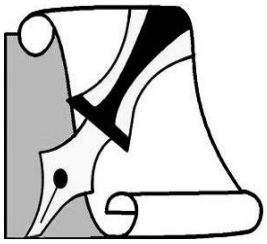
مركز باحث للدراسات الفلسطينية والاستراتيجية

التقدير نصف الشهري

تحليل للتطورات السياسية والأمنية في «إسرائيل»

www.bahethcenter.net
Email: baheth@bahethcenter.net
bahethcenter@hotmail.com



باحث للدراسات
الفلسطينية والاستراتيجية

تحليل نصف شهري للتطوّرات السياسية والأمنية في «إسرائيل»

أهداف المركز الرئيسية:

1 إعادة فلسطين إلى موقعها الحقيقي كقضية مركزية للأمة.

2 الترويج للقيم الجهادية والنضالية في إطار استراتيجية تحرير فلسطين.

3 بناء علاقة متينة مع النخب والشخصيات المعنية بالقضية الفلسطينية.

4 إصدار دراسات وأبحاث وتقارير ذات بعد استراتيجي وتحليلي.

الحرب "التجسسية الإلكترونية الإسرائيلية"

1 – مدخل:

على مرّ السنوات الثلاث الماضية، سلَّط تورُّط نظام "بيغاسوس" التجسسي الإسرائيلي الضوء على الشركة الإسرائيلية المصنّعة NSO، ونشاطها وتعاونها مع الأنظمة القمعية والديكتاتورية في العالمين الغربي والعربي، والتي تستفيد من تقنيات الشركة في تتبُّع أهم معارضيها واختراق هواتفهم وأجهزتهم الإلكترونية الشخصية. وبينما تُنكر الشركة دائماً ذلك التعاون، مؤكِّدة أن سياستها الرسمية تضمن مكافحة الأنشطة الإجرامية بأنواعها كافة، فإن تقارير مختلفة تؤكِّد باستمرار تورُّطها الدائم في هذه الحلقة التجسسية، ولم يكن آخرها تحذير أصدره عملاق البحث والتقنية "غوغل" لمُستخدمي نظام "أندرويد" ذائع الصيت للهواتف المحمولة بتوخّي الحذر، لأن هواتفهم مُعرَّضة للاختراق من قِبل تقنيات "إن إس أو" (NSO).

لا يمتلك شباب وفتيات "إسرائيل" اختياراً بعد بلوغهم سنّ الثامنة عشرة سوى أداء الخدمة العسكرية الإلزامية في جيش الاحتلال؛ وهي قاعدة لم يكن المجنّد "شيليف هوليو" استثناءً منها، شأنه شأن زملائه الذين خدم معهم في الصفوف الأمامية حول قطاع غزة وغيره من الأراضي المحتلة. وعلى الرغم من أنه لم يكن مرتبطاً بالصناعات التقنية أو الأمن السيبراني في حياتيه المدنية أو العسكرية، فإن الأعوام القليلة لما بعد إنهائه الخدمة العسكرية كانت فاصلة في تحوّله من شاب عادي إلى شريك مؤسّس في واحدة من أكثر شركات الأمن السيبراني الإسرائيلية إثارة للجدل في العالم. فقد هدف "هوليو" بعد الخدمة العسكرية إلى الدخول في قطاع التجارة الإلكترونية الواسع وصناعة ثروته الشخصية؛ وهو شيء تخصَّص فيه الجنود الإسرائيليون بخبرات إما عسكرية وإما تقنية مُكتَسبة من أداء الخدمة في الصفوف الأمامية للجيش، أو في وحدات النخبة من أمثال الوحدة 8200 وجهاز "أمان" وغيرهما. وفي حين لم يمتلك هوليو أي خبرات تقنية، كما أخبر صحيفة "يديعوت أحرونوت" الإسرائيلية بنفسه، فإن هذا لم يمنعه هو وزميليه "نيف كارمي" و"عومري ليفي" من تأسيس شركة التقنية المتخصّصة في الأمن السيبراني "NSO Group" التي نشأت على أنقاض شركة "كوميوني–تك" (CommuniTech)، التي كان قد أسّسها من قبل كلٌّ من هوليو وليفي لمساعدة شركات الهواتف الذكية الجديدة على العالم في حينه؛ ففي وقتٍ كانت فيه تلك الصناعة الناشئة تحتاج إلى الكثير من وقت شركات الهاتف لتدريب وتعريف عملائها بكيفية تثبيت البرامج الأساسية الخاصة بالتعامل مع منتجاتها، خرجت شركة "كوميوني– تك" بحلٍ يُمكِّن شركات الهاتف من إرسال رابط إلى عملائها، ومن خلاله تقوم الشركات بالولوج إلى الهاتف نفسه وتثبيت برامجها، بما يُوفِّر

الوقت والجهد على الجميع. وقد استلزم الأمر قليلاً من الوقت بعد ذلك لتتحوَّل "كوميوني– تك" إلى "إن إس أو" NSO؛ بعدما هجر كلٌّ من هوليو وليفي الأولى لتأسيس الثانية، وكذا ليتحوَّل المُنتَج الهادف لمساعدة الناس إلى مُنتَج يتجسَّس عليهم، بعدما انتبه الشريكان للفكرة البسيطة القائلة إنه يمكن فعل الكثير بهاتف محمول نمتلك القدرة على الولوج إلى بياناته كافة بدون عِلم صاحبه، وبمقابل ماديّ أكثر بكثير.

كانت البداية من المكسيك، حيث زعم مؤسّسا "إن إس أو" (NSO) أن برنامج "بيغاسوس" (Pegasus)، وهو مُنتَجهم الرئيس، ساعد في القضاء على العديد من الشخصيات الأساسية الفاعلة في عصابات المخدّرات الكبرى هناك؛ ويمتلك "بيغاسوس" القدرة على التسلُّل إلى الهواتف المُستهدَفة من خلال رابط مزيّف يتم إرساله إلى الهاتف، ومن خلاله يتم الولوج لبيانات صاحب الهاتف كافة، بداية من الرسائل والمكالمات، ومروراً بالموقع الجغرافي الخاص به، وليس انتهاءً باستخدام الكاميرا والميكروفون لتسجيل المحادثات والحوارات التي تتم في نطاقه؛ ثم أصبحت تقنيّة "بيغاسوس" بعد ذلك قادرة على التحدّث عن نفسها في أرجاء العالم كافة، خاصة في دولتَيْ الإمارات العربية المتحدة والسعودية، حيث استُخدمت التقنية لتعقُّب الناشط الحقوقي الإماراتي الشهير أحمد منصور عام 2016 والقبض عليه، ثم في مقتل صحافي "الواشنطن بوست"، السعودي المعارض "جمال خاشقجي"، في قنصلية بلاده باسطنبول بتركيا. ومن ثمّ نال "بيغاسوس" شهرته كإحدى أهم وسائل التجسس الإلكتروني، خاصة بالنسبة للأنظمة الأوتوقراطية في الشرق الأوسط والعالم.

2 – انتهاك حقوق الإنسان:

"إدوارد سنودن"، العميل السابق بوكالة المخابرات الأميركية، لم يجد صعوبة في وصف "إن إس أو" (NSO) باعتبارها "الأسوأ من بين أسوأ" الشركات في مجال صناعات الأمن السيبراني، وذلك بسبب الاستخدام المُكثَّف لتقنياتها في انتهاكات حقوق الإنسان للنشطاء البارزين حول العالم. وقد دفع الاستنتاج نفسه منظمة العفو الدولية للبدء في اتخاذ الإجراءات القانونية اللازمة لدفع الحكومة الإسرائيلية لإلغاء ترخيص التصدير الخاص بتقنيات "إن إس أو" (NSO)، ومنعها من التربُّح من "القمع الذي ترعاه الدولة"، كما وصفته "مارغريت ساترتويت"، مديرة كليّة الحقوق بجامعة نيويورك. وفي مجال ارتكاب الجرائم عبر الاستفادة من تكنولوجيات الذكاء الاصطناعي، استخدم الجيش الإسرائيلي برنامج تحديد الأهداف التلقائي "غوسبيل" لأول مرّة في قطاع غزة، حيث ضرب 15 ألف هدف في أول 35 يوماً من الهجمات المتوحشة على مدن القطاع؛ وهذا الرقم أعلى بكثير من عدد الأهداف التي ضربها في العمليات السابقة، حين تمكّن من ضرب ما يقرب من 6 آلاف هدف خلال الصراع الذي استمر 51 يوماً عام 2014. ويمتلك "غوسبيل" القدرة على اتخاذ القرار، ويتمتع بخاصيّة القتل والتدمير بغضّ النظر

