992). Postscript on the Societies of Control. October, 59, 3–7.

سوم، مفهوم فناوری به‌عنوان ابزار سیاسی که در آن ابزارهای فنی، بی‌طرف نیستند، بلکه حامل ارزش‌ها، اهداف و ساختارهای قدرت جامعه‌ای هستند که در آن ساخته می‌شوند. برطبق این چارچوب نظری در این پژوهش صنعت جاسوس‌افزار اسرائیل را نه یک صنعت فنی، بلکه یک ابزار ژئوپلیتیک برای تثبیت قدرت دیده می‌شود.

روش گردآوری

روش تحقیق مورد استفاده، ترکیبی از تحلیل محتوای کیفی، بررسی اسناد آشکار (مانند گزارش‌های رسانه‌های معتبر، دادگاه‌ها، و منابع دولتی) و تحلیل شبکه‌ای از روابط بین شرکت‌های فناوری، نهادهای نظامی اسرائیلی (به ویژه یگان ۸۲۰۰) و مشتریان خارجی است. داده‌های تحقیق از منابع متنوعی شامل گزارش‌های عفو بین‌الملل و رسانه‌هایی چون هاآرتص و گاردین و همینطور نهادهای داخلی رژیم صهیونیستی و همچنین وبسایت‌های رسمی شرکت‌ها و پایگاه‌های استارتاپی مانند Startup Nation Central و Crunchbase جمع‌آوری شده است. این روش ترکیبی امکان تحلیل همزمان ساختارهای مادی (شرکت‌ها، محصولات، قراردادها) و ساختارهای ایدئولوژیک (گفتمان‌های مشروعیت‌بخش) را فراهم می‌کند.

یافته مدنظر شناسایی شرکت‌های مستقر در رژیم صهیونیستی یا ایجاد شده توسط اتباع این رژیم بود که به‌طور مشخص در حوزه جاسوس‌افزار و فعالیت‌های نظارتی، شنود و کنترل فعالیت می‌کنند.

یافته‌ها:

به‌طور کلی یافته‌ها را به دو بخش تقسیم کردیم، شرکت‌های تحریم‌شده توسط دولت‌های غربی و شرکت‌هایی که به شکل قانونی برای دولت‌ها و نهادهای امنیتی فعالیت می‌کنند.

تحریم‌شده‌ها

پگاسوس

معروف‌ترین این جاسوس‌افزارها پگاسوس بود، محصول شرکت NSO Group. شرکتی که توسط سربازان سابق ۸۲۰۰ با نام‌های شالو هولیو (Shalev Hulio) و عمری لاوی (Omri Lavie) تاسیس شد و در سال ۲۰۱۹ دادگاه کالیفرنیا آن را به نقض قوانین آمریکا محکوم کرد و اعلام کرد هدف این شرکت فروش پگاسوس به دولتها جهت جاسوسی از حساب‌های واتساپ افراد بوده است[۳].

جاسوس‌افزار پگاسوس قادر بود به شیوه «بدون کلیک» بر روی تلفن همراه قربانی اجرا شود؛ یعنی بدون این‌که قربانی اساساً متوجه شود. دولت‌های غربی از این ابزار برای جاسوسی از فعالان حقوق بشر و خبرنگاران[۴] استفاده می‌کردند و احتمال بسیار زیاد از آن توسط نیروهای سعودی، علیه خبرنگار روزنامه واشنگتن پست، جمال خاشقچی، پیش از ترور استفاده شده بود. شرکت متا مالک واتساپ از این شرکت صهیونیستی شکایت کرد و در نهایت دادگاه آن را به پرداخت ۱۶۷ میلیون دلار خسارت[۵] به متا محکوم کرد. در زمان بایدن این شرکت جز لیست سیاه تجارت در ایالات متحده قرار گرفت و مانع از فعالیت

[3] https://www.nbn.org.il/nbnlsp/wp-content/uploads/2020/09/parents-informational-pamphlet.pdf

[4] https://therecord.media/apple-warns-armenians-state-sponsored-hacking-attempts-azerbaijan

[5] https://www.amnesty.org/en/latest/news/2025/05/ruling-against-nso-group-in-whatsapp-case-a-momentous-win/

آن در آمریکا شـد. اما وزارت امور خارجه اسـرائیل برخلاف قاعده خود و این واقعیت که دولت اسـرائیل به این جاسـوس‌افزارها مجوز فعالیت داده بود، اعلام کرد آمریکا در این زمینه هیچ اقدامی علیه اسرائیل انجام نخواهد داد[۶].

کاندیرو

دیگر جاسوس‌افزار معروف اسـرائیلی کاندیرو Candiru نام دارد. ابزار هک این شـرکت به اندازه پگاسـوس در رسـانه‌ها سـروصدا نکرد. این شـرکت نیز توسـط سـربازان سـابق ۸۲۰۰ سـاخته شـد[۷]. بنیان‌گذاران این شـرکت Eran Shorer, Yaakov Weizman هسـتند و افراد اصـلی این شـرکت Isaac Zack (Chairman), Eitan Achlow (CEO) بودند. جاسـوس‌افزارهای این شـرکت نیز مشغول به جاسوسی از فعالان حقوق بشر[۸]، خبرنگاران، اساتید دانشگاه، کارکنان سفارتخانه‌ها و فعالان سیاسی بودند[۹].

