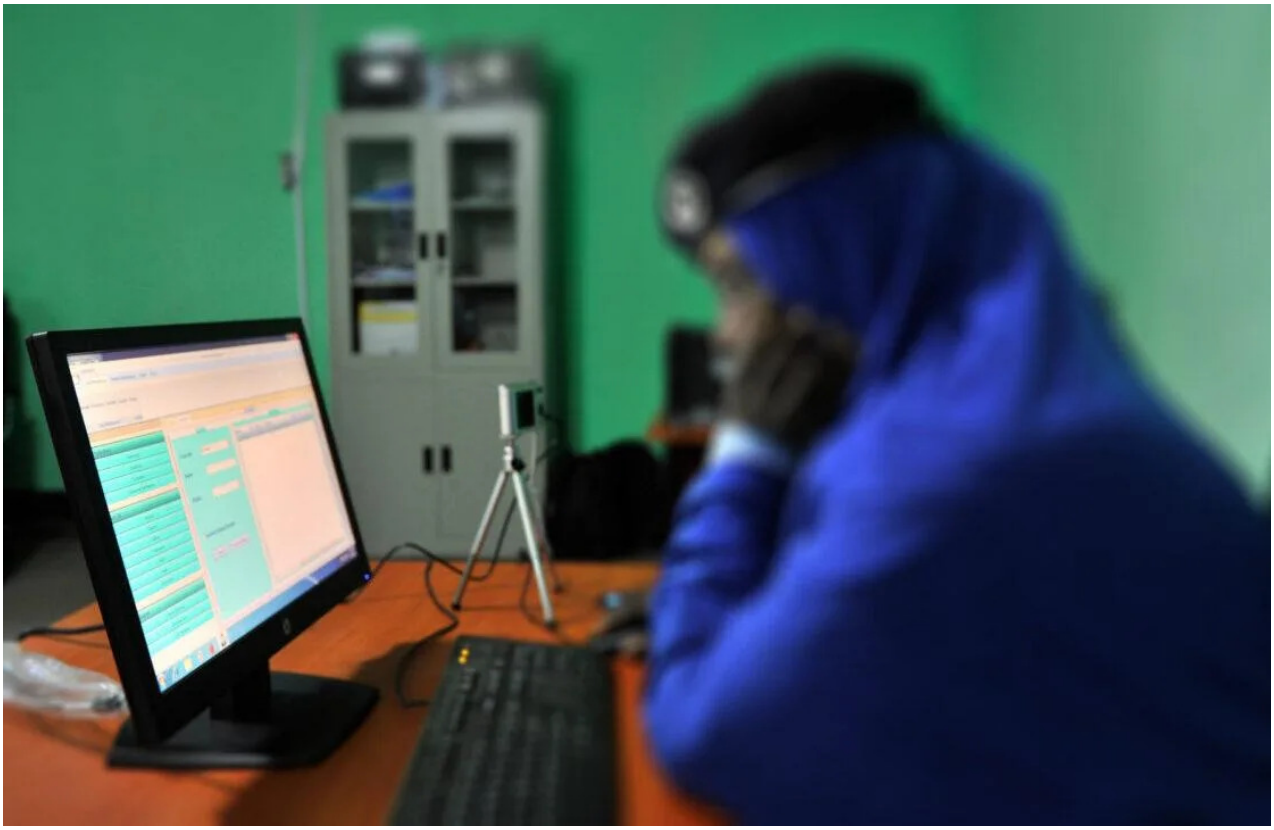
لماذا تزوّد "إسرائيل" إفريقيا بتقنيات تجسس متقدمة؟



في فبراير/شباط 2026، كشف تحقيق لصحيفة الغارديان أن سلطات كينيا استخدمت تقنية إسرائيلية متقدمة من شركة "سيلبريت" لاختراق الهاتف الشخصي للناشط والمرشح الرئاسي المحتمل بونيفاس موانغي أثناء احتجازه.

هذا البرنامج مكّن الشرطة من فك تشفير الهاتف بالكامل استخراج الرسائل والملفات الخاصة وكلمات السر والحسابات المالية من هاتفه، في واحدة من أحدث حلقات تسخير الحكومات الإفريقية للتقنيات الإسرائيلية لقمع المعارضين.

أعادت هذه الواقعة تسليط الضوء على توسع نفوذ شركات الأمن السيبراني والعتاد العسكري الإسرائيلية في القارة، وعلى الأهداف المتبادلة بين تل أبيب والعواصم الإفريقية.