عن عدد الأهداف؛ "وبالتالي فإن عدد الضحايا يمكن أن يتراوح من صفر إلى مليون"، علماً بأن الاستخبارات الإسرائيلية لديها مخزون ضخم من البيانات، ومجموعة واسعة من المعلومات عن المدنيين الفلسطينيين؛ وهي قصفت المستشفيات، برغم امتلاكها معلومات كاملة عن هؤلاء الذين يعيشون في قطاع غزة والمباني والجامعات والمدارس ومراكز الإغاثة والمصانع ومنشآت البنية التحتية. و"إسرائيل" تعمل باستمرار على تطوير تكنولوجيا الذكاء الاصطناعي، بحيث بات الفلسطينيون وكأنهم يعيشون في مختبر بشري كبير يسمح للقادة الإسرائيليين باختبار أسلحة هذه التكنولوجيا التي تستفيد منها شركاتها مادياً ومعنوياً، ومن ضمنها برنامج Fire Factory الذي استُخدم منذ عام2019؛ وهو نظام له ميزات مثل إنشاء الأهداف وتحديد الكمية المناسبة من الذخيرة، واقتراح جدول زمني للغارات الجوية. وقد تم استخدامه بشكل واسع لأول مرة في حرب 2021، التي استمرت 11 يوماً، وتم الوصول إلى 150 هدفاً بهذه التقنية. ومع تقدّم هذه التكنولوجيا، يزداد نهم "إسرائيل" للإجرام والقتل. وستكون لتقنيات الذكاء الاصطناعي هذا عواقب خطيرة للغاية، ليس على الفلسطينيين والعرب فحسب، بل على البشرية بأكملها. ولن تكون هناك بأي حال من الأحوال قوّة يمكنها ردع هذه التقنيات، مما يزيد من أهمية قيام الحكومات والبرلمانات والمنظمات غير الحكومية ومنظمات حقوق الإنسان بسنّ قوانين وتشريعات تضبط وتجرّم استخدام أسلحة الذكاء الاصطناعي الخطيرة هذه، التي تُحدِث مآسٍ انسانية لا حصر لها وغير مسبوقة بفظاعتها.

3 – مرحلة التأسيس:

تعود فكرة تأسيس منظمات استخباراتية إسرائيلية إلى ما قبل العام 1948. ففي تشرين الثاني /نوفمبر 1915، أسّس المهندس الزراعي اليهودي ذو الأصول الرومانية، آهارون آرونسون، أول وحدة استخبارات سريّة في فلسطين، وكانت تخدم وكالة تجسس بريطانية أطلِق عليها اسم "نيللي" (NILI). وخلال الحرب العالمية الأولى، جمعت وحدة (NILI) المعلومات الاستخباراتية للبريطانيين تحت ستار الأعمال الزراعية لشركة آرونسون، فقدّم الجواسيس معلومات قيّمة للضبّاط البريطانيين حول الأوضاع الداخلية، والسكك الحديدية، والطرق المحتملة التي قد يستخدمها البريطانيون لاحتلال فلسطين. وتستطيع الحواسيب المتطورة التابعة للوحدة رصد الرسائل ذات القيمة الاستخباراتية من خلال معالجة ملايين الاتصالات ومليارات الكلمات والفاكسات، وكذلك المنشورات على مواقع التواصل الاجتماعي؛ بل والتجاوب معها أيضاً بإرسال مجموعة من الرسائل يحدّدها ضبّاط متخصّصون. وتطوّر الأمر إلى تحليل الرسائل وتحويلها إلى شفرات، وتنسيقها وإرسالها إلى القسم المختص في الوحدة للتعامل معها، وتوجيه آلاف الرسائل بضغطة زر من خلف الشاشة. ويُعتبر التنصّت على أجهزة الاتصال السلكية

واللاسلكية من المهام الأساسية للوحدة «8200»؛ فالهواتف الأرضية والنقّالة وأجهزة اللاسلكي يتم التنصّت عليها بشكل دائم؛ والذي يساعد الوحدة على أداء مهمتها بشكل تام، هو حقيقة أن السلطات هي التي أقامت شبكة الاتصالات في الضفة الغربية وقطاع غزة. وهذه الوحدة تستهدف كل دول العالم، خاصة المنطقة العربية وإيران وأوروبا؛ وهي مسؤولة عن حرب الشائعات وتغييب وعي الشباب العربي عبر الصفحات المزيّفة؛ وتضع الآن قضية التطبيع على أولويات عملها.

في عام 2010، كتبت الصحيفة الفرنسية "لوموند ديبلوماتيك" أن الوحدة 8200 تُدير قاعدة SIGINT الكبيرة في النقب، وهي إحدى أكبر قواعد التنصت في العالم؛ وهي قادرة على مراقبة المكالمات الهاتفية ورسائل البريد الإلكتروني وغيرها من الاتصالات، في جميع أنحاء الشرق الأوسط، أوروبا، آسيا، إفريقيا، بالإضافة إلى تتبّع السفن.

وبحسب ما ورد، تحتفظ الوحدة 8200 أيضًا بمراكز استماع سريّة في السفارات الإسرائيلية في الخارج، وتنقر على الكابلات البحرية، وتحتفظ بوحدات استماع سريّة في الأراضي الفلسطينية، ولديها غولف ستريم طائرة مزوّدة بمعدّات مراقبة إلكترونية.

"يائير كوهين"، القائد الأسبق للوحدة بين عامي 2001 و2005، أوضح أن إسرائيل تضم للوحدة كل من تظهر عليه علامات الذكاء والإبداع مهما كان سنّه "، بمعدّل 8200 مجنّداً سنوياً"؛ ومن هنا التسمية. وتقدّم لهم التدريب والتأطير اللازم لقيادة الحرب الإلكترونية باستخدام البيانات الشخصية. وأضاف "كوهين" أن 50% من المعلومات الاستخباراتية الإسرائيلية تأتي عن طريق هذه الوحدة، ولا توجد عملية تجسسية واحدة لا تشارك فيها الوحدة، مشيراً إلى أنهم يجمعون المعلومات من التفاعلات على الصفحات الإسرائيلية الناطقة بالعربية. ولفت إلى أنهم يستخدمون تلك المعلومات لاستهداف المجتمعات المعادية لإسرائيل بالدعاية الموجّهة، ولاستغلال نقاط ضعف المجتمع المستهدف لإلحاق الهزيمة النفسية والثقافية به. وأكّد عمير رابابورت، المعلّق العسكري الإسرائيلي في صحيفة معاريف، أن الدور الذي تقوم به الوحدة التابعة لشعبة الاستخبارات العسكرية الإسرائيلية "أمان"، قد جعل من إسرائيل ثاني أكبر دولة في مجال التنصّت في العالم بعد الولايات المتحدة. وفي مقال نشره على موقع صحيفة "معاريف"، أوضح أن التقدم الهائل الذي حقّقته إسرائيل في مجال صناعة التقنيات المتقدمة قد وظّف بشكل كبير في تطوير وتوسيع عمليات التنصّت التي تقوم بها الوحدة، منوّهاً بالدور البارز لشركات القطاع الخاص في رفد الوحدة باختراعات تُعزّز من قدرات التنصّت. وأشار رابابورت إلى أن الحواسيب المتطورة التابعة للوحدة قادرة على رصد الرسائل ذات القيمة الاستخبارية من خلال معالجة ملايين الاتصالات ومليارات الكلمات. وفي السياق ذاته، كشف تحقيق أعدّه يوآف ليمور، المعلّق العسكري في الصحيفة، النقاب عن أن تحوّلاً قد طرأ

على عمل "الوحدة 8200"، التي يقودها ضابط كبير برتبة عميد، منذ أن تفجّرت الثورات العربية. ونوّه ليمور في تحقيقه الذي نُشِر على موقع صحيفة "إسرائيل اليوم" إلى أن "الوحدة 8200" باتت تهتم بمتابعة مواقع التواصل الاجتماعي التي يرتادها الشباب العربي، لا سيما "فيسبوك" و "تويتر" – إكس، لبناء تصوّر بشأن التحوّلات التي يمكن أن تطرأ في مجتمعات العالم العربي، حتى لا تتعرض إسرائيل للمفاجأة كما حدث مع تفجّر الثورات العربية.