شرکت‌های تال دیلیان

در سـال ۲۰۲۳ دولت بایدن دو شـرکت جاسـوس‌افزاری دیگر اسـرائیل را هم در لیسـت سـیاه تجارت قرار داد و بار دیگر هیچ اقدامی علیه دولت اسـرائیل نکرد. این دو شـرکت Cytrox و Intellexa بودند که توسـط تال دیلیان (Tal Dilian) تاسـیس شـده بودند؛ دیلیان حدود ۲۴ سـال در ارتش اسـرائیل مشـغول بود و به فرماندهی ۸۲۰۰ منصـوب شـده بود[۱۰]. در سـال ۲۰۱۹ دیلیان که در قبرس زندگی می‌کرد با خبرنگار نشـریه فوربز دیدار کرد؛ در طی این دیدار دیلیان به این خبرنگار نشـان داد که چطور نرم‌افزارهای او می‌تواند از راه دور تلفن همراه را در طی چندثانیه هک کند[۱۱].

در بین کشـورهای اروپا قبرس و بارسـلونا تبدیل به هابی برای سـربازان سـابق ۸۲۰۰ شـده اسـت تا شـرکت‌های جاسـوس‌افزاری بسازند.

پاراگون پرحاشیه

دیگر شرکت جاسوسی اسرائیلی با نام Paragon Solutions در سال اخیر مطرح شد[۱۲]. نرم‌افزار این شرکت قادر بود بی‌سروصدا به واتسـاپ، سـیگنال، مسـنجر و جیمیل رخنه می‌کرد و داده‌ها را بیرون می‌کشـید؛ این فرایند بدون هیچ تعاملی از سـوی کاربر رخ می‌داد. دادگاه ایتالیا شـکوائیه‌ای علیه این شـرکت اسـرائیلی به پا کرد و از آن به خاطر هک شـدن تلفن همراه خبرنگار ایتالیایی توسط دولت ایتالیا شکایت کرد. هیچ اقدام قضایی دیگری علیه این جاسوس‌افزار ثبت نشده است.

این شرکت توسط فرماندهان سابق یگان ۸۲۰۰ یعنی Ehud Schneorson, Idan Nurick, Igor Bogudlov تاسیس شد و ایهود باراک (نخست‌وزیر سابق اسرائیل) نیز مشاور است.

---

[6] https://archive.ph/kcEwA

[7] https://www.haaretz.com/middle-east-news/.premium-top-secret-israeli-cyberattack-firm-revealed-1.6805950

[8] https://www.hrw.org/news/2022/01/26/human-rights-watch-among-pegasus-spyware-targets

[9] https://www.reuters.com/world/india/indian-journalist-targeted-with-nso-spyware-anti-corruption-group-says-2023-11-07/

[10] https://archive.ph/s8yKA

[11] https://www.forbes.com/sites/thomasbrewster/2019/08/05/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van/

اما این شـرکتها تنها بخش اندکی از صـنعت جاسـوس‌افزاری اسـرائیلی را شـامل می‌شـوند. این شـرکتها تنها مواردی بودند که تنها هنگامی که فعالیت‌های مجرمانه آنها لو رفت، افشا شدند.

[12] https://apnews.com/article/spyware-italy-paragon-meloni-pegasus-f36dd32106f44398ee24001317ccf2bb

شرکت‌های قانونی

جاسوسی به شکل قانونی

شاید رازآمیزترین شرکت‌ها در صنعت جاسوسی اسرائیل، شرکت‌هایی هستند که با سرویس‌های امنیتی غربی قرارداد دارند و تجهیزات دیجیتال آنها را شنود می‌کنند. از آنجا که نهادهای امنیتی و قانونی کشورهای غربی مشتریان اصلی این شرکتها هستند، آنها ادعا دارند که محصولاتشان با ابزارهای NSO و Candiru و ... که متمرکز بر سرویس‌های هک غیرقانونی است، متفاوت است. با این‌حال در بسیاری از موارد نرم‌افزار آنها اگر نگوییم عینا با جاسوس‌افزارهای بدنام یکی است حداقل مشابهت بسیار زیادی دارد. البته حیطه کامل فعالیت‌های آن شناخته‌شده نیست.

