سلسلة مقالات علمية محكمة (11)

الوحدة الإسرائيلية 8200
ودورها في خدمة التكنولوجيا التجسسية الإسرائيلية

فاطمة عيتاني

مركز الزيتونة للدراسات والاستشارات - بيروت

سلسلة مقالات علمية محكمة

(11)

بسم الله الرحمن الرحيم

الوحدة الإسرائيلية 8200
ودورها في خدمة التكنولوجيا التجسسية الإسرائيلية

رئيس التحرير

د. محسن محمد صالح

مدير التحرير

إقبال عميش

مساعدو التحرير

فاطمة عيتاني

باسم القاسم

فاطمة حسان عيتاني

آب/ أغسطس 2019

مركز الزيتونة للدراسات والاستشارات

بيروت – لبنان

Israeli Unit 8200 and its Role in Serving Israeli Espionage Technology

By: Fatima Hassan ‘Itani

سلسلة مقالات علمية: هي سلسلة مقالات علمية محكمة، تصدر عن مركز الزيتونة للدراسات والاستشارات، تهتم خصوصاً بالشأن الفلسطيني وبكل ما يتعلق به إسرائيلياً وعربياً وإسلامياً ودولياً. ويمكن للباحثين والمختصين نشر مقالاتهم عبر هذه السلسلة، مع ضرورة مراعاة أن تتسم مقالاتهم بالمواصفات العلمية للأبحاث، ولم يسبق نشرها، وأن تناقش القضايا المتعلقة باهتمامات المركز وخصوصاً في الجوانب السياسية والاستراتيجية المتعلقة بقضية فلسطين.

حقوق الطبع محفوظة ©

الطبعة الأولى

آب/ أغسطس 2019

بيروت – لبنان

(الآراء الواردة في المقال لا تعبر بالضرورة عن وجهة نظر مركز الزيتونة للدراسات والاستشارات)

مركز الزيتونة للدراسات والاستشارات

تلفون: 44 36 80 1 961 +

تلفاكس: 43 36 80 1 961 +

ص.ب: 5034–14 بيروت – لبنان

بريد إلكتروني: info@alzaytouna.net

الموقع: www.alzaytouna.net

فهرس المحتويات

فهرس المحتويات 3

الملخص 5

المقدمة 6

أولاً: الخلفية التاريخية للنشاط الاستخباراتي الصهيوني 7

ثانياً: نشأة الوحدة 8200 وتطور هيكليتها ودورها: 9

١. نشأة الوحدة 8200 9

٢. دور الوحدة 8200 وهيكليتها 11

ثالثاً: أداء الوحدة 8200 وأنشطتها: 16

١. أنشطة الوحدة 8200 في البيئة الفلسطينية والعربية 19

٢. أنشطة الوحدة 8200 في البيئة الدولية 26

الخلاصة 34

التوصيات 35

Abstract 36

الوحدة الإسرائيلية 8200
ودورها في خدمة التكنولوجيا التجسسية الإسرائيلية

فاطمة حسان عيتاني[1]

الملخص:

يعد التجسس الإلكتروني نوعاً جديداً من حروب السيطرة على الأشخاص والمؤسسات والدول. وتعدّ "إسرائيل" من أبرز محاضن تكنولوجيا الاتصالات، فعدد كبير من هذه الشركات التي تحتل مراكز متقدمة عالمياً إما أنها اشترت شركات إسرائيلية، أو أنها أنشأت مراكز للبحث والتطوير لها في "إسرائيل".

تحاول هذه الدراسة تسليط الضوء على الخلفية التاريخية للنشاط الاستخباراتي الصهيوني، وخصوصاً نشأة وحدة المخابرات العسكرية الإسرائيلية 8200، المتخصصة في مجال تقنيات التجسس التكنولوجي، مروراً بتطورها وأنشطتها في البيئات؛ الفلسطينية، والعربية، والدولية.

وسعت هذه الدراسة إلى إبراز أهداف "إسرائيل" غير المعلنة، بتطويرها واستغلالها للتطور التكنولوجي؛ بهدف تحقيق مكاسب أمنية وسياسية واقتصادية على الصعيد الدولي.

كلمات مفتاحية:

الوحدة 8200	التجسس الإلكتروني	"إسرائيل"	شركات الأمن	الأمن السيبراني	الجيش الإسرائيلي

[1] باحثة في مركز الزيتونة للدراسات والاستشارات، ومتخصصة في الشأن الفلسطيني.

المقدمة:

أدى التطور التكنولوجي وخصوصاً تكنولوجيا الاتصالات إلى فوائد اجتماعية واقتصادية كثيرة، لكنها في الوقت نفسه فرضت العديد من التحديات الجديدة؛ فالاعتماد على تقنيات الإنترنت، واستقبال كميات كبيرة من المعلومات الشخصية للعملاء وتخزينها، واتساع المنافسة في الاقتصاد العالمي، ورقعة الخلافات والأزمات الدولية، كل ذلك وغيره سمح بتعزيز التجسس الإلكتروني، وأصبح الكشف عن معلومات الآخر الإلكترونية؛ جزءاً من مهمات أجهزة مخابرات وشركات وجِهَات لتحقيق أهداف وأجندات مختلفة.

ويعد التجسس الإلكتروني، الذي طغى بإمكانياته وخطورته على أساليب التجسس السابقة، نوعاً جديداً من حروب السيطرة على الأشخاص والمؤسسات والدول، وهو أحد أخطر أنواع التجسس، من ناحية القرصنة الإلكترونية، وعمليات الاختراق، وسرقة البيانات، وانتهاك الخصوصية... . وأصبح من غير الممكن التأمين الكامل للبيانات على جهاز الكمبيوتر أو الهاتف، في ظلّ ثورة التكنولوجيا التي نشهدها، إلا إذا كان الجهاز غير متصل بالإنترنت نهائياً، وهو أمر يصعب تطبيقه في الوقت الراهن.

واقتحمت بعض الدول خصوصيات مواطنيها من خلال مراقبة مكالماتهم الخاصة أو صفحاتهم الاجتماعية أو بريدهم الإلكتروني...، وبررت تصرفاتها هذه لتحقيق أمنهم ومكافحة "الإرهاب"، وسنَّت قوانين تمنحها العديد من الصلاحيات على حساب الحريات العامة.

ويتميز التجسس الإلكتروني، الذي يعد أحد أنواع الحروب المُستخدمة في العالم، بأنه لا يترك دليلاً مادياً له، مما يصعب معه عملية التعقب والإدانة، ويحدث في بيئة هادئة من خلال جهاز كمبيوتر وبعض البرامج وشبكة الإنترنت، ولا يحتاج إلى القوة والعنف واستعمال الأسلحة. وللتجسس الإلكتروني العديد من الأهداف كزعزعة الأمن، وتعطيل البنى التحتية لدول كشبكات الطاقة النووية، والكهرباء، والمياه وغيرها، وابتزاز الأشخاص والدول، وسرقة الأموال،... .

ولا يُستبعد أن تمارس أي من الدول الكبرى التجسس على مواطنيها، بالرغم من تغنيها بالحريات الشخصية، فمثلاً وثائق ويكيليكس Wikileaks سنة 2006؛ التي سُرِّبت من داخل الإدارة الأمريكية، حيث أفضل الشبكات الإلكترونية أمناً وأماناً في العالم، وتسريبات الموظف السابق في وكالة الأمن القومي الأمريكية National Security Agency (NSA) إدوارد سنودن Edward Snowden سنة 2013، التي كشفت عن عمليات تجسس واسعة تقوم بها الوكالة وتمس ملايين المكالمات الهاتفية والرسائل الإلكترونية دون أيّ مراعاة للحرية الشخصية، إلى غيرها من عمليات اختراق وبيع معلومات شخصية من خلال مواقع اجتماعية معروفة، خيرُ دليل على ذلك.

وتعدّ "إسرائيل" أحد أبرز محاضن تكنولوجيا الاتصالات، فعدد كبير من هذه الشركات التي تحتل مراكز متقدمة عالمياً إما أنها اشترت شركات ناشئة إسرائيلية، أو أنها أنشأت مراكز للبحث والتطوير لها في "إسرائيل".

تحاول هذه الدراسة تسليط الضوء على الخلفية التاريخية للنشاط الاستخباراتي الصهيوني، وخصوصاً نشأة وحدة المخابرات العسكرية الإسرائيلية 8200، المتخصصة في مجال تقنيات التجسس التكنولوجي، والتي يرى البعض أنها توازي وكالة الأمن القومي للولايات المتحدة الأمريكية، مروراً بتطورها وأنشطتها في البيئات؛ الفلسطينية، والعربية، والدولية. واعتمدت هذه الدراسة في أغلبية مراجعها على المصادر الإسرائيلية والأجنبية، إذ قلما نجد دراسة باللغة العربية تتناول موضوع تخصص الوحدة الإسرائيلية 8200 وتأثيرها من خلال شركاتها الناشئة المنتشرة في العالم. كما سعت هذه الدراسة إلى كشف المدى الذي وصلت إليه "إسرائيل" في أحد أبرز المجالات التكنولوجية، ومكانتها بالنسبة للدول الأخرى، من حيث اختراق خصوصيات الدول والشعوب، لنرى حتمية فقدان الأمن والأمان من ناحية الخصوصية الشخصية؛ إن على الهاتف أو الكمبيوتر الخاص.

وتندرج هذه الدراسة في إطار ضرورة المعرفة الصحيحة والموضوعية للعدو. ولا ينبغي أن يُفهم منها ترهيب بإمكاناته، ولا إحباط للقوى التي تواجه هذا المشروع. إذ إن معرفة الحقائق والتعامل المنهجي معها هو من أبرز العناصر لتعبئة طاقات الأمة وتوجيهها وتحديد أولوياتها؛ وهي بالتالي عنصر أساسي في نجاح المواجهة مع المشروع الصهيوني.

أولاً: الخلفية التاريخية للنشاط الاستخباراتي الصهيوني:

تعود فكرة تأسيس منظمات وحركات استخباراتية إسرائيلية إلى ما قبل الإعلان عن "دولة إسرائيل" سنة 1948. ففي تشرين الثاني/ نوفمبر 1915، أسس المهندس الزراعي آهارون آرونسون Aharon Aaronsohn أول وحدة استخبارات سريّة في فلسطين؛ تخدم وكالة تجسس بريطانية أطلق عليها اسم نيلي Netzah Yisrael Lo Yeshaker (NILI)، وتعني "إسرائيل الخالدة لن تكذب".[٢]

وخلال الحرب العالمية الأولى، جمعت وحدة نيلي المعلومات الاستخباراتية للبريطانيين تحت ستار الأعمال الزراعية لشركة آرونسون، فقدم الجواسيس معلومات قيمة للضباط البريطانيين حول الأوضاع الداخلية، وتحركات القوات العثمانية، والسكك الحديدية والطرق المحتملة التي قد

[٢] J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship," Thesis, The Honors Tutorial College, Ohio University, Athens, April 2017, https://etd.ohiolink.edu/!etd.send_file?accession=ouhonors1492781541344253

يستخدمها البريطانيون في هجومهم لاحتلال فلسطين. ولكن تمّ القبض على معظم أعضاء وحدة التجسس وحكم عليهم بالإعدام. وفي سنة 1920، تمّ تشكيل الهاجاناه Haganah، وهي ميليشيا سرية، لحماية اليهود في ظلّ الحكم العثماني. وبعد هزيمة العثمانيين، سيطر البريطانيون على فلسطين، وقامت الهاجاناه في سنة 1929، بتشكيل "شين ميم 2 أو Shin Mem 2"، وكانت مهامها مراقبة الخطوط الهاتفية للعرب في القدس لجمع المعلومات عن ما تُسمّيه "أعمال الشغب" المحتملة، وكانت هذه الحالة الأولى التي تُستخدم فيها الإشارات الاستخباراتية.[٣]

وبعد ثورة البراق سنة 1929، والتي أدت إلى مقتل 133 يهودياً وجرح أكثر من 300 آخرين، واستشهاد 116 فلسطينياً وجرح أكثر من 200 آخرين، أدرك اليهود أنهم لم يعودوا قادرين على الاعتماد على القوات البريطانية لحمايتهم، وبدأت الهاجاناه بتطوير نفسها وتوسيع مهامها وجندت الشباب اليهود، وأقامت دورات عسكرية لهم، وسلحتهم بالأسلحة الخفيفة التي تدفقت من أوروبا.[٤]

وخلال ثورة فلسطين الكبرى 1936–1939، حوَّلت الهاجاناه نفسها من ميليشيا إلى قوة عسكرية، وتعاونت مع قوات الأمن البريطانية في حماية المستوطنين اليهود. واستخدم البريطانيون المعلومات الاستخباراتية التي كانت تجمعها الهاجاناه لتنظيم غارات ليلية استباقية على الثوار الفلسطينيين. وفي تلك الفترة، شكلت الهاجاناه "ليه عاليه بيث (الموساد) (Mossad) Le' Aliyah Beth" الذي ساعد في تنظيم الهجرة اليهودية غير الشرعية من جميع أنحاء أوروبا إلى فلسطين.[٥]

وفي أيلول/ سبتمبر 1940، تمّ تأسيس شيروت يديعوت Sheruth Yedioth، المعروف باسم شاي Shai (دائرة المعلومات) رسمياً، بعد اقتراح من شاؤول أفيجور Shaul Avigur، القائد في "ليه عاليه بيث (الموساد)" على قادة الهاجاناه بتأسيس وحدة معلومات تعمل على مستوى فلسطين المحتلة. وقامت المخابرات العسكرية البريطانية "أم آي 4 أو MI4" بتسليحهم وتمويلهم وتدريبهم.[٦]

---

[٣] تعرف على الهاغاناه، موقع الجزيرة.نت، 2016/9/20، انظر:
https://www.aljazeera.net/home/Getpage/98de5902-f542-49cc-b509-ceb2273edfdb/4fcc6b56-b2fb-43b5-bd8c-6346060130fa؛ وانظر:
J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship."