وبخلاف "أشلون"، ذراع التنصّت التابع للمخابرات الوطنية الأمريكية التي تتخصّص فقط في مجال التنصّت الإلكتروني من قواعد ثابتة، فإن ليمور يشير إلى أن "الوحدة 8200" مسؤولة أيضاً عن قيادة الحرب الإلكترونية في الجيش الإسرائيلي؛ علاوة على قيامها بعمليات تصوير؛ فضلاً عن أن الضبّاط والجنود العاملين في إطارها يتولّون القيام بعمليات ميدانية أثناء الحروب والعمليات العسكرية. وأوضح ليمور أن الوحدة تضم بين صفوفها ضبّاطاً وجنوداً يقومون بمرافقة قوات المشاة أثناء العمليات العسكرية والحروب، حيث يتولّون جمع المعلومات الاستخبارية التكتيكية من أرض المعركة. وأشار ليمور إلى أن "الوحدة 8200" لعبت دوراً أساسياً في الحرب الإلكترونية ضد المشروع النووي الإيراني، مشيراً إلى أن الوحدة أسهمت في تطوير فيروس "stuxnet"، الذي استهدف عام 2009 المنظومات المحوسبة التي تتحكم في أجهزة الطرد المركزية المسؤولة عن تخصيب اليورانيوم في المنشآت النووية الإيرانية، مما أدّى إلى تعطيلها. ودلّت الوثائق الجديدة التي كشف عنها مخزن الأرشيف الرسمي الإسرائيلي أخيراً بمناسبة مرور 40 سنة على حرب 1973، أن الوحدة مسؤولة عمّا بات يُعرف بـ "الوسائل الخاصة"، والتي تتضمّن زرع أجهزة تنصّت في مكاتب ومرافق حيوية في عمق البلدان العربية، لا سيما البلدان التي تكون في حالة عداء مع إسرائيل. وتعمل "الوحدة 8200" بشكل وثيق مع وحدة "سييرت متكال"، الوحدة الخاصة الأكثر نخبوية في الجيش الإسرائيلي، والتي تتبع مباشرة لرئيس شعبة الاستخبارات العسكرية. وبالإضافة إلى تخصّصها في تنفيذ عمليات الاغتيال التي تتم في قلب العالم العربي، فإن "سييرت متكال" تلعب دوراً مركزياً في جمع المعلومات الاستخبارية عبر زرع أجهزة تنصّت وتصوير، بناءً على تنسيق مسبق مع "الوحدة 8200".

من ناحية أخرى، تتنافس شركات التقنيات المتقدمة الرائدة في إسرائيل على استيعاب الضبّاط والجنود الذين يتسرّحون من الخدمة في "الوحدة 8200" بسبب قدراتهم الكبيرة في المجال التقني. وذكر تقرير عرضته قناة التلفزة الإسرائيلية العاشرة أخيراً أن خرّيج "الوحدة 8200" أصبح "رديفاً لكلمة عبقري"، مشيرة إلى أن الخدمة في هذه الوحدة أصبح "جواز سفر في نظر الشباب الإسرائيلي" لكي يصبحوا من أصحاب الملايين بسبب استيعابهم في شركات التقنيات الرائدة، أو بفعل قيامهم بتدشين شركات خاصة لهم.

والوحدة هي ما يعادل وكالة الأمن القومي الأمريكية، وهي مؤسسة النخبة، بحيث يمكن لخرّيجيها، بعد ترك الخدمة، استثمار مهارات التطفل والقرصنة المتطورة والحديثة لديهم في وظائف في إسرائيل، أو وادي السليكون، أو ممر التكنولوجيا الفائقة في بوسطن. ومؤلّفا كتاب "أمّة الشركات الناشئة"، الكتاب المهم الذي ظهر في عام 2009 عن ثقافة الشركات الناشئة في إسرائيل، وصفا الوحدة 8200 ووحدات النخبة الأخرى في الجيش الإسرائيلي بأنها "المؤسسة الإسرائيلية التي تعادل جامعات هارفارد، وبرنستون، ويل".

تتجسّس الوحدة 8200 أيضاً على الفلسطينيين الذين يعيشون تحت الاحتلال الإسرائيلي في الضفة الغربية، أو تحت الحصار البحري والجوي في قطاع غزة، وفقاً لتسريب "ويكيليكس" الذي أحدث ضجّة قبل أعوام.

في خطاب مفتوح في أيلول (سبتمبر) 2014، نشرته صحيفة "يديعوت أحرونوت" الإسرائيلية وبُثّ على "القناة 10"، كشفت مجموعة مكوّنة من 43 شخصاً في الخدمة، وجنود احتياط سابقون في الوحدة 8200، عمّا قالوا إنها كانت تكتيكات تجسس قسرية يجري استخدامها على الفلسطينيين الأبرياء، بما في ذلك مجموعة من المعلومات الجنسية والمالية المحرجة وغيرها من المعلومات الشخصية.

4 – حيثيات الوحدة:

يؤكّد دانيال كوهين، الخبير من "معهد دراسات الأمن القومي" في تل أبيب، أن إسرائيل تحتل الطليعة في العالم بالنسبة لكلّ ما يتعلق بمجال الإنترنت". ويشرح كوهين أن هذا التقدم يأتي أساساً من دينامية عناصر سابقين من وحدات النخبة في الجيش الإسرائيلي، مثل الوحدة "8200" المتخصصة في مجال الحرب الإلكترونية.

الوحدة الاستخباراتية "8200" هي من أبرز زبائن شركة NSO المصنّعة لتقنية التجسس بيغاسوس؛ وهي وحدة خاصة تابعة للمخابرات العسكرية الإسرائيلية ومسؤولة عن التجسس وقيادة الحرب الإلكترونية، حيث تتعقب الأعداء المحتملين لإسرائيل، وتحاول التحكم في الرأي العام على منصّات التواصل الاجتماعي. فالواقع الجديد في المنطقة تطلّب تحركًا أكثر من الاستخبارات الإسرائيلية، وتحديدًا من الوحدة 8200، عندما يتعلق الأمر بوسائل التواصل الاجتماعي، حيث أصبحت تُراقب ساحة الإنترنت بشكل أكبر ومختلف، الأمر الذي دفع إسرائيل إلى زيادة الاستثمار في الاستخبارات الإعلامية الجديدة. وإلى جانب الاستماع التقليدي لوسائل الإعلام وقراءة الصحف، يجلس جنود وحدة «حتساف» التابعة للوحدة 8200 على موقع التواصل الاجتماعي إكس «تويتر» ويشاهدون مقاطع الفيديو على موقع «يوتيوب»، ويتابعون الأنشطة في مجموعات «فيس بوك» و«إنستاغرام». كما أنهم يستخدمون التطبيقات ويجمعون المعلومات من المدوّنات. ومن خلال تلك المنشورات

التي لا تخضع لقواعد الرقابة وغير مشفّرة، يمكن للجيش الإسرائيلي إثراء لوحته الاستخباراتية حول المزاج الشعبي العام في العالم العربي.

تأسّست الوحدة 8200 في عام 1952 باستخدام فائض بدائي من المعدّات العسكرية الأمريكية. وقد أسّسها جهاز الاستخبارات العسكرية «أمان» بغرض تقديم رؤية استخبارية متكاملة مع المعلومات التي توفّرها المصادر البشرية القائمة تجاه الأهداف العربية حول العالم، وتعتمد على عدة طرق في العمل وهي: الرصد، والتنصت، والتصوير ، والتشويش، والتفكيك، والاعتراض، والتحليل، والترجمة، وإشعال الفتن والأزمات في المجتمعات العربية والإسلامية. ويتطلب هذا النوع من المهام مجالاً واسعاً من وسائل التقنية المتقدمة – كونه يستهدف ملايين الأشخاص في الوقت نفسه– ويقوم مجمع الصناعات العسكرية الإسرائيلية بتطوير أجهزة إلكترونية بناءً على طلبات خاصة من القائمين على الوحدة «8200»، التي تقودها مجموعة صغيرة من الضبّاط وتضم آلاف المجنّدين؛ وكانت تُسمّى في الأصل وحدة المخابرات الثانية، ثم وحدة المخابرات رقم 515. وفي عام 1954، انتقلت الوحدة من يافا إلى قاعدتها الحالية عند تقاطع غليلوت. وتراقب الوحدة وتجمع المخابرات العسكرية – المعلومات ذات الصلة من: التلفزيون ، الراديو ، الصحف ، والإنترنت . وتمثّل ترجمة العناصر المختلفة جزءًا ممّا يسمّى "الذكاء الأساسي"، والذي تقوم الوحدات بجمعه. ووفقًا لتقارير وسائل الإعلام، توفّر الوحدة أكثر من نصف المعلومات الاستخباراتية الإجمالية لمجتمع الاستخبارات الإسرائيلي .

