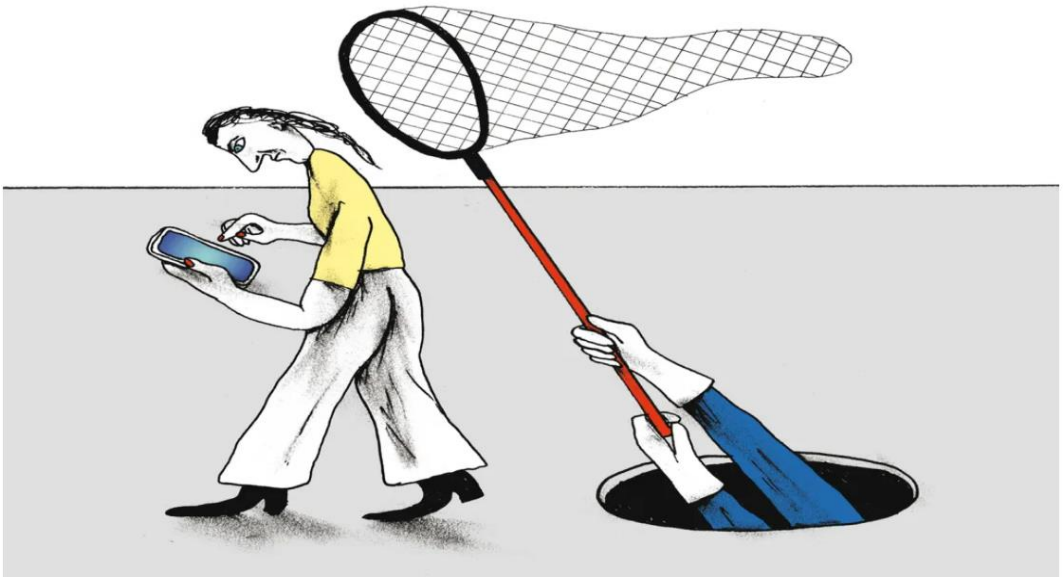
مختارات من الصحف العبرية

العدد 4106، 15-9-2023

نشرة يومية يعدها جهاز متخصص يلخص أهم ما في الصحف الإسرائيلية من أخبار وتصريحات وتحليلات لكبار المحللين السياسيين والعسكريين

مؤسسة الدراسات الفلسطينية
Institute for Palestine Studies

المحررة: رندة حيدر



كاريكاتور يرمز إلى تجسس شركات إسرائيلية على الهواتف الخليوية (نقلاً عن ملحق "كالكاليست")

في هذا العدد

متوفرة على موقع المؤسسة:

https://digitalprojects.palestine-studies.org/ar/daily/mukhtarat-view

مؤسسة الدراسات الفلسطينية
شارع أنيس النصولي ـ فردان
ص. ب.: 7164 ـ 11
الرمز البريدي: 1107 2230
بيروت ـ لبنان
هاتف
(+961) 1 868387 - 814175 - 804959
فاكس
(+961) 1 814193
ipsbeirut@palestine-studies.org
www.palestine-studies.org

[يوآف غالانت يلمّح إلى مسؤولية إسرائيل عن آخر الهجمات التي تعرضّت لها مواقع في الأراضي السورية]

"معاريف"، 2023/9/15

لمّح وزير الدفاع الإسرائيلي يوآف غالانت إلى مسؤولية إسرائيل عن الهجمات التي تعرّضت لها مواقع في الأراضي السورية أول أمس (الأربعاء)، وأسفرت عن مقتل جنديين سوريين وإصابة آخرين بجروح.

وجاء هذا التلميح في تصريحات أدلى بها غالانت خلال مراسم احتفالية بمناسبة رأس السنة العبرية الجديدة أقيمت أمس (الخميس)، وشارك فيها أيضاً رئيس الحكومة الإسرائيلية بنيامين نتنياهو، ورئيس هيئة الأركان العامة للجيش الإسرائيلي الجنرال هرتسي هليفي، وأعضاء هيئة الأركان العامة للجيش.

وقال غالانت: "تلقينا الليلة الماضية دليلاً آخر على أن هدير الطائرات في دولة إسرائيل أعلى من أي ضجيج آخر في الخلفية. وفي نهاية الأمر، فإن العبرة هي بالأفعال وليس بالأقوال."