3 أدوات تجسس إسرائيلية متطورة

تنتشر برامج التجسس الإسرائيلية في إفريقيا بشكل واسع، فقد جرى توثيق استهداف نشطاء حقوقيين في أنغولا والمغرب ورواندا، وصحفيين في توغو، ومصادر صحفية في بوتسوانا.

كما جرى استهداف معارضين في إثيوبيا وغانا والغابون، وحتى دبلوماسيين أمريكيين في أوغندا، وفق بحث لمعهد الدراسات الأمنية الإفريقي.

وتعتمد كثير من الحكومات الإفريقية على هذه التقنيات لتعقب المعارضين والخصوم السياسيين، ما يعمق التوجهات السلطوية ويقوض الديمقراطية كما يحذر تقرير لمعهد بروكينغز.

التكنولوجيا التي تُصدّرها شركات إسرائيلية إلى إفريقيا تشمل أدوات تجسس معقدة قادرة على تحويل الهاتف إلى جهاز مراقبة كامل، أبرزها:

1- برنامج بيغاسوس من مجموعة "NSO": قادر على التسلل إلى الهواتف بدون أي تفاعل من المستخدم؛ ويمكنه سرقة الصور والرسائل وكلمات المرور، وتفعيل الكاميرا والميكروفون وتتبع المواقع.

2- برنامج بريداتور: تطوره مجموعة إنتيليكسا – وهي شبكة شركات يقودها الضابط الإسرائيلي السابق تال ديليان – ويوفر للمهاجمين وصولًا كاملًا للميكروفون والكاميرا والبيانات من الهاتف المصاب.

3- جهاز سيلبريت: يسمح باستخراج كافة البيانات والملفات من أجهزة أندرويد وآيفون، ويُعد جزءًا من سوق أدوات تحليل الأدلة الجنائية التي تباع لحكومات العالم.

أبرز وقائع التجسس المكتشفة في إفريقيا

1- كينيا: استهداف المعارضين باستخدام "سيلبريت"

في يوليو/تموز 2025 اعتقلت السلطات الكينية الناشط بونيفاس موانغي وصادرت هاتفه. تحليل تقني لـ"Lab Citizen" كشف أن الشرطة استخدمت برنامج "سيلبريت" لفك تشفير هاتفه بالكامل.

عُثر على تطبيق يحمل توقيع "سيلبريت" داخل الهاتف، ومن خلاله اسُتخرجت رسائله الخاصة وملفاته وحساباته المالية وكلمات المرور، في خرق واضح للدستور الكيني وقانون حماية البيانات.

بونيفاس موانجي: أعلم أن مكالماتي الهاتفية مراقبة ورسائلي تُقرأ (AFP)

2- أنغولا: الصحافة تحت مقصلة "بريداتور"

في فبراير/شباط 2026 أكد تحقيق لمنظمة "لجنة حماية الصحفيين" أن هاتف الصحفي والمحامي الأنغولي تيشيرا كانديدو تعرّض للتجسس بواسطة برنامج "بريداتور" وذلك قبل انتخابات 2027، وفي سياق بيئة تضييق على الصحافة.

أرسل مجهول رسالة واتساب تتظاهر بأنها من مجموعة طلاب، وبمجرد أن نقر كانديدو على الرابط تم تثبيت البرنامج على هاتفه، مما منح المهاجمين قدرة على التحكم بالميكروفون والكاميرا والوصول إلى جهات الاتصال والرسائل والصور.

كانديدو وصف التجربة بقوله "شعرت وكأنني عارٍ في الشارع، لا أعلم ما المعلومات التي حصلوا عليها عن حياتي الخاصة".

3- توغو: استهداف الصحفيين بـ"بيغاسوس"

في يناير/كانون الثاني 2024 كشفت منصة الأمن السيبراني "دارك ريدينغ" أن تحقيقًا لمنظمة "مراسلون بلا حدود" رصد اختراق هواتف عدة صحفيين توغوليين بواسطة برنامج بيغاسوس.

أظهرت النتائج أن برنامج التجسس استخدم بين فبراير/شباط ويوليو/تموز 2021 لاختراق هاتف لويك لوسون، ناشر صحيفة فلامبو دي ديموقرات، على الأقل 23 مرة، وتعرض الصحفي الحر أناني سوسو لهجوم مماثل في أكتوبر/تشرين الأول 2021.