سلبرایت

در این دسته، شرکت سلبرایت/ Cellebrite پیشگام است که مدیریت آن به عهده سرباز سابق ارتش اسرائیل Yossi Carmil است و چندین عضو سابق ۸۲۰۰ در آن حضور دارند[۱۳]. محصول اصلی این شرکت دستگاه استخراج جرم‌شناسی دیجیتال عمومی نام دارد که می‌تواند داده‌های مختلفی چون مخاطبان، موقعیت‌های مکانی، پیام‌های حذف‌شده و تماس‌ها را از طیف وسیعی از دستگاه‌ها از جمله تلفن‌های هوشمند، پدها، سیم‌کارت‌ها و دستگاه‌های GPS بیرون بکشد. در ایالات متحده شرکت سلبرایت قراردادی به ارزش ۳۰ میلیون دلار با ICE (اداره ضدمهاجرت) منعقد کرده است و ۱.۶ میلیون دلار نیز با اداره حفاظت از مرزها قرارداد بسته است. هدف از این قراردادها بیرون کشیدن اطلاعات از دستگاه‌های هوشمند ضبط‌شده در مناطق مرزی است.

این شرکت اسرائیلی همچنین با FBI همکاری کرد تا تلفن همراه توماس کوک (فردی که اقدام به ترور دونالد ترامپ کرد) را رمزگشایی کند. شرکت سلبرایت همچنین به دنبال نفوذ بیشتر در ساختار امنیتی و نظارتی آمریکاست. سال گذشته سلبرایت اعلام کرد که یک موسسه حقوقی متخصص در حوزه لابی‌گری را استخدام کرده است و یک شاخه کسب‌وکار خود را جهت دریافت قراردادهای بیشتر دولتی از سوی آمریکا اختصاص داده است[۱۴].

در سال ۲۰۲۴ این شرکت توانست مبلغ ۱۸ میلیون دلار از قراردادهای با دولت فدرال آمریکا دریافت کند. در دسامبر ۲۰۲۳ در تبلیغی اعلام کرد که توانسته قراردادی به ارزش یک میلیون دلار با «یکی از بزرگترین دپارتمان‌های پلیس» در آمریکا امضا کند[۱۵]. طبق اسناد اداره پلیس شهر نیویورک سالهاست با این شرکت اسرائیلی برای دریافت تجهیزات جاسوسی همکاری دارد[۱۶].

مهم‌تر از اینها تحقیقات نشان می‌دهد که شرکت سلبرایت قراردادهای فعال زیادی با آژانس‌های فدرال آمریکا منعقد کرده است[۱۷]؛ از نیروی دریای گرفته تا اداره مبارزه با مواد مخدر، گارد ساحلی و ... تعدادی از سفارتخانه‌های آمریکا نیز با این شرکت

---

[13] https://www.linkedin.com/search/results/people/?currentCompany=%5B%22100045%22%5D&keywords=unit%208200%20cellebrite&origin=FACETED_SEARCH&sid=lHR

[14] https://www.dropsitenews.com/p/israel-digital-intelligence-cellebrite-gaza

[15] https://cellebrite.com/en/one-of-the-largest-police-departments-in-the-u-s-doubles-down-with-cellebrite-digital-forensic-technology/

[16] https://onezero.medium.com/exclusive-inside-new-yorks-partnership-with-israeli-iphone-cracking-company-cellebrite-12a2252c3ebf

[17] https://www.highergov.com/contract/H9225725P0004/

قرارداد دارند؛ از جمله سفارت آمریکا در لیما (پرو)، بوگوتا (کلمبیا) و آسونسیون (پاراگوئه). مرکز فرماندهی عملیات‌های ویژه ارتش آمریکا (آژانسی که بر برنامه‌های عملیات ویژه در شاخه‌های مختلف نظامی نظارت می‌کند) نیز با این شرکت اسرائیلی قرارداد دارد[۱۸]. فرماندهی Global Strike Command ارتش آمریکا نیز که یگانی در نیروی هوایی مختص حملات اتمی است با این شرکت قرارداد بسته است[۱۹].

سلبرایت در انگلستان نیز به شدت فعال است. در سال ۲۰۲۰ پلیس متروپولیتن لندن قراردادی سه ساله به ارزش ۲ میلیون پوند با این شرکت بست تا از محصولات ویژه آن استفاده کند[۲۰]. پلیس لندن اعلام کرد که نرم‌افزار شرکت سلبرایت تنها نمونه در بازار است که «کاملاً نیازمندی‌های پلیس را برطرف می‌کند» و به‌خصوص به قابلیت نفوذ به گوشی‌های اندروید اشاره دارد. مشخص نیست که آیا این قرارداد تمدید شده است یا خیر.

در سال ۲۰۱۸ نیز پلیس اسکاتلند قراردادی به ارزش ۳۷۰ هزار پوند با شرکت سلبرایت بست[۲۱] تا ۴۱ «کیوسک سایبری» برای پلیس در سراسر اسکاتلند ایجاد کند که اقداماتی چون نفوذ به تلفن همراه در آن محل فراهم شود. در سال ۲۰۲۲ نیز پلیس ولز شمالی اعلام کرد که حدود ۲۵۰ هزار پوند به شرکت سلبرایت پرداخت کرده تا ابزارهایی در زمینه «عبور از رمزعبور» و «ورود از طریق زور» به تلفن‌های همراه خریداری کند[۲۲].