تتكوّن الوحدة بشكل أساسي من مُجنّدين تتراوح أعمارهم بين 18 و 21 عاماً. وعادة ما يتم الاختيار والتجنيد في الوحدة في سن 18 من خلال عملية فحص الجيش الإسرائيلي بعد المدرسة الثانوية. ومع ذلك، تقوم الوحدة أيضًا باستكشاف المجنّدين الأصغر سنًا المحتملين من خلال دروس الكمبيوتر بعد المدرسة. تعمل فصول الكمبيوتر هذه بعد المدرسة، والتي تدرّس مهارات الترميز والقرصنة الحاسوبية لمن تتراوح أعمارهم بين 16 و 18 عاماً، في بعض الأحيان، كبرنامج تغذية للوحدة، حيث يتلقّى الطلاب خطابات دعوة من الجيش الإسرائيلي.

5– تطوّر الوحدة وآلية عملها:

كشف الصحافي النيوزلندي "نيك هاغر"، المتخصّص في مجال العلوم والتكنولوجيا والتنصّت الإلكتروني، في تحقيق نشره يوم الأحد 5 أيلول 2010، في صحيفة "لوموند دبلوماتيك"، النقاب عن أهم وأكبر قاعدة تجسس صهيونية مُقامة في منطقة غرب النقب، جنوب الكيان الصهيوني بفلسطين المحتلة. ووصف الصحافي، في تحقيقه الموسّع، القاعدة بأنها إحدى أكبر قواعد التنصّت الإلكتروني في العالم، مؤكّداً وجودها بالقرب من كيبوتس "إرويم"، وتُعتبر جزءاً مهماً من تجهيزات وحدات التنصّت المركزية التابعة للاستخبارات الإسرائيلية،

والمعروفة باسم الوحدة" 8200"، والمرتبطة مباشرة بقسم الاستخبارات العسكرية (أمان) التابع لجيش الاحتلال الصهيوني. وجاء في التحقيق بأن القاعدة تضم 30 برجاً هوائياً وصحوناً لاقطة من أنواع وأحجام مختلفة، مهمتها التنصّت على المكالمات الهاتفية واختراق العناوين الإلكترونية التابعة لحكومات أجنبية ومنظمات دولية وشركات أجنبية ومنظمات سياسية؛ إضافة إلى الأشخاص والافراد. وأهم أهداف القاعدة التجسسية، وفقاً للتحقيق: التنصّت على الاتصالات اللاسلكية ومراقبة حركة السفن في البحر المتوسط؛ إضافة إلى اعتبارها مركزاً مهماً لشبكات التجسس، عبر الكوابل البحرية التي تربط الكيان الصهيوني بدول أوروبا عبر مياه المتوسط؛ إضافة لامتلاك القاعدة محطات تنصّت سريّة تزيد من فاعليتها. ويتم نقل المعلومات التي تحصل عليها القاعدة المذكورة إلى قيادة خاصة تابعة للوحدة 8200 موجودة في مستوطنة هرتسيليا على البحر الأبيض المتوسط، لاستكمال العمل عليها وتمييزها؛ وبعد ذلك يجري تمرير المعلومات إلى قيادة الموساد الصهيوني ووحدات الجيش المعنيّة بذلك. ونقل الصحافي عن مُجنّدة سابقة كانت تعمل في صفوف الوحدة 8200 ضمن طاقم تحليل المعلومات، قولها بأن مهمتها كانت تتمثل باعتراض الاتصالات الهاتفية والرسائل الإلكترونية "الإيميل"، وترجمتها من الإنجليزية والفرنسية للغة العبرية، مضيفة: "لقد كنتُ أعمل في التعقّب والرصد والتشخيص وفرز المفيد من بين الاتصالات العادية والاعتيادية".

تمتلك الوحدة 8200 العديد من القواعد المنتشرة في فلسطين المحتلة، والمصنّفة كوحدات مركزية لجمع المعلومات تحمل اسم "سيغينت". وتعمل الوحدة المذكورة في مجالات: التنصّت، الاعتراض، التحليل، الترجمة، ونشر المعلومات المتوفّرة لديها، من خلال التنصّت على البث الإذاعي والاتصالات الهاتفية واعتراض الفاكسات والبريد الإلكتروني. وأكّد كاتب التحقيق بأن قاعدة التجسس في النقب تغطّي مناطق جغرافية واسعه جداً في الشرق الأوسط وقارّتي آسيا وأفريقيا، ما جعلها من حيث الأهمية موازية لقواعد مماثلة في العالم، مثل القواعد التابعة لوكالة الأمن القومي الأمريكي " NSA" التي تمتلك قاعدة ضخمة على الأراضي البريطانية، وقاعدة مماثلة في فرنسا باسم "GCHQ"، مع فارق وحيد بينها هو مدى سريّة القاعدة الإسرائيلية التي بقيت سراً غير معروف حتى نشر هذا التحقيق؛ فيما تُعتبر القواعد الغربية المذكورة واقعاً معروفاً منذ فترة طويلة.

من ناحية أخرى، وفي دراسة نشرها مركز الزيتونة للدراسات والاستشارات، تقول الباحثة فاطمة عيتاني، إن الوحدة 8200 نشأت قبل عام 1948 كمجموعة من الأشخاص الذين حاولوا تطوير مهاراتهم التكنولوجية بجمع وفك رموز الخصوم البريطانيين والعرب. وفي العام نفسه، أنشأ الجيش الإسرائيلي وحدة حرب إلكترونية في مدينة يافا، أُطلق عليها اسم شيفرة «الأرنب Rabbit»، وكانت مهمّتها التنصّت على المكالمات بين الفلسطينيين

وفكّ رموزها، في وقتٍ كانت الولايات المتحدة وبريطانيا والاتحاد السوفياتي من الدول القليلة التي باستطاعتها فك رموز وشيفرة الاتصالات.

واجهت الوحدة بعض المشاكل في بدايتها، كنقص الخبرة التقنية، ونقص القوى العاملة، وغيرها، فلجأت إلى تقنيات بدائية للتنصّت، ثم طوّرتها عام 1949. وفي العام 1950، حصلت الوحدة على ميزانية قدرها 15 ألف دولار، و110 آلاف دولار إضافية للمشتريات الإلكترونية من الخارج، وهو مبلغ ضئيل عند محاولة شراء أنظمة الكمبيوتر الأكثر تقدّماً. غير أن الوحدة، وحفاظاً على سريّة قدراتها الاستخباراتية، طوّرت تكنولوجياتها داخلياً؛ ولكن ظلّت قدراتها محدودة وبجنود عديمي الخبرة. وبحلول عام 1959، حصلت الوحدة على إمكانية الوصول إلى تقنيّة حوسبة أكثر تقدّماً، وذلك بعد أن أنشأت وحدة رفائيل RAFAEL في الجيش الإسرائيلي، المسؤولة عن تطوير الأسلحة، جهاز كومبيوتر أطلقت عليه اسم ايتسيك Itzik، والذي سمح بإجراء عمليات محاكاة على نطاق واسع؛ أي محاولة تنفيذ عملية ما في ظروف اصطناعية مشابهة إلى حد ما للظروف الطبيعية، وذلك بهدف دراسة النتائج المتوقعة. وفي عام 1960، اشترى الجيش الإسرائيلي جهاز كمبيوتر فيلكو Philco من الولايات المتحدة الأمريكية، وأنشأ «مركز أجهزة الكمبيوتر وإدارة السجلّات The Center for Computers and Mechanized Records» المعروفة باسم مامرامMAMRAM، مما جعل الوحدة 8200 من أفضل وحدات القرصنة الإلكترونية (الهاكرز Hackers) وفك الشفرات المعقّدة في العالم. واستخدم الجيش الإسرائيلي هذه القوّة الحاسوبية خلال حرب 1967، عندما تمكّنت من اعتراض وفك رموز الاتصالات الجويّة المصرية والسورية. وكان العام 1973م خطأً مفصلياً في تاريخ الوحدة، إذ ألحَق أسْر الضابط الإسرائيلي عاموس ليفينبرغ Amos Levenberg، المطّلع على أسرار حسّاسة جداً، في قبضة السوريين، وفشله في الوقوف أمام الحرب النفسية التي أدارها المحقّقون السوريون، ضرراً كبيراً بالاستخبارات الإسرائيلية، لاعترافه لهم بكلّ شيء يعرفه، كتنصّت «إسرائيل» على كافة وسائل البث العسكرية السورية، بما فيها الاتصالات التي تحصل بين الرئيس السوري وقادة الفرق، واختراق الأراضي السورية، وتثبيت أجهزة تنصّت كانت موصولة بكافة كابلات Cables الاتصالات السورية، والتي كانت بدورها تنقل كل المعلومات إلى قواعد الوحدة 8200.