وتضمنت قائمة 50 ألف رقم مسربة من مشروع "بيغاسوس" أسماء ثلاثة صحفيين توغوليين آخرين. التقرير يشرح أن البرنامج الذي تصنعه شركة "NSO" الإسرائيلية يسمح للمشغل باستخراج كامل البيانات واعتراض الرسائل والبريد الإلكتروني وكلمات المرور والموقع دون علم المستخدم.

4- المغرب ورواندا: التجسس على قادة ومسؤولين

تكشف دراسة نشرها مركز بروكينغز في 2021 عن اتساع نطاق استخدام بيغاسوس عبر إفريقيا. وتشير إلى أن الحكومتين المغربية والرواندية استخدمتا البرنامج للتجسس على معارضين وسياسيين خارج

الحدود.

فالمغرب يُعتقد أنه استهدف ما يصل إلى 10 آلاف رقم، بينما استخدمته رواندا لمراقبة حوالي 3500 ناشط وصحفي وسياسي ودبلوماسي، بينهم ابنة معارض رواندي يعيش في المنفى.

هذه الأدوات تُستخدم أيضًا للتجسس على دول مجاورة؛ فقد أدرجت رواندا رقم رئيس جنوب إفريقيا سيريل رامافوزا ضمن قائمة الأهداف.

فيما وضع المغرب مسؤولين جزائريين وفرنسيين على لائحة المراقبة. هذه الممارسات تظهر كيف تسهم التكنولوجيا الإسرائيلية في إشعال سباق تجسس إقليمي وتزيد من ميول الاستبداد.

الأهداف الإسرائيلية.. رافعة دبلوماسية

1- اختراق "القلعة" الإفريقية: الهدف الأسمى لـ"إسرائيل" هو كسر "الأغلبية التلقائية" المؤيدة لفلسطين في المنظمات الدولية.

صرح مسؤولون إسرائيليون سابقون وصحفيون (مثل أميتاي زيف من هآرتس) بوضوح: "عندما تبيع إسرائيل السايبر لدولة إفريقية، فهي تضمن صوتها في الأمم المتحدة".

مبيعات السلاح والسايبر هي الرشوة الدبلوماسية التي مكنت "إسرائيل" من الحصول على صفة مراقب في الاتحاد الإفريقي (قبل تجميدها لاحقًا).

قطاع السايبر يمثل نسبة ضخمة من صادرات الهايتك الإسرائيلية

2- تصدير نموذج الاحتلال: تسعى "إسرائيل" لتطبيع ممارساتها القمعية عالميًا. عندما تستخدم دول ذات سيادة تقنيات طُورت لقمع الفلسطينيين، فإن ذلك يمنح شرعية ضمنية لهذه التقنيات ولهذا النموذج الأمني. يصبح الاحتلال "مختبرًا" للابتكار، وتصبح إفريقيا "السوق".

3- العائد الاقتصادي: قطاع السايبر يمثل نسبة ضخمة من صادرات الهايتك الإسرائيلية (13 مليار دولار

صادرات دفاعية في 2023 جزء كبير منها سايبر)، وهي أموال ضرورية لاستدامة المجمع الصناعي العسكري الإسرائيلي.

المكاسب الإفريقية.. بقاء الأنظمة

1- التفوق الاستباقي: توفر التكنولوجيا الإسرائيلية لأنظمة الحكم الإفريقية القدرة على "التنبؤ" بالاحتجاجات وإجهاضها قبل بدئها، ومعرفة نوايا المعارضين.

2- تجاوز العقبات الغربية: الدول الغربية تضع نظريًا شروطًا حقوقية لبيع السلاح. "إسرائيل" تبيع "بدون أسئلة"، ما جعلها الشريك المثالي للأنظمة المنبوذة.

3- الوصول إلى واشنطن: يعتقد العديد من القادة الأفارقة أن الطريق إلى البيت الأبيض يمر عبر "تل أبيب". شراء التكنولوجيا الإسرائيلية يعد "عربون صداقة" يفتح أبواب اللوبي الصهيوني في واشنطن للدفاع عن هذه الأنظمة وتبييض صورتها أمام الكونغرس.

يظهر التقرير أن التكنولوجيا الإسرائيلية في إفريقيا ليست أداة للتنمية أو الأمن بمفهومه الإنساني، بل "سوط رقمي" يلهب ظهور الشعوب الساعية للحرية ومحاولة إسرائيلية لاستنساخ نموذج "دولة المراقبة" في الضفة الغربية وتطبيقه على نطاق قاري.

رابط المقال: https://www.noonpost.com/358250/