پلیس شهر کنت، نیروی پلیسی که به تازگی تهدید کرده بود افرادی را که پرچم فلسطین در اختیار داشته باشند، دستگیر می‌کند[۲۳]، سال پیش قراردادی یک‌ساله با سلبرایت بست[۲۴]. امسال دو نیروی پلیس دیگر در انگلستان با سلبرایت قرارداد امضا کردند. در ماه فوریه نیرو پلیس شهر لندن (پلیس فعال در حوزه مالی لندن و متفاوت با پلیس متروپولیتن) صد هزار پوند برای دریافت ابزارهای سلبرایت پرداخت کرد[۲۵]. در ماه آوریل نیز پلیس لسترشایر قراردی یکساله با سلبرایت به ارزش ۳۲۸هزار پند امضا کرد[۲۶]. سلبرایت همچنین قراردی با وزارت خزانه‌داری انگلیس نیز امضا کرده است[۲۷].

در انگلستان برطبق ساختار قانونی «سامانه پویا خرید ابزارهای جرم‌شناسی دیجیتال»، شرکت سلبرایت یک تامین‌کننده ثبت‌شده و مورد تایید به حساب می‌آید. به گزارش نهاد مسئول جهت امضای قراردادهای تجاری برای نیروهای پلیس در انگلستان این قانون «به‌کارگیری مستقیم ابزارهای شرکت سلبرایت برای نیروهای پلیس در سراسر انگلستان را امکان‌پذیر می‌سازد»[۲۸].

---

[18] https://www.highergov.com/contract/H9225725P0004/
[19] https://www.highergov.com/contract-opportunity/notice-of-intent-to-sole-source-cellebrite-f3c3sf5100aw01-s-cdfd9/
[20] https://www.london.gov.uk/programmes-strategies/mayors-office-policing-and-crime/governance-and-decision-making/mopac-decisions-0/licences-and-ongoing-support-cellebrite-premium-tool
[21] https://www.publictechnology.net/2018/04/09/business-and-industry/police-scotland-invests-cyber-kiosks-extract-data-mobile-devices/
[22] https://bidstats.uk/tenders/2022/W37/782631280
[23] https://skwawkbox.org/2025/07/15/video-police-using-palestine-action-proscription-to-target-even-mention-of-palestine-gaza-freedom/
[24] https://intelapp.io/explore/contracts/9ca94fc9-f978-4871-b4c1-7c5e5997c64e/cellebrite-licences-kent-essex
[25] https://www.contractsfinder.service.gov.uk/notice/6e107d92-a73e-456d-a2d2-de17fcaa2608
[26] https://www.find-tender.service.gov.uk/Notice/016210-2025
[27] https://bidstats.uk/tenders/2024/W24/824377435
[28] https://bluelightcommercial.police.uk/helping-police/forensics/digital-dps/

این که نیروهای پلیس در انگلستان تا چه اندازه از این ابزارهای جاسوسی استفاده می‌کنند، مشخص نیست. تحقیق سازمان حریم‌شخصی بین‌المللی (Privacy International) (سازمان مردم‌نهاد در زمینه دفاع از حقوق بشر ثبت‌شده در انگلیس) نشان می‌دهد که ۲۶ نیرو از مجموع ۴۷ نیروی پلیس در انگستان به استفاده از این محصولات معترف بودند و سایرین به برنامه‌ریزی جهت استفاده آزمایشی از آن اذعان داشتند[۲۹]. درخواست‌ها جهت دسترسی به اطلاعات شخصی و نقض حریم شخصی با مبنای موارد امنیتی و امنیت ملی در سالهای اخیر افزایش داشته است.[۳۰،۳۱]

شرکت سلبرایت به نقش خود در نسل‌کشی ارتش صهیونیستی در غزه افتخار می‌کند و اعلام کرده با ارائه سرویس‌های هک تلفن همراه خود به سرویس اطلاعاتی اسرائیل پس از طوفان‌الاقصی، «نقشی بنیادی» در این زمینه ایفا کرده است[۳۲].

کاب‌وب تکنولوژیز

دیگر شرکتی که به ارائه ابزارهای جاسوسی می‌پردازد و محصولاتی حتی شاید به‌روزتر دارد، شرکت «کاب‌وب تکنولوژیز» (Cobweb Technologies) نام دارد که توسط اعضای سابق ۸۲۰۰ Omri Timianker, Udi Levy, و Shay Attias[۳۳] تاسیس شده و تعداد زیادی از اعضای سابق ۸۲۰۰ در آن فعالیت می‌کنند[۳۴]. این شرکت در سال ۲۰۲۳ به شرکتی به نام PenLink فروخته شد اما تیم مدیریتی کاب‌وب حفظ شدند. در میان سرویس‌هایی که این شرکت به فروش می‌رساند، می‌توان به سامانه‌های تشخیص چهره و تشخیص تصویر در شبکه‌های اجتماعی و دیپ وب (deep web) و خصیصه‌ای به اسم WebLoc اشاره کرد؛ WebLoc دنبال کردن جابجایی‌های تلفن‌های همراه در مناطق خاصی را امکان‌پذیر می‌سازد که توسط کاربر انتخاب شده است. این قابلیت که به آن geofencing می‌گویند توسط تبلیغات درون‌برنامه‌ای نرم‌افزارها امکان‌پذیر شده که داده‌های شخصی را از تلفن‌های همراه بیرون می‌کشند و سپس به شرکت‌های حوزه فناوری جاسوسی مانند کاب‌وب می‌فروشند تا این داده‌ها را در ابزارهایی مانند WebLoc ادغام کنند.