[٤] من ذاكرة القدس.. ثورة البراق، موقع الجزيرة.نت، 2016/4/13، انظر:
https://www.aljazeera.net/home/Getpage/db8bd9b0-0739-484d-9100-ff486339852a/c70b8611-42d7-4d17-8910-3d9104eb1e3a؛ وانظر:
J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship."

[٥] تعرف على الهاغاناه، موقع الجزيرة.نت، 2016/9/20؛ وانظر:
J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship."

[٦] J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship."

وفي نهاية الحرب العالمية الثانية، تألفت حركة المقاومة اليهودية الموحدة في تشرين الأول/ أكتوبر 1945، من الهاجاناه ومن منظمتين شبه عسكريتين هما الإرجون Irgun وليحي Lehi، والتي تحولت فيما بعد إلى الجيش الإسرائيلي Israeli Defense Force (IDF).[٧]

في 1948/5/14، انتهى الانتداب البريطاني وأعلن ديفيد بن جوريون David Ben-Gurion إقامة "دولة إسرائيل"، وتدخلت الجيوش العربية لدعم الفلسطينيين ضدّ القوات الصهيونية،[٨] وكان لشبكة المخابرات الواسعة التي طورتها الهاجاناه، دور مهم في هزيمة القوات العربية.[٩]

ثانياً: نشأة الوحدة 8200 وتطور هيكليتها ودورها:[١٠]

1. نشأة الوحدة 8200:

بدأت الوحدة 8200 قبل سنة 1948 كمجموعة من الأشخاص الذين حاولوا تطوير مهاراتهم التكنولوجية بجمع وفك رموز الخصوم البريطانيين والعرب. وفي سنة 1948، أنشأ الجيش الإسرائيلي وحدة حرب إلكترونية في مدينة يافا، أُطلق عليها اسم شيفرة "الأرنب Rabbit"، وكانت مهمتها التنصت على المكالمات بين الفلسطينيين وفكّ رموزها، في وقت كانت الولايات المتحدة وبريطانيا والاتحاد السوفييتي من الدول القليلة التي باستطاعتها فك رموز وشيفرة الاتصالات.[١١]

وتشير بعض المصادر إلى أنه تمت الاستفادة من الخبرات والقدرات التكنولوجية الغربية الموجودة لديهم، وتمّ تطويرها من قِبل مهندسي الكمبيوتر الإسرائيليين الذين هاجر بعضهم من الاتحاد السوفييتي. وواجهت هذه الوحدة بعض المشاكل؛ كنقص الخبرة التقنية، والقوى العاملة، وغيرها، فلجأت إلى تقنيات بدائية للتنصت، ثم طورتها سنة 1949.[١٢]

وفي سنة 1950، حصلت الوحدة 8200 على ميزانية قدرها 15 ألف دولار (ما يعادل 478 ألف دولار بأسعار بداية سنة 2019)، و110 آلاف دولار إضافية للمشتريات الإلكترونية من الخارج (ما

---

[٧] Ibid.

[٨] Ibid.

[٩] Ibid.

[١٠] لمزيد من المعلومات حول السعي الإسرائيلي للريادة على مستوى العالم في مجال الأمن الإلكتروني، ومن خلال الوحدة 8200، انظر فيديو على موقع يوتيوب:

Vice News, How Israel Rules The World Of Cyber Security, YouTube Channel, https://www.youtube.com/watch?v=ca-C3voZwpM

[١١] J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship."

[١٢] Ibid.

يعادل 3.5 مليون دولار بأسعار بداية سنة 2019)؛[١٣] وهو مبلغ ضئيل عند محاولة شراء أنظمة الكمبيوتر الأكثر تقدماً. غير أن الوحدة حفاظاً على سرية قدراتها الاستخباراتية، طورت معظم تكنولوجياتها داخلياً. ونشرت قواعد التنصت في كافة أنحاء "إسرائيل" في أوائل خمسينيات القرن العشرين، ولكن بمعدات غير متطورة، وجنود عديمي الخبرة. وبحلول سنة 1959، حصلت الوحدة على إمكانية الوصول إلى تقنية حوسبة أكثر تقدماً، وذلك بعد أن أنشأت وحدة رفائيل RAFAEL في الجيش الإسرائيلي، المسؤولة عن تطوير الأسلحة، جهاز كومبيوتر أطلقت عليه ايتسيك Itzik، والذي سمح بإجراء عمليات محاكاة على نطاق واسع، أي محاولة تنفيذ عملية ما في ظروف اصطناعية مشابهة إلى حدّ ما للظروف الطبيعية، وذلك بهدف دراسة النتائج المتوقعة.[١٤]

وفي سنة 1960، اشترى الجيش الإسرائيلي جهاز كمبيوتر فيلكو Philco من الولايات المتحدة الأمريكية، وأنشأ "مركز أجهزة الكمبيوتر وإدارة السجلات The Center for Computers and Mechanized Records" المعروفة باسم مامرام MAMRAM، ما جعل وحدة 8200 تكون من أفضل وحدات القرصنة الإلكترونية (الهاكرز Hackers) وفك الشفرات المعقدة. واستخدم الجيش الإسرائيلي هذه القوة الحاسوبية خلال حرب سنة 1967، عندما تمكنت من اعتراض وفكّ رموز الاتصالات الجوية المصرية والسورية، مما ساعد القوات الجوية الإسرائيلية على التفوق في المجال الجوي والسيطرة عليه.[١٥]

وكانت سنة 1973 خطأً مفصلياً في تاريخ الوحدة، إذ ألحق أسر الضابط الإسرائيلي عاموس ليفينبرغ Amos Levenberg، "الضابط المغني Singing Officer" كما كان يسمى في "إسرائيل"، المطلع على أسرار حساسة جداً، في قبضة السوريين، وفشله في الوقوف أمام الحرب النفسية التي أدارها المحققون السوريون، ضرراً كبيراً بالاستخبارات الإسرائيلية، لاعترافه لهم بكل شيء يعرفه، كتنصت "إسرائيل" على كافة وسائل البث العسكرية السورية، بما فيها الاتصالات التي تحصل بين الرئيس السوري وقادة الفرق، واختراق الأراضي السورية، وتثبيت أجهزة تنصت كانت موصولة بكافة كابلات Cables الاتصالات السورية، والتي كانت بدورها تنقل كل المعلومات إلى قواعد الوحدة 8200.[١٦] كما فشلت الاستخبارات الإسرائيلية في أثناء حرب سنة 1973 (ما يُسمى

---

[١٣] بلغ سعر أونصة الذهب 1,281.3$ في 2019/1/1، و40.25$ سنة 1950.

[١٤] Ibid; and Stacy Perman, *Spies, Inc.: Business Innovation from Israel's Masters of Espionage* (United Kingdom (UK): Pearson Education, 2010), p. 92.

[١٥] J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship"; and Ronen Bergman, The Spies Inside Damascus, site of Foreign Policy, 20/9/2013, https://foreignpolicy.com/2013/09/20/the-spies-inside-damascus/

[١٦] Ronen Bergman, The Spies Inside Damascus.

إسرائيلياً حرب يوم الغفران)، بتوفير الإنذار للجيش في الوقت المناسب، مما اضطر رئيس هيئة الأركان ديفيد (دادو) إيلْعَزار David "Dado" Elazar ورئيس هيئة الاستخبارات في الجيش الإسرائيلي حينها إلى الاستقالة، وبدأت الوحدة 8200 في تغيير هيكلها التنظيمي وتطويره، وأصبحت أكبر وحدة فنية متخصصة في الجيش الإسرائيلي.[١٧]

2 . دور الوحدة 8200 وهيكليتها:

الوحدة 8200 هي وحدة نخبة تابعة لجهاز الاستخبارات العسكرية الإسرائيلية (أمان) Aman، وهي ركن أساسي للمخابرات العسكرية الإسرائيلية، تسعى لإنتاج أفضل المواهب التكنولوجية على مستوى العالم. وهي المسؤولة عن جمع المعلومات الاستخبارية المشفرة SIGINT، أي من الإشارات الإلكترونية وأنظمة الاتصالات الأخرى التي تستخدمها الأهداف الأجنبية والمحلية، من خلال الرصد، والتنصت، والتصوير، والتشويش، ثم يتم تحليل هذه البيانات لتقييم التهديدات المحتملة للأمن القومي الإسرائيلي.[١٨]

وتعد هذه الوحدة منظمة سرية وغامضة، وذات بيانات محدودة متاحة للجمهور، لذلك يصعب الحصول على البيانات الدقيقة التي يحتاجها أي بحث أكاديمي حولها. وقدَّر موقع فوربس Forbes، سنة 2016، عدد أفراد الوحدة بـ 5 آلاف شخص، وكلهم يعملون لإيجاد أحدث التقنيات التكنولوجية مع القليل من التوجيه.[١٩] ويُفترض أن يتفوق خريجو الوحدة بثلاث صفات ريادية هي أخذ المخاطر، والاستقلالية، والابتكار.[٢٠]

ووفق بعض الباحثين، تعد هذه الوحدة من أفضل وكالات الاستخبارات العسكرية في العالم، ويرى البعض أنها توازي وكالة الأمن القومي للولايات المتحدة الأمريكية.[٢١]

---

[١٧] ديفيد إيلعازر، صحيفة يديعوت أحرونوت، انظر: https://www.ynet.co.il/yaan/0,7340,L-8333-PreYaan,00.html (بالعبرية)؛ ونتانئِل لورْخ، حرب يوم الغفران (تشرين الأول أكتوبر 1973)، موقع وزارة الخارجية الإسرائيلية، انظر: http://mfa.gov.il/MFAAR/InformationaboutIsrael/TheHistoryOfTheJewishPeople/WarsOfIsrael/Pages/yom%20kippur%20war%201973.aspx؛ وانظر:

J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship."

[١٨] وحدة 8200، موقع ويكيبيديا، انظر: https://ar.wikipedia.org/wiki/%D9%88%D8%AD%D8%AF%D8%A9_8200؛ وانظر:

J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship"; and Unit 8200, site of Wikipedia, https://en.wikipedia.org/wiki/Unit_8200#cite_ref-bamahane_9-0

[١٩] Richard Behar, Inside Israel's Secret Startup Machine, site of Forbes, 11/5/2016, https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#3b08bdd01a51

[٢٠] J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship."

[٢١] John Reed, Unit 8200: Israel's cyber spy agency, site of Financial Times, 10/7/2015, https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c

في سنة 2010، ذكرت صحيفة لو موند ديبلوماتيك Le Monde diplomatique الفرنسية أن الوحدة 8200 تدير قاعدة تجسس كبيرة في النقب، أُطلق عليها اسم أوريم Urim، وهي واحدة من أكبر قواعد الإشارات الاستخباراتية في العالم، قادرة على مراقبة المكالمات الهاتفية ورسائل البريد الإلكتروني، ووسائل الاتصالات الأخرى، في جميع أنحاء الشرق الأوسط، وأوروبا، وآسيا، وإفريقيا، وكذلك تتبع السفن. كما ذكرت أن الوحدة 8200 تحتفظ بمواقع استماع سرية في السفارات الإسرائيلية في الخارج، وتتنصت على الكابلات الموجودة تحت البحر، لا سيّما كابلات البحر المتوسط التي تربط "إسرائيل" بأوروبا عبر صقلية، وتحتفظ بوحدات استماع سرية في الأراضي الفلسطينية، كما تستخدم طائرات غلف ستريم Gulfstream مزودة بمعدات مراقبة إلكترونية.[٢٢]

وباستثناء الأقمار الصناعية المختصة بالبث التلفزيوني، فإن معظم الأقمار الصناعية الأخرى، امتداداً من المحيط الهندي إلى المحيط الأطلسي، هي أهداف محتملة، سواء كانت أوروبية، أم عربية، أم روسية، أم آسيوية، وكذلك الأقمار الصناعية إنتلسات Intelsat، التي تتابع المكالمات الهاتفية بين البلدان، وإنمارسات Inmarsat، التي تغطي الاتصالات البحرية.[٢٣]

تعمل وحدة 8200 كشركة ناشئة عالية التقنية في تدريب عناصرها الجدد، وهي تركّز على العناصر الذين تتراوح أعمارهم بين 18 و21 عاماً، إذ تضعهم في بيئة تدريب تشبه بيئة الشركات الناشئة لتحقيق مزيد من التحفيز والتدريب. ويتم اختيار المجندين فيها بحسب القدرة على التكيف والتعلم السريع والابتكار، فهي تستهدف الطلاب الذين يتمتعون بقدرات تحليلية فائقة، ويمكنهم اتخاذ قرارات سريعة والعمل بشكل جيد ضمن فريق، ويتحملون المخاطر باستمرار في المواقف الصعبة، حتى عند مواجهة الخصوم، ولديهم الرغبة المستمرة في التحسن والتعلم من الفشل. ويتعرض جنود الوحدة 8200 لعملية فحص صارمة ودقيقة قبل قبولهم في الوحدة، كما يتم فحص جميع المجندين المحتملين من قِبل الجيش الإسرائيلي عند اقترابهم من التخرج من المدرسة الثانوية، وفي بعض الأحيان تبدأ متابعتهم عندما يكونون أصغر سناً، وذلك باستخدام برامج ما بعد المدرسة للفتيان الذين تتراوح أعمارهم بين 16–18 سنة، بتعليمهم الكمبيوتر ومهارات القرصنة.[٢٤]

---

[٢٢] Nicky Hager, Desert base listens to the world talking, Israel's omniscient ears, *Le Monde diplomatique* newspaper, September 2010, https://mondediplo.com/2010/09/04israelbase

[٢٣] Ibid.

