التجسس الإلكتروني: سلاح إسرائيل الذهبي لمراقبة العرب

كتبه إلهام محمد | 8 سبتمبر ,2016

أصبح التجسس الإلكتروني أحد أخطر وأجدى أنواع التجسس، فقد طغى بإمكانياته الهائلة ودقة نتائجه على أساليب التجسس المعهودة في السابق.

وأدركت إسرائيل أهمية هذا النوع من التجسس وخصصت إمكانياتها للتجسس على بعض الدول العربية وعلى رأسهم فلسطين ومصر، بالإضافة إلى حلفائها كالأمريكيين والغرب، وبذلك امتد ذراع التجسس الإلكتروني الإسرائيلي إلى أقصى حد ممكن يخدم مصلحة الاحتلال الإسرائيلي.

واعتمد جيش الاحتلال الإسرائيلي خلال السنوات الماضية، بشكل كبير على الأقمار الصناعية للتجسس على الدول العربية، فقد ارتفعت نسبة الاعتماد تلك من 150% إلى 200%، بهدف مراقبة ما يجري في المنطقة العربية، ويؤكد ضابط إسرائيلي من شعبة التنصت التابعة للمخابرات الحربية في دولة الاحتلال: "أن الاعتماد على الأقمار الصناعية في الحصول على المعلومات وعمليات الرصد لن يتوقف بل سيزداد خلال السنوات القادمة، نظرًا لما تتعرض له المنطقة من أحداث".

وكشفت صحيفة "إسرائيل اليوم" أنّ دولة الاحتلال تُسيطر على فضاء جميع الدول العربية بواسطة 6 أقمار صناعية مهمتها تصوير كل صغيرة وكبيرة تحدث في الدول العربية وغير العربية، وتعرف الوحدة المسؤولة عن إدارة الأقمار الصناعية ذات أغراض التجسس في جيش الاحتلال،

بمجموعة أقمار "عاموس"، حيث يقوم كل واحد من الأقمار الستة بتغطية الكرة الأرضية بأكملها كل 90 دقيقة.

"بيغاسوس" يزلزل كيان آيفون

يكشف التحذير الذي أطلقته شركة أبل بعد اكتشاف برنامج تجسس يسمح باختراق أجهزة آيفون وآيباد، عن مدى التقدم الذي حققته الشركات الإسرائيلية المتخصصة في اعتراض الاتصالات.

وفي مواجهة هذا التهديد الإلكتروني، عمدت الشركة الأمريكية بشكل عاجل إلى تحديث نظام تشغيل أجهزة الآيفون التي وزعتها في الأسواق منذ عام 2011 لحمايتها من برنامج "بيغاسوس" الذي صممته مجموعة (أن.أس.أو) ومقرها هرتسيليا المعروفة بـ "وادي السيليكون" الإسرائيلي، شمال تل أبيب.

وليست مجموعة (إن. إس. أو) الوحيدة في هذا المجال في الدولة العبرية التي تطلق على نفسها لقب "أمة الشركات الناشئة" والتي تعتبر عملية جمع المعلومات ضرورة حيوية في ظل المخاطر الأمنية.

تقدر منظمة "برايفيسي انترناشونال" البريطانية غير الحكومية أن هناك 27 شركة إسرائيلية على الأقل ناشطة في هذا المجال، وهذا الرقم يضع إسرائيل البالغ عدد سكانها 8 ملايين نسمة، في طليعة التصنيف العالمي للشركات في هذا المجال، أي 3.3 شركة لكل مليون شخص، مقابل 0.4 في الولايات المتحدة و1.6 في بريطانيا، بين مستخدمي هذه البرمجيات حكومات في أمريكا اللاتينية وآسيا الوسطى وإفريقيا.

ووصفت "أوت لوك" لأمن الهواتف النقالة برنامج بيغاسوس بأنه الهجوم الأكثر تطورًا، الذي اكتشفته بسبب قدرته على التسلل خلسة إلى أجهزة الهاتف التي يخترقها وصولًا إلى المكالمات والكاميرات والبريد الإلكتروني ونظام تحديد الموقع الجغرافي وكلمات المرور والتطبيقات مثل فيسبوك وسكايب وواتساب وفايبر وغيرها.