اعضای این شرکت در یک نشست خبری[۳۵] (اکنون حذف شده اما آرشیو اینترنتی آن موجود است) از جزئیات اقداماتشان صحبت کرده‌اند. کاب‌وب پیش از این قراردادی به ارزش ۲.۷ میلیون دلار با اداره مهاجران غیرقانونی آمریکا منعقد کرده بود و یک قرارداد فعال به ارزش ۳.۲ میلیون دلار با وزارت امنیت داخلی آمریکا دارد[۳۶] . از ماه ژوئن نیز این شرکت قراردادی به ارزش ۵.۳ میلیون دلار با اداره ایمنی عمومی ایالت تگزاس امضا کرده است[۳۷]. یک گزارش در سال ۲۰۲۴ نیز نشان می‌دهد نیروی پلیس لس‌آنجلس (LAPD) از ابزارهای کاب‌وب جهت نظارت، شنود و موقعیت‌یابی در طول سالیان اخیر استفاده کرده است[۳۸].

---

[29] https://www.infosecurity-magazine.com/news/uk-police-secretly-hoover-up/
[30] https://www.south-wales.police.uk/foi-ai/south-wales-police/disclosure-log/2025/april/foi-365252/
[31] https://www.westyorkshire.police.uk/freedom-of-information/march-2025-foi-2431829-25-cellebrite
[32] https://www.jns.org/israels-cellebrite-plays-key-role-in-trump-shooting-and-oct-7-probes/
[33] https://ictidc.wixsite.com/ict18/omri-timianker
[34]https://www.linkedin.com/search/results/people/?currentCompany=%5B%22946609%22%5D&keywords=unit%208200&origin=FACETED_SEARCH&sid=.uA
[35] https://web.archive.org/web/20230207115908/https://cobwebs.com/press-releases/cobwebs-technologies-redefining-the-norms-of-cyber-intelligence/
[36] https://www.usaspending.gov/search/?hash=fcef1f90000404554ca15e6b5373d65c
[37] https://www.codastory.com/surveillance-and-control/texas-state-police-gear-up-for-massive-expansion-of-surveillance-tech/
[38] https://www.vice.com/en/article/the-lapd-is-using-controversial-mass-surveillance-tracking-software/

در سال ۲۰۲۰ این شرکت یک دفتر در لندن تاسیس کرد[۳۹] تا بتواند فناوری‌های جاسوسی خود را در بازار انگلیس به نیروهای پلیس و سرویس‌های امنیتی این کشور به فروش برساند. هیچ اطلاعاتی به شکل علنی از همکاری نهادهای انگلیسی با این شرکت در اینترنت اما موجود نیست.

شرکت کاگنایت

دیگر شرکت مهم فناوری جاسوسی اسرائیلی که با سرویس‌های امنیتی غربی همکاری می‌کند، شرکت کاگنایت (Cognyte) نام دارد. این شرکت شاخه جداشده‌ای از دیگر شرکت جاسوسی اسرائیلی با نام Verint است. مدیریت کاگنایت با ایلاد شارون (Elad Sharon)[۴۰]، گیل کوهن (Gil Cohen) و رونی لمپل (Ronny Lempel) است. تمام این افراد نیروهای سابق ارتش اسرائیل و یگان ۸۲۰۰ هستند. تصویر صفحه لینکدین ایلاد شارون همراهی این شرکت با اسرائیل است.

محصولات کاگنایت ابزارهای اطلاعات شبکه است[۴۱] که می‌تواند حجم زیادی از اطلاعات را در بربگیرد. به خصوص منظور اطلاعات برج‌های مخابراتی 4G و 5G، متادیتاهای مخابراتی، پلتفرم‌های پیامرسان، تماس‌های صوتی و سیگنال‌های شبکه است. محصولات این شرکت قادر هستند با ارزیابی این داده‌ها بتوانند الگوها و روندهای غیرمعمول را در ارتباطات صورت‌گرفته را شناسایی کنند. چنین خدمتی در یک پلتفرم مبتنی بر داده عرضه می‌شود که به کاربران اجازه می‌دهد نکات مدنظر را به هم متصل کنند تا تحلیل مناسب را دریافت کنند. اعلام شده که تمام این فرایند کاملاً قانونی صورت می‌گیرد؛ با این‌حال هیچ اطلاعات دقیقی درباره نحوه عملکرد محصولات این شرکت ارائه نشده است و اخباری پیرامون نحوه استفاده دستگاه‌های امنیتی غربی از این ابزار درز نشده است.