[٢٤] Richard Behar, Inside Israel's Secret Startup Machine; Idan Tendler, From The Israeli Army Unit 8200 To Silicon Valley, site of TechCrunch, 20/3/2015, https://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley/; Unit 8200, site of Wikipedia; Dan Senor and Saul Singer, *Start-up Nation: The Story of Israel's Economic Miracle* (New York: Hachette Book Group, 2009); and J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship".

وتشير إنبال أريلي Inbal Arieli، وهي خريجة من هذه الوحدة، أن عملية الفرز تختلف عن وكالة الأمن القومي الأمريكية، لأنها لا تعتمد على الخبرة السابقة.[٢٥]

وبعد قبول المرشحين في الوحدة، يبدأ برنامج تدريبي شاق ومكثف لمدة ستة أشهر، ما بين 16 إلى 18 ساعة في اليوم، وهو يعد "معسكراً للأذهان"، يهدف إلى إعداد الأفراد وتمكينهم بالمهارات التقنية الضرورية للقيام بعملهم بشكل جيد، فيتم وضع المجند في فريق صغير "حيث يدرس ويجري عصفاً ذهنياً ويتدرب ويحلل ويحل المشاكل، من الصباح الباكر إلى وقت متأخر من الليل".[٢٦] ويقول نداف زافرير، قائد "سابق"[٢٧] لوحدة 8200: "يتدفق كل سنة على الوحدة 8200 الكثير من الشباب والشابات المتحمسين لحل مشاكل الوحدة من منظور جديد تماماً، نحن لا نخبرهم بأن أشخاصاً آخرين حاولوا حلّ المشكلة نفسها عدة مرات وفشلت".[٢٨]

وكثيراً ما يكون الضباط المسؤولون عن التدريب أكبر بسنتين فقط من المجندين الجدد. ويستخدم هؤلاء الضباط منهجاً تعليمياً طوره مركز أجهزة الكمبيوتر وإدارة السجلات (مامرام) خلال سنة 1980 باسم "التخطيط حسب الحالات Planning By Situations (PBS)". وهذا البرنامج هو نهج شمولي عملي، يركّز على أهم الصفات والمهارات الضرورية التي يجب على الطالب اكتسابها للقيام بعمله، وتعرف هذه الصفات والمهارات باسم "المكونات المهنية".[٢٩]

بعد هذا التدريب، يتم وضع الجنود في وحدات فرعية مختلفة في الوحدة 8200؛ في حين قد تختلف مسؤولياتهم الفردية، فإن أساسيات عملهم تبقى هي نفسها. ويتم تحفيز جنود الوحدة 8200 لتعلم المهارات الفنية اللازمة لإنشاء شركة إلكترونية خلال فترة وجودهم في الوحدة وبيعها. وبعد انتهائهم من الخدمة في الوحدة يصبحون قادرين على تأسيس واحتلال المراكز العليا في العديد من شركات تكنولوجيا المعلومات الدولية.[٣٠]

---

[٢٥] Richard Behar, Inside Israel's Secret Startup Machine.

[٢٦] Ibid.

[٢٧] إن إطلاق كلمة "سابق"، على الأعضاء الذين تركوا الوحدة 8200 لاستلام شركات أخرى، لا يعني توقف ارتباطهم وخدمتهم للمخابرات الإسرائيلية، بل يُمثل انتقالهم لأماكن عمل أخرى فرصة للاختراق الإسرائيلي بشكل آخر، فهم احتفظوا بصفة "العميل" دون أن يعملوا مباشرة داخل الوحدة.

[٢٨] Richard Behar, Inside Israel's Secret Startup Machine.

[٢٩] Dan Breznitz, "The Military as a Public Space: The Role of the IDF in the Israeli Software Innovation System," Industrial Performance Center, Massachusetts Institute of Technology, Working Paper Series, April 2002, p. 23, https://ipc.mit.edu/sites/default/files/documents/02-004.pdf

[٣٠] J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship"; and Unit 8200, site of Wikipedia.

ومن أشهر الشركات الرائدة في العالم والتي أسستها الوحدة 8200، شركة شيك بوينت Check Point Software Technologies Ltd. سنة 1993، وهي تقوم بتطوير وتسويق ودعم مجموعة من المنتجات والخدمات لأمن تكنولوجيا المعلومات، وشركة سايبر آرك CyberArk Software Ltd. سنة 1999، وهي شركة أمن معلومات تحمي المؤسسات من الهجمات الإلكترونية، تقدر قيمتها بحوالي ٢ مليار دولار، وشركة إمبيرفا Imperva, Inc. سنة 2002، لحماية البيانات، وشركة بالو آلتو Palo Alto Networks, Inc. سنة 2005، وهي منصة أمان، تقدر قيمتها بأكثر من 14 مليار دولار، وشركة ويكس Wix.com, Ltd. سنة 2006، وهي واحدة من منصات تطوير الويب على مستوى العالم، قام بتأسيسها أفيخاي أبراهامي Avishai Abrahami بعد أن ترك الوحدة 8200، بالإضافة إلى العديد من الشركات الأخرى التي تقدر قيمتها بمليارات الدولارات، والتي تمّ تأسيسها من قبل أعضاء "سابقين" في الوحدة 8200، وهو حال العديد من مجندي الوحدة بعد انتهاء خدمتهم.[٣١]

وفي سنة 1999، فازت مجموعة مير Mer Group الإسرائيلية،[٣٢] التي يتولى رئاستها التنفيذية نير ليمبرت Nir Lempert، وهو من العناصر "السابقة" في وحدة 8200،[٣٣] بعقد للشرطة الإسرائيلية لإنشاء مابات 2000 أو Mabat 2000، وهو نظام أمني يتألف من شبكة معقدة من كاميرات مراقبة، وقامت بزرع مئات الكاميرات في مدينة القدس القديمة. وفي مقابلة مع مجلة "إسرائيل غيتواي Israel Gateway"، أوضح حاييم مير Haim Mer، رئيس مجلس إدارة الشركة، وجندي "سابق" في وحدة 8200، أن "الشرطة كانت بحاجة إلى نظام يتحكم فيه "الأخ الأكبر Big Brother" ويسمح بمتابعة الأحداث في أرجاء المدينة القديمة كافة". وقال إيال راز Eyal Raz، مدير الإنتاج في شركة مير للأمن Mer Security، أن الشركة تقوم بعمل تطوير مشترك مع الوحدة 8200، كما يتم تجنيد العناصر "السابقة" من الوحدة للعمل في الشركة. وتقدم مير خدماتها لعملائها المنتشرين حول

---

[٣١] J. Peter Rousseau, "The History and Impact of Unit 8200 on Israeli HI-TECH: Entrepreneurship"; and Richard Behar, Inside Israel's Secret Startup Machine.

[٣٢] وهي شركة تأسست سنة 1982، وتدير حالياً (2019) بحسب صفحتها على موقع اللينكدإن linkedin عشرات الشركات الفرعية التابعة لها في العالم وخصوصاً في أمريكا اللاتينية وإفريقيا و"إسرائيل"، وتوظف حوالي 1,200 موظف في أكثر من أربعين دولة، وتعمل في البنية التحتية اللا سلكية، وبرامج أنظمة التذاكر العامة، ومعالجة مياه الصرف الصحي، ومنتجات المراقبة، وغيره. انظر:

Mer Group, Overview, site of linkedin, https://www.linkedin.com/company/mer-technologies/about/

[٣٣] Alex Kane, How Israel Became a Hub for Surveillance Technology, site of The Intercept, 17/10/2016, https://theintercept.com/2016/10/17/how-israel-became-a-hub-for-surveillance-technology/

العالم، ففي سنة 2011، وقّعت مير عقداً بقيمة 42 مليون دولار مع بوينس آيريس Buenos Aires عاصمة الأرجنتين لإنشاء نظام "المدينة الآمنة"، وذلك من خلال نشر 1,200 كاميرا مراقبة في المدينة تحتوي على تقنية التعرف على لوحات أرقام السيارات.[٣٤]

ومن الجدير بالذكر، أنه في آب/ أغسطس 2016، نشرت منظمة الخصوصية الدولية Privacy International، والتي تتخذ من لندن مقراً لها، تقريراً حول شركات تصنيع تقنيات المراقبة في العالم، ذكرت فيه وجود 27 شركة مراقبة إسرائيلية؛ وهي أعلى نسبة لكل فرد في أي بلد في العالم، إذ تدير الولايات المتحدة الأمريكية 122 شركة مراقبة. وتدير الوحدة 8200 ما لا يقل عن ثمانية من شركات المراقبة الإسرائيلية الـ 27 التي ذكرتهم منظمة الخصوصية الدولية. ولكن هذا الرقم ليس حقيقياً، إذ أن هناك شركات مراقبة إسرائيلية مصنفة كشركات من دول أخرى لأن مقرها الرئيسي لا يقع في "إسرائيل"، كشركة ناروس Narus، التي أسسها عناصر "سابقة" في الجيش الإسرائيلي في الوحدة 8200، ولكن اشترتها شركة Boeing الأمريكية، ومقرها الرئيسي في كاليفورنيا، لذلك صنفتها منظمة الخصوصية الدولية كشركة أمريكية.[٣٥] وهذا ما يتوافق مع نتيجة التقرير الذي خلصت إليه شركة بيانات في نيويورك "سي بي انسايتس CB Insights"، في نيسان/ أبريل 2018، والذي أظهر أن "إسرائيل" شكلت 7% من حصة التعامل العالمي للأمن الإلكتروني في السنوات 2013–2017، وما تزال بعد الولايات المتحدة، والتي تمثل 69% من حصة السوق العالمية، لكنها أعلى من المملكة المتحدة، والتي تمثل 6% من المجموع الكلي. واختار التقرير 29 شركة ناشئة في مجال الأمن الإلكتروني، ومن بين هذه الشركات، هناك ست شركات إسرائيلية، لتصنف ما يسمى ببلد الشركات الناشئة، كثاني أعلى تركيز للعاملين في مجال الحماية الإليكترونية، بعد الولايات المتحدة.[٣٦]

---

[٣٤] Alex Kane, How Israel Became a Hub for Surveillance Technology.

[٣٥] Ibid.

[٣٦] شوشانا سولومون، إسرائيل تحصل على ثاني أكبر عدد من صفقات الأمن السيبراني على مستوى العالم، موقع تايمز أوف إسرائيل، 2018/4/16، انظر: http://ar.timesofisrael.com/?p=971007؛ وانظر:

Shoshanna Solomon, Israel wins second-largest number of cybersecurity deals globally, site of The Times of Israel, 15/4/2018, https://www.timesofisrael.com/israel-nabs-second-largest-number-of-cybersecurity-deals-globally/

ثالثاً: أداء الوحدة 8200 وأنشطتها:

تعدّ "إسرائيل" أحد أبرز محاضن تكنولوجيا الاتصالات، وأكثرها ازدهاراً في العالم،[٣٧] حيث قُدِّر حجم الصادرات الإسرائيلية للمنتجات الإلكترونية وصناعة أمن المعلومات خلال سنة 2018 بنحو خمسة مليارات دولار، في حين بلغ حجم الاستثمار في هذا المجال نحو مليار دولار، بزيادة ٢٢% عن سنة 2017، وبلغ عدد الشركات الإلكترونية في "إسرائيل" 450 شركة.[٣٨]

كما أن نصف شركات تكنولوجيا الاتصالات التي تحتل مراكز متقدمة عالمياً إما أنها اشترت شركات ناشئة إسرائيلية، أو أنها اشترت مراكز للبحث والتطوير لها في "إسرائيل"؛ فشركة سيسكو Cisco مثلاً، وهي شركة أمريكية رائدة في شبكات الإنترنت في العالم، تمتلك تسع شركات إسرائيلية وتسعى للمزيد.[٣٩] وفي سنة 2016، أعلنت الشركة عن عزمها الحصول على شركة أمن الإنترنت كلاودلوك CloudLock، التي أسسها سنة 2011 ثلاثة من عناصر الوحدة 8200، مقابل 293 مليون دولار.[٤٠] وكانت الشركة قد صرَّحت في سنة 2013، أنها ستشتري شركة إنتوسل Intucell الإسرائيلية لتصنيع البرمجيات مقابل نحو 475 مليون دولار نقداً، وذلك لتوسيع إدارة شبكات الهاتف المحمول.[٤١]

وخلال سنة 2018، قامت أفضل عشر شركات تقنية في العالم وهي؛ مايكروسوفت Microsoft، وآبل Apple، وأمازون Amazon، وجوجل Google، وفيسبوك Facebook، وعلي بابا Alibaba، وإنتل Intel، وأوراكل Oracle، وسامسونغ Samsung، وبايدو Baidu، بأعمال تطويرية لها في "إسرائيل".