وكانت وكالة الأنباء السورية الرسمية "سانا" أعلنت أن جنديين في الجيش السوري قُتلا، وأصيب 6 جنود آخرين في غارة جوية إسرائيلية استهدفت مدينة طرطوس الساحلية المطلة على البحر الأبيض المتوسط، كما أشارت إلى شنّ غارة إسرائيلية ثانية في وقت لاحق، استهدفت ضواحي محافظة حماة.

وبحسب المرصد السوري لحقوق الإنسان، استهدفت الغارة مستودعات لحزب الله في طرطوس، بينما استهدفت الغارة الثانية مستودعات أسلحة لميليشيات إيرانية في منطقة مركز البحوث العلمية في جبل قرية تقسيس في ريف حماة.

[الجيش الإسرائيلي يفرض إغلاقاً شاملاً على مناطق الضفة الغربية وعلى المعابر مع قطاع غزة خلال رأس السنة العبرية]

"يديعوت أحرونوت"، 2023/9/15

أعلن الجيش الإسرائيلي مساء أمس (الخميس) فرض إغلاق شامل على مناطق الضفة الغربية، وعلى المعابر مع قطاع غزة، خلال أيام عيد رأس السنة العبرية، وذلك بدءاً من منتصف اليوم (الجمعة) وحتى ليلة الأحد الاثنين المقبلة.

وجاء في بيان صادر عن الناطق بلسان الجيش الإسرائيلي أن رفع هذا الإغلاق سيكون مرتبطاً بتقييم الوضع الأمني، وأشار إلى أنه سيُسمح خلال فترة الإغلاق بمرور حالات إنسانية وطبية واستثنائية، بناءً على موافقة مسبقة من منسّق شؤون الحكومة الإسرائيلية في المناطق [المحتلة].

[14 عضو كنيست من أحزاب الائتلاف الحكومي يطالبون رئيس "الشاباك" بتحسين ظروف سجن قاتل عائلة دوابشة الفلسطينية]

"يديعوت أحرونوت"، 2023/9/15

طالب 14 عضو كنيست من أحزاب الائتلاف الحكومي رئيس جهاز الأمن العام الإسرائيلي ["الشاباك"] رونين بار بتحسين ظروف سجن قاتل عائلة دوابشة الفلسطينية عميرام بن أوليئيل، وشككوا في قرار إدانته، وفي مواقف قضاة المحاكم الإسرائيلية، ودعوا إلى تغيير القضاة.

وتمت إدانة بن أوليئيل بقتل سعد دوابشة وزوجته ريهام وطفلهما علي ابن العام ونصف العام، عندما قام بإلقاء زجاجة حارقة داخل منزل العائلة في قرية دوما في الضفة الغربية في تموز/يوليو 2015. وفي أيلول/سبتمبر 2020، حُكم عليه بالسجن بثلاثة مؤبدات و20 عاماً.

وجاء في رسالة أعضاء الكنيست إلى رئيس "الشاباك": "إننا نتوجه إليك، طالبين نقل بن أوليئيل إلى القسم التوراتي في السجن بأسرع وقت ممكن، فمن غير المعقول أن يبقى وحيداً في زنزانة في عزل كامل، وفي أشد ظروف السجن في دولة إسرائيل منذ سجنه قبل 7 أعوام ونصف العام." وأشارت الرسالة إلى أن الوضع النفسي لبن أوليئيل تدهور مؤخراً بسبب العزل المتواصل، ويوجد تخوّف كبير على صحته النفسية والجسدية. كما أشارت إلى أنه عشية عيد الفصح العبري الأخير، تمت المصادقة لأول مرة على طلب بن أوليئيل، الانتقال إلى القسم التوراتي في السجن، من أجل أداء فرائض العيد.

وقالت مصادر مسؤولة في قيادة جهاز "الشاباك" إنه قبل تلقّي رسالة أعضاء الكنيست هذه لم يعارض الجهاز نقل بن أوليئيل إلى القسم التوراتي خلال رأس السنة العبرية و"يوم الغفران" من أجل أن يشارك في دروس توراتية يقدمها حاخامون معتدلون، لكنه يعارض نقله بشكل دائم.