6- منتسبو الوحدة:

لا يُعدّ الانضمام للوحدة "8200" شيئاً هيّناً. فالعرب في إسرائيل ممنوعون من الانضمام للجيش عامة، ووحدات الأمن السيبراني خاصة. ويقوم مجتمع الاستخبارات الإسرائيلي بجمع المعلومات، وتحديثها بشكل دائم، عن العناصر المتميزة في مجالات التقنية، من الشباب والفتيات الإسرائيليين في مرحلة الثانوية. ويشمل التدقيق

ومراحل اختيار المرشّحين للانضمام للوحدة اختبارات سنوية ونصف سنوية، في اللغات والعلوم والبرمجة والتفكير الإبداعي وسرعة البديهة، بالإضافة إلى الاختبارات الجسدية. وهناك أيضاً برنامج "مغا شميم" بجامعة "بن غوريون"، جنوب الكيان الغاصب، حيث يُمكن للمتميّزين من الشباب والفتيات الدراسة لـ3 سنوات، قد تؤهّلهم للالتحاق بالوحدة "8200". والعمل في هذه الوحدة يُعدّ حلماً لضبّاط الاحتلال، لأنها إحدى وحدات النخبة في سلاح المخابرات، وتعطي للمنتسب فيها منزلة معنوية كبيرة بمجرّد قبوله في إحدى مناصبها؛ فضلاً عن فرص العمل الخارجية، التي لا حصر لها، التي ستوفّرها الخدمة فيها.

تضم الوحدة مسارين للتخصص: الأول تحت اسم مسار "أوفيك"، ويسلكه المرشّحون ذوو القدرات العالية والبيانات المناسبة. ويتلقّى من يريد أن يسلك هذا التخصص تدريبات قبل بدء الخدمة العسكرية، فضلاً عن تعلّم اللغتين العربية والفارسية، اللتين تُظهر الوحدة اهتماماً خاصاً بهما من بين اللغات؛ كما أنه ليس هناك شرط المعرفة المسبقة بهذه اللغات، حيث تشمل التدريبات لغات ربما لم يعرفها المُرشّح من قبل. أما المسار الثاني، فهو مسار "ماتان"؛ ويتعامل هذا المسار مع البحث وتطوير المصادر. وسيكون المرشّحون المناسبون مؤهّلين لشغل منصب يجمع بين العمل التكنولوجي والعمل الاستخباري.

7- كيف توظّف "8200" إمكانياتها للتجسس؟

قبل سنوات قليلة، أثارت هذه الوحدة الكثير من التعليقات بسبب دورها في الحرب الإلكترونية، وبسبب ما تملكه من قدرات فائقة في مجال التكنولوجيا. كما أدلى المسؤولون الإسرائيليون باعترافات تفيد بتحوّل عمل الوحدة من الدفاع إلى الهجوم في مجال تكنولوجيا المعلومات. تنوّعت أدوات التجسس والتجنيد؛ ومن بينها استخدام الرسائل النصيّة، بهدف اختراق الهواتف المحمولة، وهو الأمر الذي تستخدمه أجهزة المخابرات في الدول المتقدمة. ولربما هذا الأمر ليس بجديد؛ لكن عندما يتعلق الأمر بشركة إسرائيلية بعينها وارتباطها بالوحدة "8200"، حيث تمكّنت شركة إسرائيلية خاصة، وهي "إن إس أو" (NSO) التي خدم مؤسّسوها في الوحدة، أن تكشف ثغرة في هواتف "آيفون"، التي تتمتّع بحماية قوية مقارنة بالهواتف المحمولة الأخرى، وطوّرت برنامجاً لاختراقها عن بُعد واستخدامها كأداة تجسس. ومما لا شك فيه أن هناك علاقة كبيرة بين الشركات الخاصة، التي تتولّى عمليات تطوير البرمجيات في إسرائيل والوحدة "8200"، خصوصًا أن مُديريها من خرّيجي تلك الوحدة؛ وهذا الأمر يتيح للاستخبارات الإسرائيلية استخدام تلك القدرات لصالح "إسرائيل"، عن طريق عملية التجسس التي تقوم بها الوحدة التي يتحدث معظم العاملين فيها باللغتين العربية والفارسية. ويؤكّد تلك الفرضية ما كشفته معاهد متخصصة بأن شركة "إن إس أو" وحدها استهدفت حوالي 180 شخصاً ببرامجها للتجسس خلال عامين فقط. ويوضح أفيفا

ليتان، الباحث والمحلّل بـ"مركز غارتنر" (Gartner Research)، ما يحدث، فيُخبرنا أن هذه الطفرة في صناعة الأمن السيبراني في إسرائيل "تُنسب لروّاد الأعمال ذوي الخلفيات العسكرية، الذين قضوا خدمتهم في وحدات النخبة الإسرائيلية المتخصصة في الأمن السيبراني، ثم جلبوا خبراتهم العسكرية إلى القطاع الخاص.

هذا التطوّر في العلاقة الوثيقة بين الجيش وشركات القطاع الخاص في إسرائيل، يُعتبر "غير محدود". فلا توجد قوانين تضع للمجنّدين حدوداً لما يمكن استخدامه، تقنياً أو من حيث المهارة، في سبيل حماية الأمن السيبراني الإسرائيلي. كذلك، فإن محاولة احتلال "إسرائيل" للضفة الغربية وقطاع غزة توفّر ما يُشبه ساحات تجارب واسعة ومجّانية وآمنة لاختبار التقنيات التي تستخدمها أو تطوّرها تل أبيب، وهو ما يجعلها جاهزة بصورة شبه مثلى للاستخدام الداخلي أو لتصديرها للعالم.

بالعودة إلى عام 2018، نجد أنه في إطار مواكبة لغة العصر للحفاظ على مستوى عمليات التجنيد عبر الإنترنت، فإن الوحدة جنّدت مجموعات من طلاّب المرحلة الثانوية للعمل على شبكات التواصل الاجتماعي؛ للحديث مع الجيل الجديد بأسماء مزوّرة وعربية في أغلب الأحيان، نظراً لاستهداف الجمهور العربي، وذلك لتسهيل المهمة وعدم ترك مجال للشك من الشخصية المستهدفة. وعن استخدام الوحدة لتطبيقات التواصل الاجتماعي، يقول أحد القادة السابقين: "يبدو أن العصر الجديد هو جنّة تكنولوجية للوحدة. فكلّ شخص لديه جهاز حاسوب، والجميع يتصفح الإنترنت ويُرسل رسائل البريد الإلكتروني، وكل شخص لديه هاتف محمول، وفيسبوك، ووتساب؛ وكل هذا يُنتج كماً لا نهائياً من المعلومات؛ يحتاج المهاجم فقط إلى تطوير الأدوات والأساليب لجمع هذه المعلومات وتحليلها".