فشركة إنتل مثلاً قررت استثمار 11 مليار دولار في "إسرائيل" في تطوير صناعاتها التكنولوجية والإلكترونية، وأعلنت أن صادراتها من "إسرائيل" بلغت 4 مليارات دولار سنة 2018، بزيادة قدرها 300 مليون دولار مقارنة بسنة 2017.[٤٢]

---

[٣٧] Site of The Times of Israel, UNIT 8200, https://www.timesofisrael.com/topic/unit-8200/

[٣٨] محمد وتد، "إنتل".. سلاح أميركي لمواجهة النفوذ الصيني بإسرائيل، الجزيرة.نت، 2019/1/31، انظر: https://bit.ly/2Go4v2r؛ وانظر:

Lilach Baumer, Israeli Companies Bagged a Fifth of All Cyber Venture Capital Investments in 2018, site of CTech, 30/1/2019, https://www.calcalistech.com/ctech/articles/0,7340,L-3755323,00.html

[٣٩] Dan Senor and Saul Singer, *Start-up Nation: The Story of Israel's Economic Miracle*, p. 17; and Cisco Systems, site of Wikipedia, https://en.wikipedia.org/wiki/Cisco_Systems

[٤٠] Abigail Klein Leichman, Cisco to pay $293 million for Israeli-founded CloudLock, site of Israel21c, 30/6/2016, https://www.israel21c.org/cisco-to-pay-293-million-for-israeli-founded-cloudlock/

[٤١] Mike Blake, Cisco to buy Israel-based software maker for $475 million, Reuters News Agency, 23/1/2013, https://uk.reuters.com/article/us-intucell-cisco-offering/cisco-to-buy-israel-based-software-maker-for-475-million-idUKBRE90M0PO20130123

[٤٢] Kahlon confirms Intel's NIS 40b Israel investment, site of Globes, 29/1/2019, https://en.globes.co.il/en/article-kahlon-confirms-intels-nis-40b-israel-investment-1001270735; and Steven Scheer, Ari Rabinovitch, Intel to get $1 billion state grant for $11 billion Israel chip plant expansion, Reuters News Agency, 28/1/2019, https://reut.rs/2RkOvSB

وشركة مايكروسوفت، التي تمتلك تاريخاً من الاستثمار في القدرات الإسرائيلية منذ سنة 1989، استعانت برئيس جديد للبحث والتطوير في "إسرائيل"، يبلغ من العمر 34 عاماً، وهو عضو "سابق" في وحدة 8200 التابعة للاستخبارات العسكرية الإسرائيلية.[٤٣]

كما صرَّح رئيس شركة مايكروسوفت بيل غيتس Bill Gates في سنة 2002، لصحيفة يديعوت أحرونوت Yediot Aharonot أن شركته ستستمر في الاستثمار وتطوير إنتاجها في "إسرائيل"، وقال إنه "على الرغم من الوضع السياسي والأمني، تواصل إسرائيل تمثيل الطليعة الرائدة في الابتكار، وستظل مايكروسوفت جزءاً منها". وقال إن المخاوف الأمنية "لن تمنعنا من تعميق أنشطتنا في إسرائيل".[٤٤]

واستثمرت مايكروسوفت مبلغاً لم يُكشف عنه في شركة تيم 8 أو Team 8، وهي شركة إسرائيلية لتشغيل الأمن الإلكتروني أسسها عدد من كبار العناصر "السابقة" في وحدة 8200. وقد شارك في تأسيسها ويشغل منصب رئيسها التنفيذي نداف زافرير Nadav Zafrir؛ الذي انضم إلى الوحدة 8200 سنة 2005 وشغل منصب قائدها في الفترة 2009–2013، وهو مؤسس القيادة الإلكترونية للجيش الإسرائيلي. وقال ناجراج كاشياب Nagraj Kashyap، نائب رئيس قسم المشاريع في شركة مايكروسوفت: "إن النظام البيئي التكنولوجي في إسرائيل معروف على مستوى العالم، بفضل ابتكاره وإبداعه، كما أن خبرته في مجال الأمن الإلكتروني بارزة بالفعل"، مشيراً إلى أن الشركة ستعمل بشكل وثيق مع شركة تيم 8 لمعالجة تحديات الدفاع عن الشبكات من المهاجمين.[٤٥]

وفي سنة 2011، قررت شركة أبل افتتاح مركز تطوير لها في "إسرائيل"، وهو أول مركز تطوير لشركة أبل خارج مقرها في كاليفورنيا، وتمّ تعيين أهارون أهارون Aharon Aharon رئيساً تنفيذياً للشركة.[٤٦] وأهارون، الذي عُيِّن في سنة 2016 أول مدير لسلطة الابتكار الإسرائيلية المستحدثة،

---

[٤٣] Amir Mizroch, What The World's Top 10 Tech Firms Have In Common, site of Forbes, 20/2/2018, https://www.forbes.com/sites/startupnationcentral/2018/02/20/what-the-worlds-top-10-tech-firms-have-in-common/#61b850ee2b3a

[٤٤] Allison Kaplan Sommer, Microsoft's Bill Gates: Israel is a vital resource for us, site of ISRAEL21c, 2/12/2002, https://www.israel21c.org/microsofts-bill-gates-israel-is-a-vital-resource-for-us

[٤٥] Site of Team8, https://www.team8.vc/about/about-us/; Nadav Zafrir, Team 8, https://www.team8.vc/member/nadav-zafrir/; Robert Hackett, Microsoft and Qualcomm Are Backing This Israeli Security Startup Studio, site of Fortune, 9/1/2017, http://fortune.com/2017/01/09/microsoft-qualcomm-citi-israel-security-startup-team8/; and Richard Behar, Inside Israel's Secret Startup Machine.

[٤٦] Shmulik Shelach, Apple to set up Israel development center, site of Globes, 14/12/2011, https://en.globes.co.il/en/article-1000706928

خدم في وحدة استخبارات الجيش الإسرائيلي 8200 وحصل على شهادتين من معهد تخنيون Technion الإسرائيلي للتكنولوجيا في هندسة الكمبيوتر والكهرباء.[٤٧]

وكشفت صحيفة يديعوت أحرونوت أن الشركة الإسرائيلية الناشئة برايمسنس PrimeSense والتي اشترتها آبل في سنة 2013 مقابل 350 مليون دولار، هي المسؤولة عن التطويرات والتقنيات الجديدة للتعرف على الوجه في جهاز الآيفون X أو iPhone X.[٤٨] وتأسست شركة برايمسنس سنة 2005 من قِبل خمسة مستثمرين من تل أبيب، خدموا جميعهم في الوحدة 8200، وهم: ديمتري رايس Dmitry Rice، وأليكس شبونت Alex Shpunt، وأوفير شارون Ofir Sharon، وآفياد مايسيلز Aviad Meisels، وتامير برلينر Tamir Berliner. ومن أهم المستثمرين الاستراتيجيين في الشركة، شركة مايكروسوفت.[٤٩]

كما صرَّح الرئيس التنفيذي ورئيس شركة جوجل إريك شميدت Eric Schmidt في مقابلة معه في حزيران/ يونيو 2009، أن الولايات المتحدة هي المكان الأول في العالم لرواد الأعمال، ولكن "بعد الولايات المتحدة، إسرائيل هي الأفضل".[٥٠] وكانت جوجل قد اشترت مقابل أكثر من مليار دولار تطبيق ويز Waze، وهو تطبيق يعتمد على البيانات الضخمة، طورته مجموعات "سابقة" من قبل قوات الجيش الإسرائيلية، وتأمل شركات ناشئة جديدة مثل ستايلت Stylit أن تحاكي نجاح ويز.[٥١]

وتأتي "إسرائيل" بعد الولايات المتحدة والصين، في عدد الشركات المدرجة في بورصة ناسداك NASDAQ، وهي سوق مالي أمريكي أنشئ سنة 1971، مقره الرئيسي في مدينة نيويورك. ووفقاً لأرقام منظمة التعاون الاقتصادي والتنمية OECD لسنة 2016، تنفق "إسرائيل" 4.3% من الناتج المحلي الإجمالي على الأبحاث والتطوير، وهي النسبة الأعلى في العالم، مقارنة بأي بلد آخر. فكوريا الجنوبية أنفقت ما نسبته 4.2% سنة 2016، بينما أنفقت الولايات المتحدة 2.8%. كما

---

٤٧ Eliran Rubin, Aharon Aharon, Apple Israel Chief, to Head Innovation Authority, *Haaretz* newspaper, 28/12/2016, https://www.haaretz.com/apple-israel-chief-to-head-innovation-authority-1.5479002; and Shoshanna Solomon, Apple's Aharon to head Israel Innovation Authority, site of The Times of Israel, 27/12/2016, https://www.timesofisrael.com/apples-aharon-to-head-israel-innovation-authority

٤٨ Israeli developers behind new iPhone X tech, Ynetnews, 19/9/2017, https://www.ynetnews.com/articles/0,7340,L-5018743,00.html

٤٩ Site of Consulate General of Israel in Petersburg, Russia, 25/11/2013, http://embassies.gov.il/spb/NewsfromIsrael/ScienceandTechnology/Pages/Apple-PrimeSense.aspx; and Shmulik Shelach and Tzahi Hoffman, PrimeSense in strategic cooperation talks, Globes, 16/7/2013, https://en.globes.co.il/en/article-1000862638

٥٠ Dan Senor and Saul Singer, *Start-up Nation: The Story of Israel's Economic Miracle*, p. 17.

٥١ Matthew Kalman, Israeli military intelligence unit drives country's hi-tech boom, *The guardian* newspaper, 12/8/2013, https://www.theguardian.com/world/2013/aug/12/israel-military-intelligence-unit-tech-boom

جمعت شركات التكنولوجيا الإسرائيلية رقماً قياسياً في رأس المال المخاطر (وهو أحد أشكال التمويل لمشاريع في أولى مراحل إنشائها، والتي تتميز بكونها تمتلك فرصة نجاح ونمو عالية، وفي الوقت نفسه يتسم الاستثمار فيها بمخاطرة عالية)، لتمويل الشركات الناشئة والذي بلغ 4.8 مليار دولار في سنة 2016.[٥٢]

كما حصلت "إسرائيل"، في قائمة بلومبرغ للبلدان المبتكرة Bloomberg's list of innovative countries وقائمة المنتدى الاقتصادي العالمي The World Economic Forum's الخاصة بأكثر عشرة اقتصادات ابتكاراً، على المركز الثالث في تقرير التنافسية العالمي 2017–2018 أو The Global Competitiveness Report 2017-2018 بعد سويسرا والولايات المتحدة الأمريكية.[٥٣]

ومن الجدير بالذكر أن شركة سيناريو Synereo الناشئة في "إسرائيل"، تحاول أن تُروِّج بأنها البديل المستقبلي لشبكات التواصل الاجتماعي. وهي شركة شارك في تأسيسها أندرسون ماكوتشيون Anderson McCutcheon، جندي "سابق" في الوحدة 8200. وتفخر سيناريو أنها أول شبكة تواصل اجتماعي لا مركزية وموزعة بالكامل في العالم، ويمكن للمستخدمين التفاعل مباشرة مع بعضهم البعض دون الحاجة إلى وسيط أو طرف ثالث، على عكس الحالة مع فيسبوك، وتويتر، وجوجل+ أو +Google، ولينكدإن Linkedin.[٥٤]

وبالتالي، لن تخصص "إسرائيل" إمكانياتها الكبيرة في هذا النطاق بالتجسس إلكترونياً على الفلسطينيين فقط، بل سيمتد ذراع التجسس الإلكتروني الإسرائيلي إلى أقصى حدٍّ ممكن أن يخدم مصلحتها.

1 . أنشطة الوحدة 8200 في البيئة الفلسطينية والعربية:

لا يقتصر دور العناصر "السابقة" في الوحدة 8200 على إنتاج بعض الشركات الناشئة الطموحة في "إسرائيل"، والتي يتم استغلالها في أنشطة الحرب الإلكترونية الإسرائيلية، بل إنها تساعد أيضاً في التوظيف لصالح الموساد والشاباك.[٥٥]

---

٥٢ Gross domestic spending on R&D, site of OECD, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm; John McKenna, South Korea and Sweden are the most innovative countries in the world, site of World Economic Forum, 6/2/2018, https://www.weforum.org/agenda/2018/02/south-korea-and-sweden-are-the-most-innovative-countries-in-the-world/; and John McKenna, Israel is a tech titan. These 5 charts explain its startup success, site of World Economic Forum, 19/5/2017, https://www.weforum.org/agenda/2017/05/tiny-israel-is-a-tech-titan-these-5-charts-explain-its-startup-success/

٥٣ John McKenna, South Korea and Sweden are the most innovative countries in the world, site of World Economic Forum, 6/2/2018.