وبعث رئيس "الشاباك" برسالة إلى رئيس الحكومة بنيامين نتنياهو ووزير الدفاع يوآف غالانت، قال فيها إن بن أوليئيل لا يزال يشكل نموذجاً للتقليد في أوساط المستوطنين المتطرفين، وهو على اتصال بهم، ولذا، لا يمكن نقله إلى القسم التوراتي بشكل دائم. وأضاف أنه تبيّن من محادثات أُجريت مع سجناء في القسم التوراتي أن أياً منهم لا يريد أن يكون في زنزانة واحدة مع بن أوليئيل.

[المحكمة الإسرائيلية العليا تطالب ليفين والحكومة بتفسير أسباب عدم عقد اجتماع للجنة تعيين القضاة بشكل فوري]

"هآرتس"، 2023/9/15

أصدرت المحكمة الإسرائيلية العليا أمس (الخميس) أمراً احترازياً ضد وزير العدل ياريف ليفين يطالبه، هو والحكومة الإسرائيلية، بتفسير أسباب عدم عقد اجتماع للجنة تعيين القضاة بشكل فوري.

وجاء قرار المحكمة العليا هذا غداة قيام ليفين بشنّ هجوم حاد على المستشارة القانونية للحكومة الإسرائيلية غالي بهراف – ميارا التي انتقدت عدم عقد اجتماع للجنة تعيين القضاة، وأكد أنه لا ينبغي لأي طرف كان أن يتدخّل في قراره بشأن عقد اجتماع لهذه اللجنة.

ولا يُلزم قرار المحكمة العليا ليفين بعقد اجتماع للجنة تعيين القضاة، لكنه يعني أن هذه المحكمة ستنظر في طلبات الالتماس التي قُدمت إليها ضد قرار عدم عقد اجتماع لهذه اللجنة، وستُصدر قراراً بشأنها.

وطالب ليفين والحكومة المحكمة العليا بإلغاء الأمر الاحترازي، وأكدا أن المحكمة لا تمتلك صلاحية إصدار أمر كهذا.

[أوحانا: في حال قيام المحكمة العليا بإلغاء قانون تقليص حجة المعقولية، لدى الائتلاف الحكومي عدة مقترحات للالتفاف على هذه المحكمة]

"يديعوت أحرونوت"، 2023/9/15

قال رئيس الكنيست أمير أوحانا إنه في حال قيام المحكمة الإسرائيلية العليا بإلغاء قانون تقليص حجة المعقولية، توجد لدى الائتلاف الحكومي عدة مقترحات للالتفاف على قرارات المحكمة العليا، بينها إقامة محكمة دستورية لا تكون مؤلفة من قضاة فقط.

وجاءت أقوال أوحانا هذه في سياق مقابلة أجرتها معه صحيفة "يديعوت أحرونوت"، وستُنشر كاملة في الملحق الأسبوعي للصحيفة اليوم (الجمعة).

وأضاف أوحانا: "توجد لدينا أفكار متنوعة لمشاريع قوانين، سيطرحها الكنيست من أجل مواجهة الدوس عليه، وبينها إقامة محكمة للشؤون الدستورية. في هذه المحكمة الدستورية التي ستخوَّل النظر في مواضيع دستورية مطروحة على الرغم من أنه لا يوجد دستور لإسرائيل، وفي قيم وأفكار ومصطلحات من عوالم أيديولوجية، لن تكون أي أفضلية لخبراء القانون. ويمكن أن يجلس فيها مندوبو

الجمهور من مجالات متنوعة. وهذا هو أحد المقترحات بين مشاريع قوانين كثيرة سيتم بحثها عندما تقتضي الحاجة."

وطالب أوحانا المحكمة العليا بتقليص قوتها، وأضاف أنه يأمل بأن تدرك هذه المحكمة قيود قوتها، وتمتنع من التسبب بهذه الأزمة.

وتعقيباً على أقوال أوحانا هذه، قالت حركة "حرّ في بلدنا" المناهضة لخطة إضعاف الجهاز القضائي، إن ما كشف عنه النقاب رئيس الكنيست يثبت أن وجهة الحكومة الحالية هي نحو القضاء على أي جهة تمنعها من تحويل إسرائيل إلى ديكتاتورية، مثل المحكمة العليا والمستشارة القانونية للحكومة ورئيس هيئة أركان الجيش والقائد العام للشرطة والمؤسسة الأكاديمية ووسائل الإعلام.