8 – أكثر من فشل وأكثر من نجاح:

بعد أيام قليلة من بدء حرب تشرين الأول 1973، سقط "عاموس ليفنبرغ" في أيدي القوات السورية. وعلى الفور نقله السوريون إلى مكان مجهول لاعتصار ما يمكن منه. ولم يكن الأمر يحتاج إلى كثير من الجهود لإقناع "عاموس"، أحد أرفع ضبّاط الوحدة 8200، وأحد القلائل المالكين لتصريح أمني بالغ الخصوصية، بالإدلاء بما لديه. هندس ضبّاط التحقيقات السوريون حينها ببراعة سيناريو، أقنعوا "عاموس" من خلاله أن الجيوش المصرية والسورية قد وصلت تل أبيب بالفعل، وأن إسرائيل قد انتهت للأبد. ومع نقطة ضعف "عاموس" الضخمة "رهاب الأماكن المغلقة"، والضغط النفسي، وبراعة نسج سيناريو الانتصار الخيالي، وبذاكرة استثنائية ونادرة اشتُهر بها في أروقة الوحدة السيبرانية الإسرائيلية الأشهر، أدلى "ليفنبرغ" بكلّ ما لديه؛ وكان الأمر أشبه بالصاعقة: "كانت كل كلمة مهمة تصنع قراراً في سوريا تُسمع في إسرائيل".

يُوصَف "عاموس" في أروقة مجتمع الاستخبارات الإسرائيلي بأنه الرجل المُتسبِّب في "أكبر ضرر شهدته الاستخبارات الإسرائيلية في تاريخها". وعلى الرغم من دفاع تل أبيب الرسمي أمام الرأي العام عنه، خاصة ضابط استجوابه حين عودته للأراضي المحتلة، "شيمعون ليفي"، فإنّ ما قاله "عاموس" أرَّخ لبداية سُمعة الوحدة 8200، على الرغم من فشلها في حرب "يوم الغفران"، وخط نقطة البداية لقوّة إسرائيل السيبرانية بأكملها.

الفشل الاستخباري الثاني كان في عدم توقّع حصول الثورات العربية. وعلى الأثر أنشأت الاستخبارات العسكرية الإسرائيلية قسماً تابعاً للوحدة 8200 لمراقبة وسائل الإعلام العربية، ومواقع التواصل الاجتماعي، لرصد توجهات العالم العربي من رسائل معادية لإسرائيل في أعقاب الثورات، وجمع المواد الإخبارية والتصريحات السياسية على مدار 24 ساعة، في جميع المواقع الفلسطينية والصفحات الشخصية لمسؤولين فلسطينيين وعرب، لرصد أي إشارات لتغيير قادم. ويقول أحد القادة السابقين لوحدة «حتساف» التابعة للوحدة 8200، إنه «منذ ذلك الحين تكثّف الاستخدام التجسسي بشكل كبير، ولم يعد من الممكن الانخراط فقط في وسائل الإعلام المكتوبة والمسموعة، أو النظر فقط إلى ما يفعله القادة. فعالم الإنترنت ووسائل التواصل الاجتماعي شكّلت فرصة جديدة لا نهاية لها في جمع المعلومات؛ فهذا جزء لا يتجزأ من صورة الاستخبارات». ويضيف أنه إلى جانب الاستماع التقليدي لوسائل الإعلام وقراءة الصحف، يجلس جنود وحدة «حتساف» على مواقع التواصل الاجتماعي ويشاهدون مقاطع الفيديو على موقع ويتابعون الأنشطة؛ كما أنهم يستخدمون التطبيقات ويجمعون المعلومات من المدوّنات، مضيفًا أنه «من خلال تلك المنشورات التي لا تخضع لقواعد الرقابة وغير مشفّرة، يمكن للجيش الإسرائيلي إثراء صورته الاستخباراتية حول المزاج الشعبي العام في العالم العربي». وبذلك استطاعت الوحدة 8200 – من خلال المجنّدين المدرّبين على التحدّث والكتابة باللغة العربية– استشعار الخطورة أو معرفتها قبل وقوعها، وإبلاغ الجهات المسؤولة لتنفيذ ضربات استباقية. وبعد جمع المعلومات المتاحة، يتمكّن عناصر الوحدة من الانخراط في نقاشات وطرح موضوعات جدلية تُحدث بلبلة بين جمهور "السوشيال ميديا" من الجنسيات العربية المختلفة، لتحقيق أهدافها.

من ناحية أخرى، يقول رونين بيرغمان في كتاب له صدر عام 2009، إن قنبلة مدسوسة لحزب الله، متخفّية في شكل هاتف خلوي، التقطها عملاء اسرائيليون، وأخذوها للتحقيق إلى مقر الوحدة 8200 في شباط/فبراير 1999. وفي داخل المختبر انفجر الهاتف الخلوي. فأصيب اثنان من أفراد الوحدة 8200.

في المقابل، نجحت الاستخبارات الإسرائيلية في زرع أجهزة تنصُّت بطول سوريا وعرضها على مدار سنوات ما قبل حرب يوم الغفران. ولم تسْلم مصر والأردن أيضاً من الشبكة الواسعة. فعندما دقَّت "النكسة" أبواب التحالف الثلاثي "المصري، السوري، الأردني" عام 1967، ودُكَّ سلاح الجو المصري كاملاً من دون أن يرتفع شبراً

واحداً عن الأرض، هاتَف الرئيس المصري جمال عبد الناصر العاهل الأردني الملك حسين حينها، طالباً منه تدخُّل القوات الأردنية امتثالاً للمعاهدة الثنائية بين القاهرة وعَمّان، وما تنص عليه من تدخُّل قوات إحدى العاصمتين للدفاع في حال تعرُّض الأخرى لاعتداء شامل. كانت المكالمة تجري بين رأسَيْ الدولتين، بينما تُسمع وتُسجَّل بالكامل في تل أبيب. وفي وقتٍ لم يكن فيه العرب يسمعون عن الوحدة 8200 بالأساس، كانت تُسجَّل المكالمات الشخصية لرؤسائهم.

في عام 2010، وبينما جَلس العلماء الإيرانيون غير قادرين على تفسير ما يحدث بأي شكل، كانت أجهزة الطرد المركزية في المفاعلات النووية الإيرانية في نطنز تتهاوى كأحجار الدومينو، وهي التي شكَّلت حجر الأساس للبرنامج النووي الإيراني. وخلال أيام قليلة، توقَّف عن العمل ما يقرب من 10% من أجهزة الطرد المركزية، قبل أن يُدرك الإيرانيون حقيقة ما حدث . ففي ذلك العام، أعلن مختبر أبحاث شركة "سيمانتيك" (Symantec)، المتخصصة في أمن المعلومات، اكتشافه لفيروس "زيرو داي" (Zero-day)، المعروف عالمياً باسم "ستكسنت" (Stuxnet)، بعد أن تسبَّب في إلحاق أضرار جسيمة بآلاف من أجهزة الحاسوب في إندونيسيا والهند وباكستان والولايات المتحدة وعدة دول أخرى، وبعد أن أوقع خسائر ليست بالقليلة في المفاعل النووي الإيراني "نطنز".

كان الفيروس مُتطوِّراً جداً إلى حدٍّ "مخيف لم يُرَ من قبل"، كما وصفه بعض خبراء التقنية؛ وهو مستوى أجمعوا بأكملهم على أنه لا يُمكن أن يوجد إلاّ بقدرات دول متورّطة في ابتكاره وتمويل هندسته إلكترونياً، بحسب وصف خبراء شركة "سيمانتِك"؛ وهو التكهُّن الذي استمر حتى قال "يائير كوهين"، أحد المسؤولين عن تصنيعه، في مقابلة صحفية، إن الفيروس كان "نتيجة أشهر طويلة من البحث والتحليل والتطوير المشترك بين المخابرات المركزية الأميركية، ووكالة الأمن القومي الأميركي، والموساد الإسرائيلي، والوحدة 8200"؛ وكان الهدف منه، كما أُعلن فيما بعد، هو محاولة تعطيل البرنامج النووي الإيراني وتحجيمه إلى حين الوصول إلى اتفاق بشأنه مع إيران. وفيما اعتُبر "ستكسنت" أول سلاح رقمي يُستَخدم بالفعل لتحقيق أهداف عسكرية محدّدة، فإن التعاون بين الولايات المتحدة وإسرائيل لم يبدأ عنده، ولن ينتهي بالتأكيد. فقد تمّت الموافقة، أواخر عام 2016، على عدة تشريعات تُفضي بواشنطن إلى توسيع التعاون مع تل أبيب في مجال بحوث الأمن السيبراني . وهذا التوسع يوافق احتمالات واسعة بنمو سوق الأمن السيبراني في العالم، من 122 بليون دولار عام 2015 إلى 200 بليون دولار عام 2021، ويُصاحبه تعاون وثيق بين العناصر السابقة بوحدات الأمن السيبراني والمستثمرين الحاليين داخل إسرائيل للنمو بالاقتصاد عامة، و"بمكانة إسرائيل في مجال الأمن السيبراني خاصة" .