٥٤ Israeli Startup Synereo Offers Decentralized Social Network, site of Jewish Business News, 28/1/2015, https://jewishbusinessnews.com/2015/01/28/israeli-startup-synereo-offers-decentralized-social-network/

٥٥ Richard Silverstein, New York Jewish Federation Executive, Veteran of IDF Cyber-War Unit 8200, site of Tikun Olam, 3/4/2014, https://www.richardsilverstein.com/2014/04/03/new-york-jewish-federation-executive-is-veteran-of-idf-cyber-war-unit-8200/

واستطاعت الوحدة 8200 أن تعترض في أوائل أيام حرب 1967 مكالمة هاتفية جرت بين رئيس جمهورية مصر العربية جمال عبد الناصر والملك الأردني الحسين بن طلال، وأكّد فيها عبد الناصر أن نتائج الحرب تجري لصالح مصر، وذلك لإقناع الملك الأردني بخوض الحرب ضدّ الإسرائيليين، إلا أن نشر المحادثة وتّر العلاقات بين زعماء الدولتين حينها لصالح "إسرائيل". وكذلك اعترضت الوحدة مكالمة هاتفية جرت بين ياسر عرفات ومسلحين تابعين لمنظمة جبهة التحرير الفلسطينية (أبو العباس)، الذين اختطفوا سنة 1985 سفينة الركاب الإيطالية أكيل لورو Achille Lauro في أثناء إبحارها في مياه المتوسط. وعندما ادعى ياسر عرفات أنه لا علاقة له بخطف السفينة، والتي أسفرت عن مقتل أمريكي، قدمت الوحدة 8200 مكالمة هاتفية تمّ اعتراضها لعرفات أثبتت عكس ذلك، وهو ما شكل رأي عام منحاز لـ"إسرائيل".[٥٦]

ودلت وثائق كشف عنها الأرشيف الرسمي الإسرائيلي بمناسبة مرور أربعين عاماً على حرب 1973، أن الوحدة مسؤولة عن ما بات يعرف بـ"الوسائل الخاصة"، والتي تتضمن زرع أجهزة تنصت في مكاتب ومرافق حيوية في عمق البلدان العربية، خصوصاً البلدان التي تكون في حالة عداء مع "إسرائيل".[٥٧]

وتحاول الوحدة 8200 أن تبتز الفلسطينيين من خلال المعلومات الشخصية والخاصة التي تقوم بجمعها عنهم، لإجبارهم على التعاون معها.[٥٨] وفي سنة 2014، وقّع 43 من العناصر "السابقة" في وحدة 8200، رسالة احتجاج تندد بالمشاركة في عمليات ابتزاز الفلسطينيين لتعزيز الاحتلال العسكري الإسرائيلي. وأشار الموقعون إلى أن أسلوب التجنيد الذي تتبعه الوحدة هو استغلال العيوب الشخصية أو نقاط الضعف بين الفلسطينيين، من أجل ابتزازهم ليصبحوا عملاء لها. ويعد اعتراض المحادثات الهاتفية الخاصة والرسائل النصية والبريد الإلكتروني أداة أساسية في هذه العملية.[٥٩]

---

[٥٦] Ronen Bergman, The Spies Inside Damascus; Yossi Melman, Foreign Report: Israel Has One of World's Largest 'Eavesdropping' Intel Bases, *Haaretz*, 5/9/2010, https://www.haaretz.com/1.5109596; and Richard Behar, Inside Israel's Secret Startup Machine.

[٥٧] صالح النعامي، "وحدة 8200".. ذراع التنصت الإلكتروني بإسرائيل، الجزيرة.نت، 2013/10/31، انظر:
https://www.aljazeera.net/home/Getpage/f6451603-4dff-4ca1-9c10-122741d17432/673dd7bd-b318-4294-b540-7b217d7397e0

[٥٨] Richard Silverstein, Unit 8200: Teaching NSA a Thing or Two About Dark Arts, site of Tikun Olam, 17/9/2014, https://www.richardsilverstein.com/2014/09/17/unit-8200-teaching-nsa-a-thing-or-two-about-dark-arts/

[٥٩] Richard Silverstein, IDF Unit 8200 Officers Refuse to Fight Palestinians, site of Tikun Olam, 12/9/2014, https://www.richardsilverstein.com/2014/09/12/israels-nsa-staff-refuse-to-fight-palestinians/; and Unit 8200, site of Wikipedia.

وفي آب/ أغسطس 2016، نشر باحثون في الأمن الرقمي في منظمة سيتيزن لاب Citizen Lab في جامعة تورونتو University of Toronto تقريراً مفصلاً عن مصدر نوع معين من برامج التجسس المتطورة، التي لديها القدرة على تحويل جهاز الآيفون iPhone الخاص بالشخص إلى جهاز مراقبة متحرك؛ يمكنه تتبع حركته وتسجيل مكالماته الهاتفية، والتحكم بكاميرا هاتفه والميكروفون. وقد استهدفت هذه البرامج أحمد منصور، وهو ناشط بارز في مجال حقوق الإنسان في الإمارات، بعد أن تلقى رسالة نصية على جهازه الآيفون الخاص به، وُعِدَ فيها بتقديم معلومات سرية حول استخدام التعذيب في البلاد، إذا نقر على رابط مرفق، وكان الرابط من برنامج التجسس بيجاسوس Pegasus، المطوَّر من قبل شركة أن أس أو NSO الإسرائيلية (وهي شركة مراقبة إسرائيلية سرية، أسسها عمري لافي Omri Lavie وشاليف هوليو Shalev Hulio، وهما عنصران "سابقان" في الوحدة 8200، ويعمل ثلاثة على الأقل من موظفي مجموعة أن أس أو في وحدة الاستخبارات، وفقاً لصفحات لينكدإن الخاصة بهم[٦٠])، والذي تمّ تحديده من قبل منظمة سيتيزن لاب، وصرحوا بأنه من المحتمل أن الإمارات العربية المتحدة هي التي استهدفته. وقال منصور إنه مستهدف منذ سنة 2011، وهي السنة التي وقّع فيها عريضة تطالب بالإصلاحات الديموقراطية في الإمارات. وخلص تقرير منظمة سيتيزن لاب إلى أن السبب وراء برنامج التجسس هو مجموعة أن أس أو. ويقضي أحمد منصور حكماً بالسجن لمدة عشرة أعوام في الإمارات بتهمة نشر أخبار غير صحيحة على مواقع التواصل الاجتماعي.[٦١]

وكشف تقرير لمنظمة سيتيزن لاب، نُشِرَ في 2014/7/31، أن التكنولوجيا التي طورتها مجموعة أن أس أو استهدفت حوالي 175 شخصاً منذ سنة 2016، بينهم ناشطون في مجال حقوق الإنسان ومعارضون، مشيراً إلى أن شركات إسرائيلية أخرى تقدم خدمات مماثلة. وبحسب التقرير، فإن "إسرائيل" تظل قادرة على ضبط بيع التكنولوجيا من خلال "القانون"، فحتى تستطيع مجموعة أن أس أو بيع التكنولوجيا للإمارات مثلاً، فإن عليها الحصول على تصريح وزارة الدفاع الإسرائيلية. ويشير التقرير إلى تقديم عامل سابق في مجموعة أن أس أو للمحاكمة في تموز/ يوليو، حيث وجهت له السلطات الإسرائيلية عدداً من الاتهامات، منها سرقة معلومات حساسة،

---

[٦٠] Alex Kane, How Israel Became a Hub for Surveillance Technology.

[٦١] شوشانا سولومون، سنودن في تل أبيب: تكنولوجيا إسرائيلية ساعدت السعوديين على قتل خاشقجي، تايمز أوف إسرائيل، 2018/11/7، انظر: http://ar.timesofisrael.com/?p=989163؛ وانظر:

Alex Kane, How Israel Became a Hub for Surveillance Technology; Hagar Shezaf and Jonathan Jacobson, Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays, *Haaretz*, 20/10/2018, https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027; and Neri Zilber, The Rise of the Cyber-Mercenaries, site of Foreign Policy, 31/8/2018, https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/

ومحاولة بيعها بـ 50 مليون دولار من خلال الإنترنت. وتعتقد ساشا رومانوسكي Sasha Romanosky، الباحثة في مؤسسة راند Rand Corp، أن "هذه الشركات تستعمل تقنيات أكثر تعقيداً من وكالات الاستخبارات الأمريكية".[٦٢]

وكانت الوحدة 8200 قد قدمت لمجموعة أن أس أو مبلغ 1.6 مليون دولار في شكل أموال ابتدائية لتطوير برنامج بيجاسوس. وتُعد عملية البيع التي جرت بين مجموعة أن أس أو والإمارات العربية المتحدة مؤشراً على العلاقات المتنامية بين "إسرائيل" والدولة الخليجية.[٦٣]

وفي سنة 2008، وبحسب صحف ومواقع إماراتية، أبرمت حكومة أبو ظبي اتفاقية بقيمة 3 مليارات درهم (816 مليون دولار) مع الشركة الأمنية آسيا جلوبال تكنولوجي (أيه جي تي) إنترناشيونال Asia Global Technology (AGT) International، التي ترأسها ماتي كوخافي Mati Kochavi. وتضمنت الصفقة تقديم كاميرات مراقبة، وأسيجة إلكترونية، وأجهزة استشعار لمراقبة البنية التحتية الاستراتيجية وحقول النفط في أبو ظبي، بما في ذلك تأمين حدود دولة الإمارات العربية المتحدة.[٦٤]

وأفاد الصحفي روري دوناجي Rori Donaghy في تقرير له بموقع Middle East Eye في شباط/ فبراير 2015، أن الإمارات وقّعت عقداً مع شركة أيه جي تي، وهي شركة مسجلة في سويسرا يملكها إسرائيلي، ويقال إن موظفي الاستخبارات الإسرائيليين "السابقين" يعملون فيها، لإنشاء نظام مراقبة يضم الآلاف من الكاميرات. وقال دوناجي، وهو أيضاً مؤسس مركز الإمارات لحقوق الإنسان، إن الإمارات اشترت بمئات الملايين من الدولارات من المنتجات الأمنية من "إسرائيل". وقال إن الإمارات تلجأ إلى "إسرائيل" لأنها تعتقد أن الإسرائيليين هم ببساطة الأفضل في هذا السوق من حيث معدات التجسس، والأكثر سرية.[٦٥]

---

[٦٢] فورين بوليسي: هذا دور إسرائيل في تصدير القرصنة السايبرية، عربي 21، 2018/9/2، انظر: https://arb.im/1119941؛ وانظر:

Bill Marczak, John Scott-Railton, and Ron Deibert, NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident, site of The Citizen Lab, 31/7/2018, https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/; and Neri Zilber, The Rise of the Cyber-Mercenaries.

[٦٣] Alex Kane, How Israel Became a Hub for Surveillance Technology; and Hagar Shezaf and Jonathan Jacobson, Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays.

[٦٤] Nissar Hoath, Security expo closes with mega contracts, site of Emirates24|7, https://www.emirates247.com/eb247/news/security-expo-closes-with-mega-contracts-2008-03-05-1.214771; Haseeb Haider, AIS wins home land deals worth $600 million, site of Khaleej Times, 27/2/2011, https://www.khaleejtimes.com/article/20110226/ARTICLE/302269893/1036; and Rori Donaghy, Falcon Eye: The Israeli-installed mass civil surveillance system of Abu Dhabi, site of Middle East Eye, 28/2/2015, http://www.middleeasteye.net/news/uae-israel-surveillance-2104952769

[٦٥] Rori Donaghy, Falcon Eye: The Israeli-installed mass civil surveillance system of Abu Dhabi.

وتقوم معدات المراقبة المستخدمة، بدءاً من الكاميرات الموجودة بالشارع وحتى الأجهزة الذكية المتصلة بالإنترنت في المنزل وما بعده، بتتبع الأشخاص "الذين يجب اتباعهم"، وتوفر كميات كبيرة من البيانات حول جميع جوانب تحركات الفرد وأنشطته. وتتواجد كاميرات سي سي تي في CCTV على جميع طرق أبو ظبي، وكذلك في كل منشأة عامة وتجارية، وكلها متصلة بنظام مركزي واحد يتم ربطه بدوره مع عملية تحليل البيانات الكبيرة، التي تقوم بدورها بإبلاغ السلطات بمستوى التهديد المتصور.[٦٦]

وأسست كوخافي سنة 2006 شركة لوجيك إندستريز Logic Industries، وهي شركة تنتج برامج أمنية، وتعمل من كيبوتس ياكوم Kibbutz Yakum في "إسرائيل"، ويرأس هذه الشركة عاموس مالكا Amos Malka، وهو ضابط متقاعد في الجيش الإسرائيلي، شغل منصب رئيس جهاز الاستخبارات بين سنتي 1998 و2001، ويحمل مجموعة من ضباط الجيش الإسرائيلي وضباط الاستخبارات المتقاعدين عدداً كبيراً من المناصب الرئيسية في الشركة،[٦٧] والسؤال هنا إلى أي مدى اخترق الإسرائيليون أمن الإمارات عن طريق هذه الأجهزة التي تمّ توفيرها؟

بن، الذي يعمل مستشاراً لشركات المراقبة في الإمارات، تحدث مع هآرتس *Haaretz* من مقر إقامته في الخليج العربي، وقال إن الشركات الإسرائيلية معروفة في المنطقة كمورد لمعدات التجسس، وإن الإمارات هي عميل كبير لتقنيات المراقبة، لأنها تعلم "أن أفضل التقنيات تأتي من إسرائيل".[٦٨]

وفي سنة 2018، أعلنت منظمة سيتيزن لاب بأن برنامج التجسس بيجاسوس قد استُخدم لتعقّب عمر عبد العزيز، وهو معارض سعودي يعيش في كندا تحت رعاية سياسية. ووفقاً لتقرير المنظمة، استخدم عملاء النظام في الرياض تكنولوجيا أن أس أو في مونتريال Montreal ضدّ عبد العزيز.[٦٩]

وبعد مقتل الصحفي السعودي جمال الخاشقجي، أقام عبد العزيز دعوى قضائية في 2018/12/2 ضدّ الشركة الإسرائيلية أن أس أو، مدعياً أن برنامج الشركة بيجاسوس كان يستخدم لاختراق هاتفه المحمول، من أجل تتبع المحادثات مع الصحفي السعودي جمال خاشقجي. وقد

---

[٦٦] Ibid.

[٦٧] Ibid.

[٦٨] Hagar Shezaf and Jonathan Jacobson, Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays.