وأكد متحدث باسم مجموعة (إن. إس. أو) الإسرائيلية في بيان أن "مهمة برامج المجموعة هي المساعدة في جعل العالم مكانًا أكثر أمانًا عبر تزويد الحكومات الشرعية بتكنولوجيا تساعدها على محاربة الإرهاب والجريمة".

وأوضح المتحدث أن المجموعة "تلتزم تمامًا بالقوانين والأنظمة المتعلقة بالرقابة على الصادرات"، في إشارة إلى التراخيص اللازمة التي تصدرها وزارة الدفاع الإسرائيلية لبيع الأسلحة والتقنيات، التي يمكن أن تكون لها استخدامات عسكرية في الخارج، ولم تشأ وزارة الدفاع الإسرائيلية التعليق على المسألة ردًا على طلب من وكالة الصحافة الفرنسية.

الحرب الإلكترونية

تقول برايفيسي إنترناشونال إن هذه القوانين والأنظمة لا تأخذ بالاعتبار وضع حقوق الإنسان في البلدان التي تطلب هذه البرامج، ما يسمح للأنظمة بمراقبة أو قمع المعارضين.

وفيما يتعلق بشركة أبل، فقد تخشى من تعرض عملائها من الأفراد والشركات إلى التجسس من خلال استلامهم روابط تتعلق بأنشطتهم.

وبحسب شركة "سيتيزن لاب" فإن المستخدمين حين ينقرون على الرابط، تدخل برامج التجسس إلى أجهزتهم سواء كانت هواتف ذكية أو أجهزة لوحية أو أجهزة كومبيوتر، لتبدأ بتتبع مكان وجودهم ومحادثاتهم وتفاصيل حساباتهم الشخصية والمصرفية والتجارية.

وبحسب وسائل الإعلام الإسرائيلية، فإن مجموعة (إن. إس. أو) قامت قبل عامين بعد حصولها على موافقة من وزارة الدفاع ببيع برمجياتها إلى عدد من دول العالم بينها دولة خليجية لم تحددها.

ويؤكد دانيال كوهين، الخبير من معهد دراسات الأمن القومي في تل أبيب ، لوكالة الصحافة الفرنسية أن "هذه القضية ليست مفاجئة، إسرائيل من الدول التي تحتل الطليعة في العالم في كل ما يتعلق بمجال الإنترنت".

ويشرح كوهين أن التقدم يأتي أساسًا من دينامية عناصر سابقة من وحدات النخبة في الجيش الإسرائيلي، مثل الوحدة 8200 المتخصصة في مجال الحرب الإلكترونية، وأضاف أن هؤلاء الخبراء "يستخدمون مهاراتهم، بعد ترك الجيش، في تأسيس شركات ناشئة أو الحصول على وظائف بأجور طائلة لدى شركات قائمة".

وبحسب كوهين فإن في إسرائيل حاليًا "أكثر من 300 شركة من جميع الأحجام في قطاع الإنترنت، كما أن أكبر شركات الأسلحة، أقامت أيضًا وحدات متخصصة بأمن الإنترنت، ولكن في الغالبية العظمى من الحالات، فإن الشركات لا تتعامل سوى مع حماية أنظمة المعلوماتية العسكرية والمدنية والتجارية، مثل البنوك والشركات العامة والخاصة".

يشير كوهين إلى أن أقل من 10%من شركات الأمن الإلكتروني اختارت التخصص في الأعمال الهجومية أي التقنيات التي تسمح باختراق الأنظمة المعلوماتية.

بينما تؤكد برايفيسي إنترناشونال أن بيع برامج التجسس "قد لعب دورًا هامًا في تعزيز التعاون بين أجهزة المخابرات" الإسرائيلية والأجنبية.

وأضافت المنظمة غير الحكومية البريطانية أن شركات ذات أصول إسرائيلية مثل "نايس سيستمز" و"فيرينت" قامت ببيع تقنيات للشرطة السرية في أوزبكستان وكازاخستان، إضافة إلى قوات الأمن في كولومبيا، كما صدرت تقنيات إلى ترينيداد وتوباغو وأوغندا وجنوب السودان وبنما والمكسيك.