في عام 2018، أعلنت منظمة "سيتيزن لاب" بأن برنامج التجسس الاسرائيلي "بيغاسوس" قد استُخدم لتعقّب المدعو عمر عبد العزيز، وهو معارض سعودي يعيش في كندا تحت رعاية سياسية. ووفقاً لتقرير المنظمة،

استخدم عملاء النظام في الرياض تكنولوجيا (أن أس أو) الإسرائيلية في مونتريال Montreal ضدّ عبد العزيز. وبعد مقتل الصحفي السعودي جمال الخاشقجي، أقام عبد العزيز دعوى قضائية في 2 كانون الأول (ديسمبر) 2018، ضدّ الشركة الإسرائيلية "أن أس أو"، مدّعياً أن برنامج الشركة بيغاسوس كان يُستخدم لاختراق هاتفه المحمول، من أجل تتبّع المحادثات مع الصحافي السعودي جمال خاشقجي. وقد نشرت شبكة "سي أن أن" مراسلات بين عبد العزيز وخاشقجي كانا يُخطّطان فيها لإنشاء حركة على الإنترنت للشباب السعودي، تُجابه دعايات النظام السعودي على الشبكات الاجتماعية. وقد وصف خاشقجي ولي العهد محمد بن سلمان بأنه لبّ المشكلة ويجب إيقافه. وقال عبد العزيز لشبكة (سي أن أن) أن "قرصنة هاتفي لعبت دوراً كبيراً في ما حدث لجمال، أنا آسف لهذا... الذنب يقتلني". وكشفت تحقيقات أجرتها صحيفة هآرتس أنّ الشركة تفاوضت مع المملكة العربية السعودية لبيعها قدرات هجومية متطوّرة لاختراق الهواتف الخليوية. وذكر تقرير لمنظمة العفو الدولية Amnesty International نشرته في آب/ أغسطس 2018، عن تلقّي ناشطين سعوديين معنيّين بحقوق الإنسان، ومنهم عددٌ من موظّفيها، لرسائل مشبوهة عن طريق برنامج واتساب، تحتوي على رابط خبيث من برنامج التجسس "بيغاسوس".

9– التموضع والإدارة:

تقبع الوحدة في صحراء النقب جنوبي فلسطين المحتلة، وهي تُعدّ إحدى أكبر قواعد التنصت في العالم. هذا ما كشفت عنه مجلة "لوموند ديبلوماتيك "الفرنسية، التي تحدّثت عن أن القاعدة مخصّصة للتنصّت على المكالمات الهاتفية واختراق مراسلات البريد الإلكتروني "للحكومات والمنظمات الدولية والشركات الأجنبية والمنظمات السياسية والأفراد". وذكرت المجلة في تقريرها أن أحد الأهداف الرئيسة لقاعدة أوريم هو التنصّت على رسائل وبرقيات السفن في البحر المتوسط، وحتى الكابلات الواقعة تحت سطح البحر، التي تربط إسرائيل ودول المنطقة بأوروبا . كما تنشر هذه القاعدة الضخمة مواقع تنصّت سريّة في مناطق بعيدة عنها. ويتم نقل المعلومات التي تلتقطها لتحليلها في المقر الرئيس للوحدة 8200 السريّة، ليتم بعد ذلك نقله إلى جهاز الاستخبارات الاسرائيلي الموساد وباقي وحدات الجيش الإسرائيلي الأمنية. ويغطّي نطاق عمل قاعدة أوريم للتنصّت مناطق جغرافية واسعة في الشرق الأوسط في قارّتي آسيا وأفريقيا. وأكّدت المجلة أن استخدام برامج الانترنت المناسبة، كـ(غوغل إيرث) مثلاً، يمكّن من مشاهدة هوائيات وصحون التقاط هذه القاعدة . وأشارت المجلة الفرنسية إلى أن هذه المعلومات تجعل من القاعدة الاسرائيلية مساوية في القدرات لعدد من أكبر قواعد التجسس والتنصّت في العالم،

وكتلك التابعة لوكالة الأمن القومي الأمريكي. لكن الفرْق، كما تنوّه "لوموند ديبلوماتيك"، هو أن هذه الوحدات التابعة للدول الغربية معروفة منذ فترة؛ لكن هذه هي المرة الأولى التي يكشف فيها عن القاعدة الإسرائيلية.
تعمل هذه الوحدة في مجالات تُعرف في عالم الاستخبارات بمصطلح "سيجينت"، أو الاستماع؛ وتشمل: التنصّت، واعتراض الإشارات، والتحليل، والترجمة، وتوزيع المعلومات التي تم جمعها من وسائل البث، كالراديو والهواتف وأجهزة الفاكس والبريد الإلكتروني. وكذلك مجال آخر يُعرف بمصطلح "الينت"، أو القراءة الصوتية؛ وتشمل تحليل ورصد الذبذبات الإلكترونية الصادرة عن أجهزة مختلفة، كالرادارات. كما تضم الوحدة إلى جانب ذلك، إدارة لفكّ الشفرات. ولا تعمل الوحدة فيما يُعرف في عالم الاستخبارات ب "هيومينت"، وهو جمع المعلومات من مصادر بشرية، وهو من اختصاص وحدة تشغيل العملاء في الموساد المعروفة ب "تسوميت"، والوحدة 504 التابعة للمخابرات العسكرية الإسرائيلية "أمان". وقد أشارت صحيفة هآرتس إلى أنّ من بين النجاحات الكبيرة للوحدة 8200، التقاط محادثة هاتفية بين الرئيس المصري جمال عبد الناصر والعاهل الأردني الملك حسين، في اليوم الأول لحرب الأيام الستة (67)، واعتراض المحادثة الهاتفية بين زعيم منظمة التحرير الفلسطينية الراحل ياسر عرفات وبين جماعة (أبو العبّاس) الفلسطينية التي اختطفت سفينة الركّاب الإيطالية "أكيلي لاورو".

10 – مجموعة أقمار عاموس:

كشفت صحيفة "إسرائيل اليوم" الإسرائيلية عن أنّ دولة الاحتلال تُسيطر على فضاء جميع الدول العربية بواسطة 6 أقمار اصطناعية، مهمتها تصوير كل صغيرة وكبيرة تحدث في الدول العربية وغير العربية. وتُعرف الوحدة المسؤولة عن إدارة الأقمار الاصطناعية ذات أغراض التجسس في جيش الاحتلال، بمجموعة أقمار "عاموس"، حيث يقوم كل واحد منها بتغطية الكرة الأرضية بأكملها كل 90 دقيقة. ويكشف التحذير الذي أطلقته شركة "آبل" بعد اكتشاف برنامج تجسس يسمح باختراق أجهزة آيفون وآيباد، عن مدى التقدم الذي حقّقته الشركات الإسرائيلية المتخصصة في اعتراض الاتصالات. وفي مواجهة هذا التهديد الإلكتروني، عمدت الشركة الأمريكية بشكل عاجل إلى تحديث نظام تشغيل أجهزة الآيفون التي وزّعتها في الأسواق منذ عام 2011 لحمايتها من برنامج "بيغاسوس" الذي صمّمته مجموعة (أن.أس.أو)، ومقرّها هرتسيليا، المعروفة بـ "وادي السيليكون" الإسرائيلي، شمال تل أبيب. وليست مجموعة (إن. إس. أو) الوحيدة في هذا المجال في الكيان العبري التي تُطلق على نفسها لقب "أمّة الشركات الناشئة"، والتي تعتبر عملية جمع المعلومات ضرورة حيوية في ظل المخاطر الأمنية. وتقدّر منظمة "برايفيسي إنترناشونال" البريطانية غير الحكومية، أن هناك 27 شركة إسرائيلية على الأقل ناشطة في هذا المجال؛ وهذا الرقم يضع إسرائيل، البالغ عدد سكّانها 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. ومن بين مُستخدمي هذه البرمجيات حكومات في أمريكا اللاتينية وآسيا الوسطى وإفريقيا. ووصفت وكالة "أوت لوك" لأمن الهواتف النقّالة برنامج بيغاسوس بأنه الهجوم الأكثر تطوراً، الذي اكتشفته بسبب قدرته على التسلل خلسة إلى أجهزة الهاتف التي يخترقها، وصولاً إلى المكالمات والكاميرات والبريد الإلكتروني ونظام تحديد الموقع الجغرافي وكلمات المرور والتطبيقات، مثل فيسبوك وسكايب وواتساب وفايبر وغيرها. وأكّد متحدث باسم مجموعة (إن. إس. أو) الإسرائيلية في بيان أن "مهمة برامج المجموعة هي المساعدة في جعل العالم مكانًا أكثر أماناً عبر تزويد الحكومات الشرعية بتكنولوجيا تساعدها على محاربة الإرهاب والجريمة". 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 تحدّدها. ويؤكّد دانيال كوهين، الخبير من معهد دراسات الأمن القومي في تل أبيب، لوكالة الصحافة الفرنسية، أن "هذه القضية ليست مفاجئة. فإسرائيل من الدول التي تحتل الطليعة في العالم في كل ما يتعلق بمجال الإنترنت". ويشرح كوهين أن التقدم يأتي أساساً من دينامية عناصر سابقة من وحدات النخبة في الجيش الإسرائيلي، مثل الوحدة 8200. 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". ويشير كوهين إلى أن أقل من 10%من شركات الأمن الإلكتروني اختارت التخصص في الأعمال الهجومية، أي التقنيّات التي تسمح باختراق الأنظمة المعلوماتية. بينما تؤكّد برايفيسي إنترناشونال أن بيع برامج التجسس "قد يؤدّي دوراً هاماً 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 السريّة في أوزبكستان وكازاخستان، إضافة إلى قوات الأمن في كولومبيا. كما صدّرت 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 موجّهة للدانمارك، ولكن تم تحويلها إلى إيران، التي هي عدو لدود للدولة العبرية؛ وسُمح لشركتي نايس وفيربنت بفتح مكاتب ومركز للمراقبة في كازاخستان وأوزبكستان، إضافة إلى تدريب موظّفين محليين في الدولتين. ونسبت وكالة الصحافة الفرنسية إلى متحدّث 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".