[٦٩] Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak and Ron Deibert, "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," site of The Citizen Lab, 1/10/2018, https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/

نشرت شبكة سي أن أن مراسلات بين عبد العزيز وخاشقجي كانا يخططان فيها لإنشاء حركة على الإنترنت للشباب السعودي، تجابه دعايات النظام السعودي على الشبكات الاجتماعية.[٧٠] وقد وصف خاشقجي ولي العهد محمد بن سلمان بأنه لب المشكلة ويجب إيقافه. وقال عبد العزيز لشبكة سي أن أن "قرصنة هاتفي لعبت دوراً كبيراً في ما حدث لجمال، أنا آسف لهذا... الذنب يقتلني".[٧١] وكشفت تحقيقات أجرتها صحيفة هآرتس أنّ الشركة تفاوضت مع المملكة العربية السعودية لبيعها قدرات هجومية متطورة لاختراق الهواتف الخليوية.[٧٢]

وقال الموظف السابق في الاستخبارات الأمريكية إدوارد سنودن إن هناك علاقة بين مقتل الصحفي السعودي جمال خاشقجي، واستخدام السعوديين برنامج بيجاسوس المطور من قبل شركة أن أس أو، والذي تمّ التنصت على خاشقجي من خلاله.[٧٣] وكشفت صحيفة جيروزاليم بوست في تقرير لها، أن "إسرائيل" باعت أنظمة تجسس متطورة للمملكة العربية السعودية بقيمة 250 مليون دولار، بعد أن تلقى فريق فني سعودي تدريباً على تشغيلها. كما كشف التقرير عن أن البلدين تبادلا المعلومات العسكرية الاستراتيجية في الاجتماعات التي أجريت في واشنطن ولندن من خلال وسيط أوروبي.[٧٤]

وذكر تقرير لمنظمة العفو الدولية Amnesty International نشرته في آب/ أغسطس 2018، عن تلقي ناشطين سعوديين معنيين بحقوق الإنسان، ومنهم عددٌ من موظفيها، لرسائل مشبوهة عن طريق برنامج واتساب WhatsApp، تحتوي على رابط خبيث من برنامج التجسس بيجاسوس.[٧٥]

ونشرت صحيفة فايننشال تايمز Financial Times تقريراً في 2019/5/14، قالت فيه إن برنامج واتساب، المملوك لشركة فيسبوك، اكتشف في أوائل أيار/ مايو 2019 تعرضه لاختراق من برنامج

---

٧٠ Chaim Levinson, Amos Harel and Yaniv Kubovich, Khashoggi's Friend Sues Israel's NSO: Spyware That Hacked My Phone Had Major Role in Murder, *Haaretz*, 3/12/2018, https://www.haaretz.com/israel-news/.premium-khashoggi-associate-sues-israeli-cyber-firm-nso-had-major-role-in-murder-1.6704486

٧١ Nina dos Santos and Michael Kaplan, Jamal Khashoggi's private WhatsApp messages may offer new clues to killing, site of Cable News Network (CNN), 4/12/2018, https://edition.cnn.com/2018/12/02/middleeast/jamal-khashoggi-whatsapp-messages-intl/index.html

٧٢ Chaim Levinson, Amos Harel and Yaniv Kubovich, Khashoggi's Friend Sues Israel's NSO: Spyware That Hacked My Phone Had Major Role in Murder.

٧٣ فيديو، حسب سنودن.. هكذا شاركت إسرائيل بقتل خاشقجي، موقع قناة روسيا اليوم، 2018/11/8، انظر: https://ar.rt.com/l1b1؛ وشوشانا سولومون، سنودن في تل أبيب: تكنولوجيا إسرائيلية ساعدت السعوديين على قتل خاشقجي، تايمز أوف إسرائيل، 2018/11/7.

٧٤ Juliane Helmhold, Report: Israel Sold $250M. of Sophisticated Spy Systems to Saudi Arabia, *The Jerusalem Post* newspaper, 28/10/2018, https://www.jpost.com/Middle-East/Report-Israel-sold-250m-of-sophisticated-spy-systems-to-Saudi-Arabia-570539

٧٥ استهداف منظمة العفو الدولية بحملة تجسس تزودها شركة استخبارات، موقع منظمة العفو الدولية، 2018/8/1، انظر: https://www.amnesty.org/ar/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign

بيجاسوس، وتم استهداف هاتف محامٍ لحقوق الإنسان مقيم في المملكة المتحدة، رفض الكشف عن هويته، يساعد مجموعة من الصحفيين المكسيكيين ومنتقدي الحكومات والمعارض السعودي عمر عبد العزيز في مقاضاة أن أس أو في "إسرائيل"، مدعياً أن الشركة تتقاسم المسؤولية عن أي سوء استخدام لبرامجها من قبل العملاء.[٧٦]

وقال علاء محاجن، وهو محامٍ مقيم في القدس يتعامل مع دعاوى قضائية من المواطنين المكسيكيين والسعوديين، ويُمثِّل عمر عبد العزيز، ضدّ أن أس أو: "إنه أمر مزعج لكن ليس مفاجئاً أن فريقي قد استُهدف بالتكنولوجيا ذاتها التي نثيرها في دعاوى قضائية لدينا". وأضاف: "إن رد الفعل اليائس هذا لعرقلة عملنا وإسكاتنا، هو نفسه يدل على كم هذه الدعاوى القضائية عاجلة، إذ يمكننا نرى أن الانتهاكات مستمرة". وقال محاجن: "يبدو أن حديثها [أن أس أو] عن اختيار العملاء بعناية هو نكتة، لأنه لديها بالفعل العديد من العقود مع دول لديها سجلات حقوق إنسان مشكوك فيها للغاية، مثل المملكة العربية السعودية".[٧٧]

وأشارت الصحيفة إلى أنه في "إسرائيل"، لم يعد يستخدم العديد من كبار المسؤولين الهواتف الذكية، وقد تحدث أفيجدور ليبرمان، وزير الدفاع السابق، بفخر للمراسلين عن اقتنائه هاتف نوكيا القديم.[٧٨]

وبالرغم من إعلان شركة أن أس أو أن لديها عقوداً مع 21 دولة من أعضاء الاتحاد الأوروبي، إلا أن أحد المستثمرين في الشركة أفاد أن نصف واردات الشركة تأتي من الشرق الأوسط. كما أعرب الباحثون في جامعة تورونتو عن اعتقادهم بأن بيجاسوس قد استُخدم في 45 بلداً من ضمنها البحرين، والمغرب، والسعودية، والإمارات. وأشارت الصحيفة إلى أنه جاء في الدعوى القضائية المقدمة في "إسرائيل" أن الإمارات طلبت من أن أس أو اختراق هاتف أمير قطر، وأمير سعودي منافس، ومحرر صحيفة منشقة عن النظام السعودي ومركزها لندن.[٧٩]

وتواجه الشركة دعوتين قضائيتين في "إسرائيل" وقبرص، جاءتا بناء على تحقيقات جماعات حقوقية، تزعم أنها لاحقت هواتف صحفيين ومعارضين ومنتقدي الحكومات في كل من السعودية والمكسيك، بالإضافة إلى باحث في منظمة العفو الدولية، وزوجة الصحفي المكسيكي خافيير

---

[٧٦] Mehul Srivastava, WhatsApp voice calls used to inject Israeli spyware on phones, Financial Times, 14/5/2019, https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab

[٧٧] Ibid; and Mehul Srivastava and Robert Smith, Israel's NSO: the business of spying on your iPhone, Financial Times, 14/5/2019, https://www.ft.com/content/7f2f39b2-733e-11e9-bf5c-6eeb837566c5

[٧٨] Mehul Srivastava and Robert Smith, Israel's NSO: the business of spying on your iPhone, Financial Times, 14/5/2019.

[٧٩] Ibid.

فالديز Javier Valdez الذي قُتل سنة 2017، وهو ناشط ضد الفساد، تلقَّت رسائل نصية فيها تفاصيل عن اغتياله. كما وتدعم منظمة العفو الدولية مجموعة من المواطنين الإسرائيليين وجماعة الحقوق المدنية طلبهم من وزارة الدفاع إلغاء ترخيص تصدير أن أس أو.[٨٠]

وكشفت صحيفة هآرتس أن شركة فيرينت Verint، التي أسسها عناصر "سابقة" في الجيش الإسرائيلي في الوحدة 8200، زوَّدت البحرين بأنظمة تُستخدم عادةً من قِبل مراكز المراقبة، ونظام آخر يُستخدم لجمع المعلومات من الشبكات الاجتماعية. ويقوم الإسرائيليون، الذين يصلون البحرين بجوازات سفر أجنبية، ويحظر عليهم عادة التنقل في البلاد، بتدريب مسؤولي النظام على استخدام الأنظمة أو للقيام بأعمال الصيانة.[٨١]

وعقب الفشل الاستخباري الإسرائيلي في توقع الثورات العربية، أنشأت الاستخبارات العسكرية الإسرائيلية قسماً يتبع الوحدة 8200 لمراقبة وسائل الإعلام العربية، ومواقع التواصل الاجتماعي، لرصد توجهات العالم العربي من رسائل معادية نحو "إسرائيل" في أعقاب الثورات، وجمع المواد الإخبارية والتصريحات السياسية على مدار 24 ساعة، في جميع المواقع الفلسطينية والصفحات الشخصية لمسؤولين فلسطينيين وعرب.[٨٢]

وقال المراسل العسكري الإسرائيلي يوآف ليمور Yoav Limor في مقال له إن اضطرابات الربيع العربي أجبرت الوحدة 8200 على مراقبة وسائل التواصل الاجتماعي، مثل فيسبوك وتويتر Twitter، لرصد أي إشارات لتغيير قادم، خصوصاً بعد سقوط الرئيس المصري حسني مبارك، وسيطرة حماس على قطاع غزة، ولإحباط هجمات المقاومة، وتسلل المهاجرين، وإطلاق الصواريخ والقذائف على السياج الحدودي.[٨٣]

2. أنشطة الوحدة 8200 في البيئة الدولية:

استنتج الكاتبان دان سينور Dan Senor وساول سينجر Saul Singer في كتابهم "أمة الشركات الناشئة: حكاية معجزة إسرائيل الاقتصادية *Start-up Nation: The Story of Israel's Economic Miracle*"، أن السر في نجاح "إسرائيل" وحصولها على المركز التكنولوجي الذي هي عليه اليوم هو بحسب رأيهم في الجمع بين "العناصر التقليدية من المجموعات (العناقيد) التقنية، مع بعض

---

٨٠ Ibid.

٨١ Hagar Shezaf and Jonathan Jacobson, Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays.

٨٢ عدنان أبو عامر، **منظومة الأمن الإسرائيلي والثورات العربية** (بيروت: مركز الزيتونة للدراسات والاستشارات، 2016)، ص 158.

٨٣ Yoav Limor, Bringing intelligence to the field, *Israel Hayom* newspaper, 25/9/2012, http://www.israelhayom.com/2012/09/25/bringing-intelligence-to-the-field/

العناصر الإسرائيلية الفريدة التي تعزز مهارات وخبرات الأفراد، وتجعلهم يعملون سوية بشكل أكثر فعالية كفريق، وتصلهم بمعارف يتسمون بالترابط، ضمن مجتمع مؤسس ومتنامي".[٨٤]

كما تنبع قوة أمن "إسرائيل" من العلاقة الوطيدة بين الجيش الإسرائيلي وقطاع التكنولوجيا، ويتباهى هذا الجيش بقدراته الإلكترونية، التي تُعدُّ الأكثر تطوراً في العالم، وبحسب ادعاء ضابط كبير في الجيش الإسرائيلي: "نحن متقدمون على بقية العالم في القدرات الرقمية لمدة لا تقل عن 15 عاماً".[٨٥] ولكن استخدام هذه القدرات وانتشارها في العالم للتجسس على الشعوب أو الدول أو غيرها من الأسباب وبأساليب ممنهجة، وتبريرات غير كافية كمحاربة "الإرهاب" وغيرها، تشكل انتهاكاً صارخاً لحقوق الإنسان. وقال إيدن أومانوفيتش Edin Omanovic، وهو باحث في منظمة برايفسي إنترناشونال Privacy International: "من المثير للقلق أن قدرات المراقبة التي تم تطويرها في بعض وكالات التجسس الأكثر تقدماً في العالم... يتم تصديرها في جميع أنحاء العالم من أجل تحقيق الربح". وأضاف: "إن انتشار مثل هذه القدرات التدخلية أمر خطير للغاية، ويشكل تهديداً حقيقياً جوهرياً لحقوق الإنسان وإرساء الديموقراطية".[٨٦]

ومن المعروف أن الاستخبارات الإسرائيلية تستغل كل وسيلة ممكنة لاختراق البلدان المستهدفة لديها. لذلك ليس من قبيل الصدفة أن تقوم الوحدة 8200 بتطوير شبكة دولية من مجموعات من عناصرها التي تُوصف بأنها عناصر "سابقة". أما الهدف الظاهر فهو تقديم المساعدة المتبادلة في النهوض بالمهن والعلاقات الاجتماعية؛ غير أنه من المرجح أن هذه الكيانات توفر معلومات غنية للاستخبارات، في جهودها لاختراق شركات التكنولوجيا المتقدمة في الولايات المتحدة والدول الأخرى من خلال بيع منتجاتها، هذا بالإضافة إلى التخلص من "أعداء إسرائيل" حول العالم.[٨٧]

---

[٨٤] Dan Senor and Saul Singer, *Start-up Nation: The Story of Israel's Economic Miracle*, p. 138.

[٨٥] Kobi Finkler, Israel '15 years ahead' in cyber warfare capabilities, site of Arutz Sheva 7 (Israel National News), 16/2/2016, https://www.israelnationalnews.com/News/News.aspx/208126

[٨٦] Alex Kane, How Israel Became a Hub for Surveillance Technology.