وكانت وسائل الإعلام الإسرائيلية قد أوردت في عام 2011 أن شركة ألوت الإسرائيلية للاتصالات

قامت بتصدير تقنيات لمراقبة الإنترنت كانت موجهة للدنمارك، ولكن تم تحويلها إلى إيران، التي يفترض أنها عدو لدود للدولة العبرية، وسمح لشركتي نايس وفيربنت بفتح مكاتب ومركز للمراقبة في كازاخستان وأوزبكستان، إضافة إلى تدريب موظفين محليين في الدولتين.

ونسبت وكالة الصحافة الفرنسية إلى متحدث باسم مجموعة (إن. إس. أو) الإسرائيلية، تأكيده أن الاتفاقيات التي تتوصل إليها الشركة مع عملائها تشترط أن "يتم استخدام المنتجات بشكل قانوني وفقط لمنع الجريمة وللتحقيقات الجنائية".

الوحدة 8200

الوحدة "8200" أحد أكبر أسلحة التجسس التي تستعين بها إسرائيل، هي أكبر وحدات التجسس الإلكتروني في جيش الاحتلال الإسرائيلي، خصصت لجمع المعلومات وفك الشيفرات عبر وسائل الاتصال، هذه الوحدة التابعة لشعبة الاستخبارات العسكرية من أكثر الوحدات تطورًا من الناحية التقنية والتكنولوجية، فهي تعتمد في المجال الاستخباراتي على الرصد والتنصت والتصوير والتشويش، ويتطلب هذا النوع من المهام مجالًا واسعًا من وسائل التقنية المتقدمة.

وتستخدم الوحدة "8200" طائرات بدون طيار تزود القيادات الأمنية والاستخبارية في دولة الاحتلال الإسرائيلي بالمعلومات خاصة المتعلقة بعمليات الاغتيال ضد الفلسطينيين، فهي مزودة بصواريخ تقوم بإطلاقها على الأشخاص الذين يراد اغتيالهم.

ويذكر تقرير ورد في "فورين ريبورت" التي تصدرها مجلة "جينز" البريطانية، أنّ الوحدة زرعت أجهزة تنصت وكاميرات وألغامًا في مناطق حساسة ومختلفة من القطاع، وذلك لأن الاحتلال يعمل من أجل السيطرة على جميع خطوط الهاتف وأنظمة الاتصال في القطاع بشكل يمكن قوات الاحتلال من رصد أيّ تحرك في غزة.

وبعد ثورات الربيع العربي، طرأ تغير على عمل الوحدة، يقول المعلق العسكري الإسرائيلي يوآف ليمور إن: "الوحدة باتت تركز معظم اهتمامها وعملها على متابعة مواقع التواصل الاجتماعي التي يرتادها الشباب العربي، وبصفة خاصة فيسبوك وتويتر، وذلك لرصد التحولات السياسة والاجتماعية والنفسية التي طرأت على الشباب العربي مع هذه الثورات، وإعداد تصورات حول كيفية التعامل مع الشباب العربي في المراحل المقبلة، حتى لا تتعرض إسرائيل للمفاجأة كما حدث مع تفجر الثورات العربية".

ودفع الكشف عن عمليات التنصت الواسعة التي تقوم بها وكالة الأمن القومي الأمريكية على حلفاء للولايات المتحدة، معلقين وكتابًا إسرائيلين إلى تسليط الأضواء على الدور الذي تقوم به "وحدة 8200" التي تعد ذراع التنصت الإسرائيلي الهائل.

وأكد المعلق العسكري الإسرائيلي عمير رايبوبورت أن الدور الذي تقوم به وحدة 8200، التابعة لشعبة الاستخبارات العسكرية الإسرائيلية (أمان)، قد جعل إسرائيل ثاني أكبر دولة في مجال التنصت في العالم، بعد الولايات المتحدة.

وفي مقال نشره على موقع صحيفة معاريف الإسرائيلية، أوضح رايبوبورت أن التقدم الهائل الذي حققته إسرائيل في مجال صناعة التقنيات المتقدمة قد وظف بشكل كبير في تطوير وتوسيع عمليات التنصت التي تقوم بها الوحدة، مشيرًا إلى وجود دور بارز لشركات القطاع الخاص في رفد الوحدة باختراعات تعزز من قدرات التنصت.