11 – سرب نحشون:

كشف كيان الاحتلال الإسرائيلي عن سرب نحشون، وقال بأنه ذراعه للتجسس الإلكتروني، وهو يغطّي العالم العربي. ويستخدم السرب طائرات "غولفستريم" الأمريكية، التي تحمل في داخلها منظومات تجسس، ومراقبة، وقيادة، وسيطرة؛ وهي طائرات في قمّة التطور والتقدم. ويشكّل السرب الجوي وحدة قيادة ومراقبة محمولة، حيث تمتلك دولة الاحتلال سربين من هذا الطراز؛ الأول ينتشر شمال دولة الاحتلال، والثاني يتّخذ من المنطقة الجنوبية قاعدة له. وتستهدف وحدة "سرب نحشون" مصر على وجه الخصوص، حيث تولي دولة الاحتلال التجسس على مصر أهمية كبيرة. فقد أكّدت وسائل إعلام إسرائيلية أن الوحدة 9900 مسؤولة أيضًا عن مراقبة تحركات الجيش المصري في سيناء، وتقوم بإمداد قيادة جيش الاحتلال بأي تطورات في شبه جزيرة سيناء. وكان قائد السرب الجوي الاستخباري الإسرائيلي قد كشف عن ارتفاع عدد المهام التي نفّذها السرب أخيراً.

من أشكال التجسس الإلكتروني لدى "إسرائيل" أيضًا، الرصد والتنصّت على أجهزة الاتصال السلكية واللاسلكية. وتُعدّ واحدة من أشهر تلك القضايا ما كُشف حول قيام شركة موبينايل المصرية بإنشاء محطات تقوية بالقرب من حدود مصر مع دولة الاحتلال الإسرائيلي، حيث أسهمت هذه المحطات بقوّة في إيصال تردّدات الاتصالات المصرية والتقاطها. وحسب تقرير النيابة المصرية، فإن توجيه معظم الهوائيات الخاصة بشركة موبينايل في منطقة العوجة في جهة الجانب الإسرائيلي مكّن من اختراق الشبكة المصرية وتمرير المكالمات الدولية؛ كما أنه سهّل عمل شبكة التجسس في متابعة الاتصالات الدولية والتجسس على شبكات المحمول المصرية واختراق الأمن القومي المصري. وذكر تقرير نشرته جريدة الدستور المصرية "أن بعض محطات التقوية للشبكة موجّهة بزاوية 75 درجة داخل الحدود المصرية باتجاه منطقة صحراوية خالية من السكّان، وأن تلك الجهة تجعل إشارة الاتصالات المصرية تدخل إسرائيل بنسبة محدودة بنسبة 10 كليومترات داخل إسرائيل".

من ناحية أخرى، تُدرك دولة الاحتلال مدى أهمية التقنية في تعقّب شبكات الهاتف ومزوّدي الإنترنت. لذا تعمل شركات التجسس الإسرائيلية على تطوير إمكانياتها في مجال تقنيّة التجسس، وهي لا تكف عن عقد الصفقات التكنولوجية مع الدول الكبرى. ويؤكّد 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. ويكشف 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 "دا فينشي"، وهو برنامج حصان طروادة يُمكّن مُستخدميه من السيطرة عن بُعد على مئات الآلاف من الحواسيب والهواتف وتشغيل الميكروفون والكاميرا فيها، والسيطرة على كل حركة فيها، بما في ذلك موقع الجهاز والمحادثات الصادرة والواردة عنه؛ كما أنه بإمكان هذه البرامج تجاوز أنظمة التشفير وجمع المعلومات من أي جهاز ومواصلة متابعة الأهداف حتى لو كانت خارج نطاق عمل هذه الشركات.

12 – خاتمة:

إنّ عالم إنترنت الأشياء هو عالم كبير وضخم، وربما يغطّي في وقتٍ ما جميع مجالات الحياة. وقد ظهرت بوادره في الوقت الحالي، إذ إن الكثير من الأشياء التي تُستخدم على نطاق واسع أصبح بالإمكان توصيلها بالإنترنت، مثل شاشات التليفزيون المنزلية والساعات والنظّارات والسيّارات والكاميرات. كما امتدّت تلك التقنية إلى الملابس والأثاث والأواني المنزلية؛ وأي شيء يمكن توصيله عبر الإنترنت يُعتبر من عالم إنترنت الأشياء. كل هذه المستلزمات قد تتيح لمن يشتري مُنتجات تلك الشركة التجسس على صاحبها، حتى وإن كان في غرفة نومه. وفي السياق، لا يكاد يُذكر ملف التجسس الإلكتروني في أي مكان بالعالم إلاّ وتُذكر "إسرائيل" كأحد أبرز الفاعلين في تزويد أدوات وبرمجيات الاختراق، مقابل مبالغ مالية ضخمة لهذه الخدمات، التي تُقدّم بسريّة وسلاسة أيضًا، خاصة وأن التجسس الإلكتروني قد أصبح أحد أخطر وأجدى أنواع التجسس في العالم؛ وهو طغى بإمكانياته الهائلة ودقّة نتائجه على أساليب التجسس المعهودة في السابق.

وقد أدركت "إسرائيل" أهمية هذا النوع من التجسس، وخصّصت إمكانياتها للتجسس على بعض الدول العربية، وعلى رأسها فلسطين ومصر، بالإضافة إلى حلفائها، كالأمريكيين والغرب. وبذلك امتدّ ذراع التجسس الإلكتروني الإسرائيلي إلى أقصى حد ممكن يخدم مصلحة كيان الاحتلال. وبالنظر إلى الإمكانيات التي تتمتع بها الوحدة 8200، وقدراتها في العمل السيبراني والتكنولوجيا الفائقة ونوعية الاختراقات التي تنفّذها تزامنًا مع التطور التكنولوجي الذي يعيشه العالم، فإنها تُعدّ نواة الاستخبارات الإسرائيلية التي تغذّي كل المؤسسات التي يعتمد عملها على معلومات استخباراتية دقيقة، سواء تعلّق الأمر بالجانب الأمني أو السياسي أو الاقتصادي. ولا يقتصر عملها على دول معيّنة، ولكنها تعمل بشكل عام، مع التركيز على فلسطين ومصر وسوريا والعراق ولبنان وإيران، عن طريق تنفيذ اختراقات تستطيع من خلالها قراءة مُجريات الأمور، لاستشعار الخطورة أو معرفتها قبل وقوعها، وإبلاغ الجهات المسؤولة لتنفيذ ضربات استباقية.