[٨٧] Richard Silverstein, Unit 8200: 'First We Take Manhattan, Then We Take Berlin,' and Tokyo, and London…, site of Tikun Olam, 4/2/2017, https://www.richardsilverstein.com/2017/02/04/unit-8200-first-take-manhattan-take-berlin-tokyo-london/

ففي سنة 2011، أسست الوحدة 8200 جمعية خريجين رسمية ومنظمة، يقودها مجموعة من خريجي الوحدة البارزين في المجتمع الإسرائيلي، وتضم هذه الجمعية أكثر من 14 ألف خريج منتشرين في جميع أنحاء العالم، وهي تسعى لتوفير التوجيه المهني.[٨٨]

وأسست جمعية خريجي الوحدة 8200 بدورها برنامج EISP 8200 (برنامج دعم الريادة والإبداع)، الذي يسعى إلى التواصل ومساعدة الشركات الناشئة الإسرائيلية على اختراق الأسواق.[٨٩] ومن بين الخريجين مؤسسي شركات كبيرة مثل جيل شويد Gil Shwed؛ أحد مؤسسي شركة تشيك بوينت سوفتوير تكنولوجيز Checkpoint Software Technologies ورئيسها التنفيذي، الذي اخترع برنامج "جدار الحماية Firewall"، وعساف رابابورت Assaf Rappaport رئيس دائرة البحث والتطوير في شركة مايكروسوفت فرع "إسرائيل"، وهو قرصان إلكتروني (هاكر) شاب من الجيش، قام ببيع شركته الناشئة أدالوم Adallom إلى مايكروسوفت سنة 2015.[٩٠]

وفي سنة 2013، كشف الموظف السابق في وكالة الأمن القومي الأمريكية إدوارد سنودن، من خلال صحيفة الجارديان The guardian عن قيام الوكالة بالاحتفاظ بسجلات المليارات من المكالمات والرسائل النصية بشكل ينتهك الحرية الشخصية للأفراد، في أعقاب هجمات 11 أيلول/ سبتمبر 2001، سواء من داخل الولايات المتحدة أم بين الولايات المتحدة والدول الأخرى. وقد جُمعت المعلومات عبر برنامج بريسم Prism (الخاص بالتنصت، والذي يتلقى الدعم الفني من شركتي فيرينت وناروس، اللتان أُسستا من قِبل عناصر "سابقة" في الجيش الإسرائيلي في الوحدة 8200[٩١]) من شركة فريزون Verizon، وهي واحدة من أكبر مزودي الاتصالات في أمريكا.[٩٢]

---

٨٨ 8200 Alumni Network, site of 8200 EISP, https://www.eisp.org.il/en/the-program/8200-Network; and David Shamah, 8200 start-up boot camp turns entrepeneurs into tech warriors, site of The Times of Israel, 31/3/2014, https://www.timesofisrael.com/8200-start-up-boot-camp-turns-entrepeneurs-into-tech-warriors/

٨٩ Max Schindler, Unit 8200 Hits the Road in America, *The Jerusalem Post* newspaper, 25/10/2017, https://www.jpost.com/Israel-News/Unit-8200-hits-the-road-in-America-508381

٩٠ Amir Mizroch, Rise of Computer Vision Brings Obscure Israeli Intelligence Unit into Spotlight, site of Forbes, 28/5/2018, https://www.forbes.com/sites/startupnationcentral/2018/05/28/rise-of-computer-vision-brings-obscure-israeli-intelligence-unit-into-spotlight/#423216c3c193

٩١ What Was the Israeli Involvement in Collecting U.S. Communications Intel for NSA?, *Haaretz*, 8/6/2013, https://www.haaretz.com/did-israelis-gather-intel-for-the-nsa-1.5275806; and Richard Silverstein, IDF Unit 8200 Cyberwar Veterans Developed NSA Snooping Technology, site of Tikun Olam, 8/6/2013, https://www.richardsilverstein.com/2013/06/08/idf-unit-8200-cyberwar-veterans-developed-nsa-snooping-technology/

٩٢ Glenn Greenwald and Ewen MacAskill, NSA Prism program taps in to user data of Apple, Google and others, *The guardian* newspaper, 7/6/2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; Glenn Greenwald, NSA collecting phone records of millions of Verizon customers daily, *The guardian* newspaper, 6/6/2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; and Orr Hirschauge, In U.S. Snooping Affair, Israeli Firms at Risk, *Haaretz*, 10/6/2013, https://www.haaretz.com/israel-news/business/.premium-prism-could-wind-up-hurting-israeli-firms-1.5276753

واتُّهمت الشركتان الإسرائيليتان، ناروس وفيرينت، أنهما تمكنتا من تحويل كميات هائلة من البيانات إلى المخابرات الإسرائيلية.[٩٣]

وكذلك تمّ رصد رسائل البريد الإلكتروني وسجلات الدردشة وغيرها من البيانات المباشرة بالاستفادة من خوادم شركات التكنولوجيا الضخمة منها؛ مايكروسوفت، وياهو Yahoo، وجوجل، وفيسبوك، وبالتوك PalTalk، ويوتيوب YouTube، وسكايب Skype، وآي أو أل AOL، وأبل، وغيرها.[٩٤] وكانت شركة بوينغ Boeing، قد اشترت في سنة 2010، شركة ناروس، ومن ثم باعتها سنة 2014 لشركة سيمناتيك Symantec. أما شركة فيرينت فاحتفظت باستقلاليتها، بعد شراء حصة الأغلبية من مالكها السابق كومفرس تكنولوجي Comverse Technology في سنة 2013.[٩٥]

دافعت شركات التكنولوجيا هذه عن "تهم" التجسس بأنها لم تكن تعرف ما يحدث، وأنها لن تسمح بهذا الفعل مرة أخرى، وسوف تكون أكثر حذراً في المستقبل. وقالت وكالة الأمن القومي الأمريكية بعدما اعترفت بالتجسس، أنها لا تقرأ محتوى رسائل البريد الإلكتروني والمكالمات الهاتفية، ولكن تحتفظ بها فقط كسجلات الاتصالات.[٩٦]

وقال الصحفي الأمريكي المعروف بكتاباته عن الاستخبارات في الولايات المتحدة الأمريكية، وخصوصاً عن وكالة الأمن القومي الأمريكية، جيمس بامفورد James Bamford، سنة 2008، أن الوكالة وضعت اتفاقيات مع شركة أي تي أند تي AT & T، وهي أهم شركة اتصالات في أمريكا، من أجل الوصول إلى الكابلات التي يتم من خلالها تبادل الاتصالات، ومن أجل ذلك، بُنيت غرف سرية للوكالة داخل المباني المخصصة للكابلات في شركة أي تي أند تي. وشرح بامفورد كيفية تشغيل برنامج التجسس بريسم، وقال إن الاتصالات تدخل على كابلات المبنى، وتمر ببرنامج التجسس بريسم الذي يقوم بدوره عبر إشارات ضوئية إلى نسخ المكالمة، وبالتالي إطلاق نسخة من المكالمة إلى المكان الذي كان من المفترض أن تذهب إليه في نظام الاتصالات، والنسخة الأخرى تتحول إلى الغرفة السرية لوكالة الأمن القومي الأمريكية. وأوضح بامفورد أن الأجهزة والبرمجيات

---

[٩٣] Jon Rappoport, Two Israeli Companies: Spying on the World, site of middleeastrising, July 2017, http://www.middleeastrising.com/two-israeli-companies-spying-world/

[٩٤] Glenn Greenwald and Ewen MacAskill, NSA Prism program taps in to user data of Apple, Google and others; Glenn Greenwald, NSA collecting phone records of millions of Verizon customers daily, *The guardian* newspaper, 6/6/2013; and Orr Hirschauge, In U.S. Snooping Affair, Israeli Firms at Risk.

[٩٥] What Was the Israeli Involvement in Collecting U.S. Communications Intel for NSA?, *Haaretz*, 8/6/2013; and Jon Rappoport, Two Israeli Companies: Spying on the World.

[٩٦] Jon Rappoport, Two Israeli Companies: Spying on the World.

the hardware and the software الموجودة داخل الغرفة السرية، والتي تقوم بتحليل المكالمات داخل الكابلات، هي من صنع شركة ناروس.[٩٧]

وقال جيمس بامفورد أن الشركتين الإسرائيليتين، ناروس وفيرينت، لعبتا دوراً رئيسياً في تطوير وبيع التكنولوجيا، التي سمحت لوكالة الأمن القومي الأمريكية بنشر برنامج التجسس بريسم الخاص بها. وأضاف أن شركة ناروس، التي تأسست في "إسرائيل" ولديها اتصالات إسرائيلية كبيرة، تقوم بشكل أساسي بالتجسس على الاتصالات التي تجري عبر شركة أي تي أند تي الأمريكية، أما شركة فيرينت، والتي تأسست أيضاً في "إسرائيل"، فتقوم بالتجسس على الاتصالات التي تجري عبر شركة فريزون الأمريكية. وهاتان الشركتان متخصصتان برصد مليارات المكالمات، وتعملان كوسيط بين شركات الاتصالات ووكالة الأمن القومي الأمريكية.[٩٨]

وقال بامفورد إن المؤسس والرئيس التنفيذي السابق لشركة فيرينت يعقوب "كوبي" ألكسندر Jacob "Kobi" Alexander هرب سنة 2006 من الولايات المتحدة الأمريكية إلى ناميبيا، بتهمة الاحتيال الإلكتروني والتنصت، ثم عاد سنة 2017 إلى الولايات المتحدة وحُكم عليه بالسجن لمدة 30 شهراً. كما أن اثنين من كبار التنفيذيين في الشركة، والمحامي العام ومسؤول كبير آخر اعترفا أيضاً بهذه التهم. وأضاف أن هذه الشركات لديها علاقات خارجية محتملة مع وكالات استخبارات غير أمريكية، ولديهم مشاكل في المصداقية. وتراقب هاتان الشركتان حوالي 80% أو أكثر من الاتصالات الأمريكية؛ ومما يزيد الأمر سوءاً أن هاتان الشركتان توفران معداتهما إلى البلدان التي ليس لديها الكثير من الاحترام للحقوق الفردية، كفيتنام والصين وليبيا، وغيرها، للتجسس على شعوبها ومنع الاحتجاجات.

وتستطيع شركات الاتصالات هذه الوصول إلى أكثر الاتصالات الخاصة بين الناس في جميع أنحاء أمريكا بل والعالم. وفي بداية صيف 2008، توافق الديموقراطيون والجمهوريون على منح حصانة بأثر رجعي لهذه الشركات، للتجسس على المواطنين الأمريكيين، بحجة حماية الأمن القومي من "الإرهاب".[٩٩]

ويمكن للوحدة 8200 أن تخترق الكثير من شركات الهاتف والإنترنت العالمية من خلال الشركات التي أنشأها عملاؤها أو مجندوها "السابقون" كفيرينت، وناروس، وكومفرس، وغيرها؛

---

[٩٧] Ibid.

[٩٨] Ibid.

[٩٩] Ibid.

والتي وفَّرَت الأجهزة والبرمجيات للشركات العميلة المتواجدة في كندا، وفرنسا، وألمانيا، وإيطاليا، والصين، والولايات المتحدة؛ كشركة برازيل تيليكوم Brasil Telecom، وشركة شانغهاي تيليكوم Shanghai Telecom، وأورانج Orange S.A. (فرانس تيليكوم France Télécom S.A. سابقاً)، واتصالات مصر Egypt Telecom، وأي تي أند تي، ومايكروسوفت، وآبل. ولدى فيرنت وناروس معدات للاتصالات أيضاً في إيران، وتركيا، وسورية، ومناطق السلطة الفلسطينية، و"إسرائيل"، والعراق، والأردن.[١٠٠]

وفي تموز/ يوليو 2016، نشرت منظمة الخصوصية الدولية تقريراً كشفت فيه عن شركات إسرائيلية قدمت تقنيات مراقبة عبر الهاتف والإنترنت للشرطة السرية في أوزبكستان وكازاخستان، بالإضافة إلى قوات الأمن في كولومبيا. كما أن بنما، ومكسيكو، وترينيداد، وتوباجو، وأوغندا، كانت جميعها من عملاء تكنولوجيا التنصت التي طورتها مجموعة أن أس أو الإسرائيلية. وأضاف التقرير أن هذا التعاون بين "إسرائيل" والبلدان المتلقية يسهم في تعزيز العلاقات العسكرية والأمنية والديبلوماسية بينها.[١٠١]

وكشف تقرير آخر لمنظمة الخصوصية الدولية سنة 2014، عن تورط شركات إسرائيلية في تمكين الحكومات في آسيا الوسطى بالتجسس على مواطنيها. وجاء في التقرير أن شركتي نايس NICE Systems وفيرينت لتكنولوجيا المعلومات الإسرائيليتين، هما الجهتان الرئيسيتان اللتان زودتا المنظمات الأمنية في هذه البلاد بنظم تكنولوجية، من أجل التجسس على نشطاء حقوقيين وصحفيين ومواطنين. وقد شمل التقرير: طاجكستان، وقيرغيزستان، وتركمانستان، وأوزبكستان، وكازاخستان، وهي دول مصنفة عالمياً ضمن الدول الأكثر انتهاكاً لحقوق الإنسان، بحسب التقرير.[١٠٢]

وفي سنة 2015، قامت الوحدة 8200 بالقرصنة على "كاسبرسكاي لاب"، الذي يعد الرائد في البرمجيات المضادة للفيروسات، وبحسب تقرير لمجلة فورين بوليسي Foreign Policy، فقد اكتشفت

---

١٠٠ Eric Karlstrom, MossadGate: "NSA Prism" Mossad Spying Cousins Out of the Closet, site of Gang Stalking, 10/12/2016, https://www.gangstalkingmindcontrolcults.com/mossadgate-nsa-prism-mossad-spying-cousins-out-of-the-closet/

١٠١ Privacy International, "The Global Surveillance Industry," site of Privacy International, July 2016, https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf; Tim Johnson, How Israel became a leader in cybersecurity and surveillance, site of Miami Herald, 21/2/2017, https://www.miamiherald.com/news/nation-world/national/article134016704.html; and Alex Kane, How Israel Became a Hub for Surveillance Technology.