کاگنایت تا به حال نام کاربران نهایی محصولاتش یا همان مشتریانش را افشا نکرده است. این شرکت تنها به جوایز متعددی که دریافت کرده اشاره می‌کند.

برطبق اطلاعات به دست آمده، سرویس‌های امنیتی غربی، نهادهای نظامی و امنیتی در مجموع قراردادهایی به ارزش ۶۰ میلیون دلار با شرکت کاگنایت منعقد کرده‌اند. این شامل قرارداد ساله یک آژانس امنیت ملی در اروپا به ارزش ۲۰ میلیون دلار[۴۲]، قرارداد به ارزش ۳ میلیون دلار با یک اداره پلیس در آمریکا[۴۳] و یک قرارداد ۱۰ میلیون دلاری با یک ارتش اروپایی[۴۴]است؛ قراردادی که به تازگی منعقد شده است. در گزارش خبری این قرارداد ذکر شده که «شرکت کاگنایت به انتقال محصولات ثابت‌شده در میدان، جهت تقویت گروه‌های نظامی در خط مقدم با اطلاعات عملیاتی که جهت اقدام به آن نیاز دارند، ادامه می‌دهد.

---

[39] https://markets.businessinsider.com/news/stocks/cobwebs-technologies-the-world-s-most-advanced-open-source-web-intelligence-company-opens-office-in-london-1028897567

[40]

[41] https://www.cognyte.com/network-intelligence/

[42] https://www.cognyte.com/news/cognyte-secures-a-20-million-annual-three-year-agreement-with-a-national-security-agency/

[43] https://www.cognyte.com/news/leading-north-american-law-enforcement-agency-places-2m-plus-follow-on-order-with-cognyte/

[44] https://www.cognyte.com/news/cognyte-wins-10m-deal-with-tier-1-military-organization-in-emea-following-competitive-evaluation/

برطبق اسناد قراردادهای دولتی دو مشتری این شرکت، سرویس مخفی آمریکا (به‌خصوص فعال در زمینه تامین امنیت و حفاظت از شخصیت‌های سیاسی آمریکایی) و سفارت آمریکا در ال‌سالوادور هستند[۴۵].

تعداد اعضای سابق ۸۲۰۰ که در این شرکت کار می‌کنند نیز زیاد است[۴۶].

شرکت ورینت

شرکت کاگنایت خود انشعابی از شرکت دیگری به نام ورینت (Verint) بود. این شرکت نیز در حوزه جاسوسی بسیار فعال است و از مدت‌ها پیش محصولاتش را به سرویس‌های امنیتی غربی می‌فروشد. در سال ۲۰۱۴ سوئیس وظیفه ساخت ساختار شنود و نظارتی خود را به این شرکت اسرائیلی سپرد[۴۷] و در سال ۲۰۱۷ نیز وزارت جنگ آمریکا مبلغ ۳۵ میلیون دلار به این شرکت جهت فعالیت بر روی پروژه‌ای محرمانه پرداخت کرد[۴۸]. در ۲۰۱۸ نیز این شرکت قراردادی به ارزش ۵۰ میلیون دلار با پلیس انگلستان منعقد کرد که ظرفیت‌های سایبری جدیدی ایجاد کند[۴۹].

شرکت Corsight AI

دیگر شرکت مطرح اسرائیلی در این حوزه Corsight AI نام دارد که محصولات تشخیص چهره خود را به پلیس اسکس بریتانیا فروخته است[۵۰]. محصولات این شرکت که قادر به شناسایی چهره افراد و بررسی آنها در چندین دیتابیس هستند، نخست بر روی فلسطینی‌ها در غزه و کرانه باختری آزمایش شدند. به گزارش مقاله bylinetimes این فناوری در طی نسل‌کشی غزه توسط ارتش به‌کار گرفته شد. بنیان‌گذار این شرکت ایگال رایشلگاز (Igal Raichelgauz) افسر سابق اطلاعاتی اسرائیل است. این شرکت همچنین محصولات تشخیص چهره خود را به پلیس نظامی سائوپائو برزیل و پلیس متروپولیتن بوگوتا کلمبیا فروخته است[۵۱].

بریفکام

دیگر شرکت اسرائیلی در حوزه ابزارهای تشخیص چهره، «بریفکام» (Briefcam) نام دارد که قراردادهایی با نیروهای پلیس انگلستان و آمریکا منعقد کرده است. اداره پلیس کامبریا انگلیس[۵۲] در شبکه دوربین‌های مداربسته خود در سراسر این منطقه از سامانه تحلیلی بریفکام استفاده می‌کند؛ هرچند مدعی شده که تجهیزات تشخیص چهره را غیرفعال کرده است. در فرانسه نیز پس از افشای همکاری نیروهای پلیس در سراسر کشور[۵۳] از محصولات این شرکت، به دلیل نقض قوانین حریم شخصی