وأشار رايبوبورت إلى أن الحواسيب المتطورة التابعة لوحدة 8200 قادرة على رصد الرسائل ذات القيمة الاستخباراتية من خلال معالجة ملايين الاتصالات ومليارات الكلمات.

وفي ذات السياق كشف تحقيق أعده المعلق العسكري يوآف ليمور النقاب عن أن تحولًا قد طرأ على عمل الوحدة التي يقودها ضابط كبير برتبة عميد، منذ أن تفجرت الثورات العربية.

وأشار في تحقيقه الذي نشر على موقع صحيفة "إسرائيل اليوم" إلى أن وحدة 8200 باتت تهتم بمتابعة مواقع التواصل الاجتماعي التي يرتادها الشباب العربي لا سيما فيسبوك وتويتر، لبناء تصور بشأن التحولات التي يمكن أن تطرأ في العالم العربي، حتى لا تتعرض إسرائيل للمفاجأة كما حدث مع تفجر الثورات العربية.

ولفت ليمور إلى أن وحدة "8200" مسؤولة أيضًا عن قيادة الحرب الإلكترونية في الجيش الإسرائيلي، علاوة على قيامها بعمليات تصوير، فضلًا عن أن الضباط والجنود العاملين في إطارها يتولون القيام بعمليات ميدانية أثناء الحروب والعمليات العسكرية.

وأوضح ليمور أن الوحدة تضم بين صفوفها ضباطًا وجنودًا يقومون بمرافقة قوات المشاة أثناء العمليات العسكرية والحروب، حيث يتولون جمع المعلومات الاستخبارية التكتيكية من أرض المعركة، مشيرًا إلى أن الوحدة لعبت دورًا أساسيًا في الحرب الإلكترونية ضد المشروع النووي الإيراني، وأسهمت في تطوير فيروس "ستوكسنت"، الذي استهدف عام 2009 المنظومات المحوسبة التي تتحكم في

أجهزة الطرد المركزية المسؤولة عن تخصيب اليورانيوم في المنشآت النووية الإيرانية، مما أدى إلى تعطيلها.

ودلت الوثائق الجديدة التي كشف عنها مخزن الأرشيف الرسمي الإسرائيلي مؤخرًا بمناسبة مرور أربعين عامًا على حرب 1973، أن الوحدة مسؤولة عما بات يعرف بـ"الوسائل الخاصة"، والتي تتضمن زرع أجهزة تنصت في مكاتب ومرافق حيوية في عمق البلدان العربية، خصوصًا البلدان التي تكون في حالة عداء مع إسرائيل.

وتعمل وحدة 8200 بشكل وثيق مع وحدة "سييرت متكال"، الوحدة الخاصة الأكثر نخبوية في الجيش الإسرائيلي والتي تتبع مباشرة لرئيس شعبة الاستخبارات العسكرية، وبالإضافة إلى تخصصها في تنفيذ عمليات الاغتيال التي تتم في العالم العربي، فإن "سييرت متكال" تلعب دورًا مركزيًا في جمع المعلومات الاستخبارية عبر زرع أجهزة تنصت وتصوير، بناءً على تنسيق مسبق مع وحدة 8200.

وتتنافس شركات التقنيات المتقدمة الرائدة في إسرائيل على استيعاب الضباط والجنود الذين يتسرحون من الخدمة في هذه الوحدة ""8200 وذلك بسبب قدراتهم الكبيرة في المجال التقني.

وذكر تقرير عرضته قناة التلفزة الإسرائيلية العاشرة مؤخرًا إلى أن الخدمة في هذه الوحدة 8200 أصبحت "جواز سفر في نظر الشباب الإسرائيلي"، لكي يصبحوا من أصحاب الملايين بسبب استيعابهم في شركات التقنيات الرائدة، أو بفعل قيامهم بتدشين شركات.