١٠٢ Oded Yaron, Israeli High-tech Companies Helping Central Asian Regimes Spy on Citizens, Report Says, *Haaretz*, 20/11/2014, https://www.haaretz.com/.premium-israeli-hi-tech-firms-help-regimes-spy-on-citizens-1.5332299

الوحدة أن شركة كاسبرسكاي هي بوابة خلفية للمخابرات الروسية للتجسس على عملائها، ومن ضمنهم أكثر من عشرين وكالة حكومية أمريكية.[١٠٣]

وتُعد إفريقيا ساحة مزدهرة أيضاً لمعدات التجسس الإسرائيلية، فقد ذكرت صحيفة هآرتس أن شركات إسرائيلية ومنها فيرينت باعت أنظمة متعلقة باعتراض الاتصالات والتجسس إلى سوازيلاند، وأنغولا، وموزامبيق، وإثيوبيا، وجنوب السودان، وبوتسوانا، ونيجيريا، وأوغندا. وقد استُخدمت هذه الأنظمة للتجسس على معارضي الأنظمة في تلك البلاد. ففي نيجيريا مثلاً، بيعت أنظمة التجسس في سنة 2012 إلى حكام الدلتا وبايلسا، وهما ولايتان في الاتحاد النيجيري، واستخدم حاكم بايلسا قبل انتخابات سنة 2015، هذه الأجهزة لمراقبة منافسه الرئيسي وزوجته ومساعديه، ولتحديد مكان واعتقال منتقدي النظام المعروفين.[١٠٤]

وفي سنة 2013، تمّ الكشف عن أن شركة إلبيت سيستمز Elbit Systems الإسرائيلية، وهي إحدى أكبر الشركات الإسرائيلية العالمية في مجال أنظمة الدفاع والأمن الإلكتروني، والتي يرأس قسم المعلوماتية والحلول الإلكترونية فيها وشارك في تأسيس هذا القسم يائير كوهين Yair Cohen، الذي خدم في الوحدة 8200 حوالي 33 عاماً، وقادها خلال الفترة 2001–2005، قد حصلت على عقد بقيمة 40 مليون دولار، لتوريد أنظمة للتحليل والتجسس والحماية الإلكترونية لنيجيريا. وقد تمّ تركيب هذه الأنظمة في مقر وكالة الاستخبارات الوطنية في العاصمة أبوجا، حتى بعد اعتراض الجمعية الوطنية النيجيرية عليها.[١٠٥] كما أعلنت إلبيت سيستمز التي تعمل مع "هيئة الجمارك وحماية الحدود بالولايات المتحدة U.S. Customs and Border Protection (CBP)" في بناء أبراج ثابتة للمراقبة مزودة بالرادارات والكاميرات، على طول 200 ميل تقريباً (نحو 322 كم) من الحدود في ولاية أريزونا، أنها مستعدة لنشر تلك المعدات في الولايات الحدودية الأخرى، بما في ذلك تكساس وكاليفورنيا. وأعلنت الشركة أنها مستعدة للمشاركة في حماية الحدود بين الولايات المتحدة والمكسيك عن طريق التكنولوجيا بدلاً من الحائط الإسمنتي غير المُتفق عليه.[١٠٦]

---

١٠٣ Neri Zilber, The Rise of the Cyber-Mercenaries.

١٠٤ Hagar Shezaf and Jonathan Jacobson, Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays; and Richard Behar, Inside Israel's Secret Startup Machine.

١٠٥ Ibid.

١٠٦ Emily Birnbaum, Trump, Dem talk of 'smart wall' thrills tech companies, site of The Hill, 31/1/2019, https://thehill.com/policy/technology/427929-trump-dem-talk-of-smart-wall-thrills-tech-companies

وعقدت شركة إلبيت سيستمز صفقات مع عدة دول، كفرنسا؛ إذ أعلنت الشركة في سنة 2011، أنها مُنحت، من خلال الشركة التابعة لها إليسرا .Elisra Electronic Systems Ltd، عقداً بقيمة خمسة ملايين يورو تقريباً (حوالي ستة ملايين دولار) لتجهيز وحدات تابعة لوزارة الدفاع الفرنسية؛ كسلاح الجو الفرنسي، والجيش، والبحرية بمعدات المراقبة.[١٠٧] كما مُنحت الشركة في إيطاليا عقداً بقيمة تزيد عن 15 مليون دولار لتزويد سلاح الجو الإيطالي بمعدات،[١٠٨] وكذلك مُنِحَت عقوداً أخرى في بريطانيا، ومقدونيا، ورومانيا، والفليبين، وعدداً من دول أمريكا الشمالية والجنوبية،... .[١٠٩]

ولفت تقرير لصحيفة فايننشال تايمز في 2019/5/14، النظر إلى أن الحكومة المكسيكية دفعت 32 مليون دولار سنة 2014 لشراء برنامج "بيجاسوس Pegasus 2 2"، المطور من قبل شركة أن أس أو، وفقاً لمكتب المدعي العام المكسيكي، مشيراً إلى أن الصفقة تضمنت خدمة من الشركة اسمها "رسالة هندسة اجتماعية محسنة"، بحيث يعمل ممثلو الشركة على صياغة رسالة نصية جذابة تدفع بالمستخدم للنقر عليها.[١١٠]

وفي سنة 2010 أعلن مختبر أبحاث شركة سيمانتيك Symantec، المتخصصة في أمن المعلومات، اكتشافه لفيروس ستكسنت Stuxnet، بعد أن تسبب 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 ناتانز Natanz، المُقام في منطقة شبه منعزلة عن العالم، تُحيطها أسلحة الجيش والحرس الثوري الإيراني من كل اتجاه، وأدى إلى توقف ما يقرب من ألف جهاز من أجهزة الطرد المركزي البالغ عددها خمسة آلاف، والتي كانت تقوم بتنقية اليورانيوم. ويُعد هذا الفيروس متطوراً جداً، وهو نتيجة أشهر طويلة من البحث والتحليل والتطوير المشترك بين المخابرات المركزية الأمريكية، ووكالة الأمن القومي الأمريكي، والموساد الإسرائيلي، والوحدة 8200، حسبما قال يائير كوهين. وكانت الهجمات على المفاعل ناتانز بأمر

---

١٠٧ Elbit Systems' Elisra to Supply Personal Search and Rescue Locator Beacons to the French Ministry of Defense, site of Elbit Systems, 19/6/2011, http://ir.elbitsystems.com/phoenix.zhtml?c=61849&p=irol- newsArticle&ID=1575276&highlight=

١٠٨ Elbit Systems to Supply DIRCM Systems to the Italian Air Force, site of Elbit Systems, 22/6/2011, http://ir.elbitsystems.com/phoenix.zhtml?c=61849&p=irol-newsArticle&ID=1576824&highlight=

١٠٩ Press Releases, site of Elbit Systems, http://ir.elbitsystems.com/; and Elbit Systems, https://en.wikipedia.org/wiki/Elbit_Systems#cite_ref-17

١١٠ Mehul Srivastava and Robert Smith, Israel's NSO: the business of spying on your iPhone, Financial Times, 14/5/2019.

من باراك أوباما Barack Obama، وكان الهدف منها، محاولة تعطيل البرنامج النووي الإيراني وتحجيمه إلى حين الوصول لاتفاق بشأنه مع إيران.[١١١]

الخلاصة:

إن انتشار التكنولوجيا ووسائل الاتصال الحديثة هو سلاح ذو حدين؛ فمن جهة، يمكن استخدامه من أجل تسهيل الاتصالات بين الأفراد، وتقريب المسافات بين الدول والحضارات المختلفة، ومن جهة أخرى، يمكن استخدامه في التسبب بأضرار جسيمة لأشخاص أو مؤسسات، أو دول في سبيل تحقيق أهداف معينة، وأصبحنا بذلك نعيش في بيئة افتراضية، يصعب أن يحكمها القانون.

سعت هذه الدراسة، التي حاولنا فيها إبراز بعضٍ مما استطاعت أن تحققه "إسرائيل" بتطويرها واستغلالها للتطور التكنولوجي الذي وصلت إليه، إلى توضيح أهدافها غير المعلنة لتحقيق مكاسب أمنية وسياسية واقتصادية على الصعيد الدولي من خلال استخدام هذه التكنولوجيا أو بيعها لشركات وحكومات ودول وجهات هي تختارهم، كما قال بنيامين نتنياهو في مؤتمر سايبرتك Cybertech في 2019/1/29، جعلتهم يصلون من خلالها وببساطة إلى ما يريدون من معلومات عن الشعوب، أو من خلال الطلب المباشر مثلاً من الشركات التجارية كجوجل، وياهو، وفيسبوك، ومايكروسوفت، وغيرها. وحتى لو تمنَّعت تلك الشركات من تقديم المعلومات المطلوبة، فلدى هذه الجهات من الإمكانات والأساليب ما يُمكِّنها من الحصول على الكثير مما تريد. وهذا يدفعنا للتساؤل؛ هل جمع الملفات الشخصية الشاملة للعملاء عند تحميلهم لتطبيق معين أو تفتيشهم على معلومات خاصة من جوجل مثلاً، هي لأغراض تجارية بحتة، تستهدف خدمة العميل، أم أنه قد تستفيد فيه بعض الجهات، بطرق مختلفة، لأغراض تجسسية؟

ما عرفناه عن الوحدة 8200، وما يتوفر من معلومات عنها على شبكة الإنترنت وفي الكتب والدراسات والأبحاث المنشورة هو مجرد قمة جبل الجليد. فالعنصر الثابت الذي يحيط بالوحدة منذ إنشائها هو السرية الصارمة، التي التزم بها جنودها في أثناء خدمتهم العسكرية وبعد الانتهاء منها.

---

[١١١] site of Symantec, W32.Stuxnet, https://www.symantec.com/security-center/writeup/2010-071400-3123-99; Yoav Limor, Bringing intelligence to the field; Ellen Nakashima and Joby Warrick, Stuxnet was work of U.S. and Israeli experts, officials say, *The Washington Post* newspaper, 2/6/2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.9608f9112b1f; David E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, *The New York Times* newspaper, 1/6/2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html; and Richard Behar, Inside Israel's Secret Startup Machine.

إن انتشار الوحدة 8200 وتسللها على مستوى العالم، من خلال عالم التكنولوجيا المتطورة، لا يعني بأنها الوحدة التكنولوجية الإسرائيلية الوحيدة التي أنتجها الجيش الإسرائيلي، بل يوجد العديد من الوحدات الأقل شهرة، ولكنها قد تضاهيها قوة وانتشاراً وتأثيراً.

ولعل هذه الدراسة تفتح الباب من جديد للبحث في باقي الوحدات السرية الإسرائيلية وأهدافها التي تسعى لها، كـ"وحدة 9900"، التي تُعدّ عين "إسرائيل" الفضائية، لاستخدامها الأقمار الصناعية للحصول على معلوماتها، وهي تتبع أيضاً لجهاز أمان الاستخباراتي. فما هي حقيقة هذه الوحدة؟ وإلى أين امتدادها؟

إن النهوض بالأمة العربية والإسلامية يجب أن يبدأ من العمل على تطوير القدرات الفردية والتكنولوجية لدى الفئة الشبابية، وتوفير البيئة المناسبة لهم للعمل فيها، والنظر من الأعلى بعين النسر عند توصيف المشاكل وتقييمها وطرح حلولها. ولعل التوصيات التالية تُسهم في وضع اللبنة الأولى نحو البدء بهذا المشروع بعيد المدى، علّنا نصل إلى نقطة التلاقي معهم أو نتفوق عليهم، وأن نحاربهم بأساليبهم لا نقف عند تطوير أساليبنا فقط.

التوصيات:

- العمل على تنمية الكوادر البشرية العاملة في المجال التكنولوجي، وخصوصاً في مجال أمن المعلومات.
- حثّ الجامعات على توجيه الطلاب نحو الدراسة التي تنفع في هذا المجال، وافتتاح مراكز للتطوير العملي.
- حثّ المراكز البحثية للبحث وكتابة الدراسات العلمية المتخصصة في المجالات التكنولوجية والقانونية المتعلقة بالجرائم الإلكترونية، لتوعية المجتمع وتحذيره.
- حثّ المؤسسات الإعلامية على توعية المجتمع عن مدى خطورة البرامج التجسسية، وما هي الدوافع الإسرائيلية وغير الإسرائيلية من ورائها.
- العمل مع المؤسسات الرسمية العربية والدولية والمراكز الحقوقية والإنسانية على تشريع قوانين دولية فعالة تحمي المواطنين من التجسس وخرق حرياتهم الشخصية، مع العلم أنه قد يكون من الصعب تطبيق هذه القوانين بشكل عملي، لأنه من النادر جداً إيجاد دلائل تكشف التجسس.
- نشر الوعي لدى مستخدمي الإنترنت بطرق حماية معلوماتهم وأمورهم الشخصية.

Abstract

Israeli Unit 8200 and its Role in

Serving Israeli Espionage Technology

Cyber espionage is considered a new form of wars to control individuals, institutions and states, and Israel is one of the leading incubators of information and communication technology. A large number of world leading companies either bought Israeli companies of such specialty, or established research and development centers in Israel.

This study attempts to shed light on the historical background of the Zionist intelligence activity, especially the founding of the Israeli Military Intelligence Unit 8200, which is specialized in cyber-surveillance technologies. The development of this unit was further discussed in addition to its activities in Palestinian, Arab and international arenas.

The study sought to highlight the undeclared objectives of Israel, which developed such technologies to seize security, political and economic gains at the international level.

Keywords:

Unit 8200	cyber espionage	Israel	security	cyber security	Israeli army

Series of Refereed Academic Articles (11)

Israeli Unit 8200 and its Role in Serving Israeli Espionage Technology

Fatima Itani

Al-Zaytouna Centre for Studies & Consultations