---

[45] https://www.highergov.com/awardee/cognyte-software-lp-12518811/
[46] https://www.linkedin.com/search/results/people/?currentCompany=%5B%223669%22%5D&keywords=unit%208200&origin=FACETED_SEARCH&sid=V!0
[47] https://www.efk.admin.ch/wp-content/uploads/publikationen/berichte/wirtschaft_und_verwaltung/informatikprojekte/14393/14393be_bericht-mit-stellungnahme-alle-sprachen_publikation.pdf
[48] https://intelligencecommunitynews.com/verint-receives-35-million-order-for-security-solution
[49] https://www.marketscreener.com/quote/stock/VERINT-SYSTEMS-INC-97645/news/Verint-Web-Intelligence-Solution-Selected-to-Support-UK-Law-Enforcement-Agencies-28922224/
[50] https://bylinetimes.com/2025/02/24/police-face-recognition-technology/
[51] https://www.businesswire.com/news/home/20240619024171/en/Corsight-AI-Partners-with-Segdboa-to-Provide-So-Paulo-Military-Police-with-Facial-Intelligence-Capabilities
[52] https://www.cumbria.police.uk/police-forces/cumbria-constabulary/areas/about-us/about-us/cctv/
[53] https://www.euractiv.com/section/tech/news/french-police-accused-of-using-facial-recognition-software-illegally/

قرارداد با این شرکت در ۲۰۲۳ کنسل شد. پلیس بروکسل و ورشو نیز از قابلیت تشخیص چهره بریفکم استفاده می‌کنند[۵۴]. در آمریکا نیز نیروهای پلیس شیکاگو، اسپرینگفیلد و بورلی هیلز استفاده خود از این محصولات را تایید کرده‌اند[۵۵].

شرکت NICE

شرکت NICE توسط سربازان سابق ارتش اسرائیل تاسیس شد[۵۶] با قابلیت شناسایی کلاهبرداری مالی توانست بسیار سروصدا کند و ۸۵ درصد از ۵۰۰ شرکت برتر دنیا (Fortune 500) و تعدادی از رگولاتورهای اروپایی از محصولاتش استفاده می‌کنند. این شرکت چندمیلیارددلاری همچنین ابزارهای نظارتی و جاسوسی برای شهرداری‌ها ارائه می‌کند، سامانه تشخیص پلاک خودرو، ضبط چهره[۵۷] و همچنین خروجی‌های ویدویی مبتنی بر GPS و سنسورهای ویدیویی موبایل جهت ردیابی شهروندان. در تحقیقات موسسه Buzfeed در سال ۲۰۱۵ مشخص شد که شرکت NICE ابزارهای محرمانه جاسوسی به تعدادی از شرکت‌ها ارائه کرده است[۵۸].

مکعب سیاه

یکی از بدنام‌ترین شرکت‌ها در این زمینه، شرکت مکعب سیاه یا Black Cube نام دارد که توسط اعضای سابق ۸۲۰۰ دن زورلا (Dan Zorella) و آوی یانوس (Avi Yanus) تاسیس شد. این شرکت توسط هاروی واینستین (Harvey Weinstein) (تهیه‌کننده فیلم و متجاوز معروف آمریکایی) استخدام شد[۵۹] تا اطلاعاتی از اتهام‌زنندگان به او دریافت کند. واینستین همیشه رابطه صمیمانه‌ای با اسرائیل داشت[۶۰]. این شرکت در چندین رسوایی جاسوسی نقش داشته است و در گذشته دیپلمات‌های سابق غربی را استخدام کرده بود؛ به‌طور مثال ویویان برکویچی (Vivian Bercovici) سفیر سابق کانادا در اسرائیل جذب این شرکت شده بود.[۶۱]

تحلیل و بررسی

رژیم صهیونیستی از یک گفتمان چندلایه برای مشروعیت‌بخشی به صادرات فناوری جاسوسی استفاده می‌کند. در سطح بین‌المللی، از گفتمان «ملت [!] استارتاپ» (Startup Nation) بهره می‌برد که اسرائیل را به‌عنوان یک کشور نوآور، دموکرات و پیشرو در فناوری معرفی می‌کند[۶۲] . این گفتمان، جایی برای بحث درباره سوءاستفاده از فناوری را فراهم نمی‌کند. در سطح امنیتی، از گفتمان «مبارزه با تروریسم» و «امنیت ملی» استفاده می‌شود تا فروش جاسوس‌افزارها به دولت‌هایی با سابقه نقض حقوق بشر را توجیه کند. این گفتمان، قربانیان جاسوسی — خبرنگاران، فعالان حقوق بشر، دیپلمات‌ها — را به‌عنوان «تهدید بالقوه» تعریف می‌کند. در سطح فناوری، محصولات با اصطلاحاتی مانند «قانونی»، «متناسب» و «جهت نظارت» توصیف

---

[54] https://algorithmwatch.org/en/computer-vision-police-discrimination/
[55] https://www.briefcam.com/resources/case-studies/briefcam-at-work-in-safe-cities/
[56] https://www.calcalist.co.il/ctechnews/article/skkvk4pqr
[57]https://www.techmonitor.ai/technology/software/nice_wins_20_million_security_project_from_emea_171108
[58] https://www.buzzfeednews.com/article/sheerafrenkel/meet-the-companies-whose-business-is-letting-governments-spy
[59] https://www.theguardian.com/film/2020/jan/30/harvey-weinstein-black-cube-new-york-times
[60] https://www.algemeiner.com/2017/09/20/oscar-winning-producer-harvey-weinstein-at-algemeiner-gala-i-am-israeli-in-my-heart-and-mind/
[61] https://www.cbc.ca/news/politics/vivian-bercovici-black-cube-1.6034555
[62] Senor, D., & Singer, S. (2009). *Start-Up Nation: The Story of Israel's Economic Miracle*. Twelve.