ماذا تعرف "سرب نخشون"؟

كشفت دولة الاحتلال الإسرائيلي عن وحدة نحشون، وقالت بأنه ذراعها للتجسس الإلكتروني، يغطي العالم العربي، ويستخدم السرب طائرات "غولفستريم" الأمريكية، التي تحمل في داخلها منظومات تجسس، ومراقبة، وقيادة، وسيطرة، وهي طائرات في قمة التطور والتقدم.

ويشكل السرب الجوي وحدة قيادة ومراقبة محمولة، حيث تمتلك دولة الاحتلال سربين من هذا الطراز، الأول ينتشر شمال دولة الاحتلال، والثاني يتخذ من المنطقة الجنوبية قاعدة له.

وتستهدف وحدة "سرب نخشون" مصر على وجه الخصوص، حيث تولي دولة الاحتلال التجسس على مصر أهمية كبيرة، فقد أكدت وسائل إعلام إسرائيلية أن الوحدة 9900 مسؤولة أيضًا عن مراقبة تحركات الجيش المصري في سيناء، وتقوم بإمداد قيادة جيش الاحتلال بأية تطورات في شبه جزيرة سيناء، وكان قائد السرب الجوي الاستخباري الإسرائيلي قد كشف عن ارتفاع عدد المهام التي نفذها السرب مؤخرًا.

من أشكال التجسس الإلكتروني لدى إسرائيل أيضًا، الرصد والتنصت على أجهزة الاتصال السلكية

والاسلكية، وتعد واحدة من أشهر تلك القضايا ما كشف حول قيام شركة موبينيل المصرية بإنشاء محطات تقوية بالقرب من حدود مصر مع دولة الاحتلال الإسرائيلي، ساهمت هذه المحطات بقوة في إيصال ترددات الاتصالات المصرية والتقاطها، فحسب تقرير النيابة المصرية فإن توجيه معظم الهوائيات الخاصة بشركة موبينيل في منطقة العوجة في جهة الجانب الإسرائيلي مكن من اختراق الشبكة المصرية وتمرير المكالمات الدولية، كما أنه سهل عمل شبكة التجسس في متابعة الاتصالات الدولية والتجسس على شبكات المحمول المصرية واختراق الأمن القومي.

وذكر تقرير نشرته جريدة الدستور المصرية "أن بعض محطات التقوية للشبكة موجهة بزاوية 75 درجة داخل الحدود المصرية باتجاه منطقة صحراوية خالية من السكان وأن تلك الجهة تجعل إشارة الاتصالات المصرية تدخل إسرائيل بنسبة محدودة بنسبة 10 كليومترات داخل إسرائيل".

تدرك دولة الاحتلال الإسرائيلي مدى أهمية التقنية في تعقب شبكات الهاتف ومزودي الإنترنت، لذا تعمل شركات التجسس الإسرائيلية على تطوير إمكانياتها في مجال تقنية التجسس، وهي لا تكف عن عقد الصفقات التكنولوجية مع الدول الكبرى.

ويؤكد تقرير نشره الملحق الاقتصادي لصحيفة "يديعوت أحرنوت" العبرية أن تعاونًا وثيقًا يجري بين شركتي البرمجة الإسرائيلية "فارينت يسرائيل" و"نايس سيستمز" وشركة البرمجة الإيطالية العملاقة بهدف التعاون في تصدير برامج تجسس خبيثة، ويؤكد التقرير أن "شركات برمجة إسرائيلية قامت ببيع برامج تجسس خبيثة للكثير من مخابرات العالم ومن بينها مخابرات دول عربية بهدف التجسس على حواسيب وهواتف شعوبها".

ويذكر التقرير أن صادرات هذه الشركات وبالتعاون مع الشركة الإيطالية هي: برامج مثل برنامج "دي فينشي" وهو برنامج حصان طروادة يمكن مستخدميه من السيطرة عن بعد على مئات الآلاف من الحواسيب والهواتف وتشغيل الميكروفون والكاميرا فيها والسيطرة على كل حركة فيها بما في ذلك موقع الجهاز والمحادثات الصادرة والواردة، كما أنه بإمكان هذه البرامج تجاوز أنظمة التشفير وجمع المعلومات من أي جهاز ومواصلة متابعة أهدافهم حتى لو كانت خارج نطاق عمل هذه الشركات.

رابط المقال : https://www.noonpost.com/13821/