می‌شوند، در حالی‌که واقعیت، استفاده غیرقانونی و گسترده از آنهاست[۶۳]. این گفتمان‌ها با هم، یک ساختار روایی می‌سازند که در آن، جاسوسی نه یک سرکوب، بلکه یک «ضرورت امنیتی» است.

اساساً وجود صنعت جاسوس‌افزار اسرائیل نشان‌دهنده یک تغییر پارادایمی در سیاست اشغالگری رژیم صهیونیستی است. پارادایم قبلی، اشغال فیزیکی از طریق قدرت فیزیکی همچون نیروی نظامی، دیوارکشی و مستعمره‌سازی بود. پارادایم جدید، اشغال دیجیتال است که در آن، کنترل از طریق کد، الگوریتم و داده انجام می‌شود. هزینه آن نیز از پول مالیات شهروندان غربی تامین می‌شود. فلسطین، به ویژه کرانه باختری و غزه، به‌عنوان یک آزمایشگاه باز برای تست فناوری‌های نظارتی عمل کرده است.

این فناوری‌ها - از تشخیص چهره گرفته تا نفوذ به تلفن‌های همراه - ابتدا روی فلسطینی‌ها آزمایش شده و سپس به بازار جهانی صادر شده‌اند. در این پارادایم جدید، اشغالگری از یک عملیات نظامی به یک صنعت فناورانه تبدیل شده و این مسئله به اسرائیل اجازه داده است تا با وجود انزوای شدید در افکار عمومی، نفوذ جهانی در بین دولتها داشته باشد. این صنعت، نه فقط درآمدزا است، بلکه یک ابزار دیپلماسی نرم و امنیت‌زا است که اسرائیل را به شریکی غیرقابل حذف برای بسیاری از دولت‌های غربی تبدیل کرده است.

باید درنظر گرفت که صنعت جاسوس‌افزار اسرائیل، یک هیبرید نظامی- تجاری - سیاسی است که در آن، مرز و تفاوت بین ارتش، صنعت و سیاست از بین رفته است. صنعت جاسوس‌افزار، تنها یک واکنش منفعلانه به تهدیدات امنیتی نیست، بلکه یک استراتژی فعال برای تثبیت قدرت رژیم است. این قدرت، نه فقط در منطقه، بلکه در سطح جهانی اعمال می‌شود.

با صادر کردن فناوری نظارت، اسرائیل نه تنها درآمد دارد، بلکه شرکایش را به ادامه حمایت از خود و سیاست‌هایش وادار می‌کند. این وابستگی به فناوری اسرائیل، انتقاد از اشغالگری را پیچیده می‌کند؛ زیرا بسیاری از کشورهایی که به ظاهر به حقوق بشر اهمیت می‌دهند، از همین فناوری‌ها برای نظارت داخلی استفاده می‌کنند.

بنابراین، مبارزه با جاسوس‌افزارهای اسرائیلی، نه تنها یک مسئله حقوق بشری، بلکه یک نیاز اخلاقی-سیاسی برای بازتعریف رابطه بین فناوری و قدرت است. بدون در نظر گرفتن این پارادایم جدید، هرگز نمی‌توان به درستی به ابعاد اشغالگری دیجیتال پی برد.

مصادیق افشاشده از فعالیت‌های شرکت‌های جاسوسی اسرائیلی — از پگاسوس تا Cellebrite — تنها نمونه‌هایی از یک صنعت بسیار گسترده‌تر و پنهان‌تر هستند. این شرکت‌ها با همکاری نهادهای امنیتی غربی و استفاده از زیرساخت‌های قانونی و غیرقانونی، سال‌هاست که در حوزه نظارت دیجیتال فعالیت دارند. آنچه تاکنون فاش شده، احتمالاً فقط "نوک کوه یخ "است. با توجه به محدودیت دسترسی به اطلاعات طبقه‌بندی‌شده، وجود شبکه‌های بیشمار دیگر از شرکت‌های ناشناس یا غیرمستقیم، و استفاده نظام‌مند از فناوری برای سرکوب و نظارت، می‌توان انتظار داشت که مقیاس واقعی این صنعت بسیار پررنگ‌تر و خطرناک‌تر از آن چیزی باشد که عموم آن را می‌دانند.

[63] Human Rights Watch. (2022). *NSO Group's Pegasus Spyware: An Overview*. https://www.hrw.org