[استطلاع "معاريف" الأسبوعي: في حال إجراء الانتخابات العامة الآن، سيحصل "معسكر نتنياهو" على 53 مقعداً ومعسكر الأحزاب المناوئة له على 57 مقعداً]

"معاريف"، 2023/9/15

أظهر استطلاع للرأي العام الإسرائيلي أجرته صحيفة "معاريف" أمس (الخميس) أنه في حال إجراء الانتخابات الإسرائيلية العامة الآن، سيحصل كلٌّ من قوائم معسكر الأحزاب المؤيدة لرئيس الحكومة بنيامين نتنياهو على 53 مقعداً (وهو عدد المقاعد نفسه الذي حصلت عليه في استطلاع الأسبوع الماضي)، في حين أن قوائم معسكر الأحزاب المناوئة له ستحصل على 57 مقعداً (بزيادة مقعد واحد عن عدد المقاعد الذي حصلت عليه في استطلاع الأسبوع الماضي)، وتحصل قائمة التحالف بين حداش [الجبهة الديمقراطية للسلام والمساواة] وتعل [الحركة العربية للتغيير] على 5 مقاعد، وتحصل قائمة راعام [القائمة العربية الموحدة] على 5 مقاعد، ولن تتمكن قائمة بلد [التجمع الوطني الديمقراطي] من تجاوُز نسبة الحسم (3.25٪).

ووفقاً للاستطلاع، ستحصل قائمة حزب الليكود برئاسة رئيس الحكومة بنيامين نتنياهو على 27 مقعداً، وتحصل قائمة تحالف "المعسكر الرسمي" برئاسة عضو الكنيست بني غانتس على 31 مقعداً، وتحصل قائمة "يوجد مستقبل" برئاسة عضو الكنيست يائير لبيد على 16 مقعداً.

وبيّن الاستطلاع أن قائمة حزب "الصهيونية الدينية" برئاسة الوزير بتسلئيل سموتريتش ستحصل على 5 مقاعد، وتحصل قائمة "عوتسما يهوديت" ["قوة يهودية"] برئاسة الوزير إيتمار بن غفير على 5 مقاعد، وتحصل قائمة حزب شاس لليهود الحريديم [المتشددون دينياً] الشرقيين على 9 مقاعد، في حين تحصل قائمة حزب يهدوت هتوراه الحريدي على 7 مقاعد، وتحصل قائمة حزب "إسرائيل بيتنا" برئاسة عضو الكنيست أفيغدور ليبرمان على 6 مقاعد، وتحصل قائمة حزب ميرتس على 4 مقاعد في حين أن قائمة حزب العمل برئاسة عضو الكنيست ميراف ميخائيلي لن تتمكن من تجاوُز نسبة الحسم.

وشمل الاستطلاع عيّنة مؤلفة من 525 شخصاً، يمثلون جميع فئات السكان البالغين في إسرائيل، مع نسبة خطأ حدّها الأقصى 4.3٪.

مقالات وتحليلات

عومر بن يعقوب – مراسل الشؤون السيبرانية
"هآرتس"، 2023/9/14

شركات إسرائيلية طوّرت قدرات تجسّسية مرعبة
وهذه المرة لا مجال للدفاع عن النفس

- هذه الحقيقة تحولت إلى مفهومة ضمناً: يلاحقوننا جميعاً في الشبكة العنكبوتية، تقريباً طوال الوقت. شركات التكنولوجيا وشركات الإعلانات يعرفون كل شيء عنا تقريباً – أين نتواجد، ماذا نشتري، وأي تطبيقات

نستعمل، وكيف نستعملها، وما هي أنماط الاستهلاك الخاصة بنا، وحتى ميولنا الجنسية. هناك فقط شيء واحد ومهم لا تستطيع شركات الإعلانات معرفته: هويتنا، التي يجب أن تبقى سرية.

- نحن نعرف كيف تجري الأمور على السطح: قرأنا منشوراً نشره صديق عاد من السفر، وفجأة يظهر لنا إعلان عن الفندق. إلا إن أغلبيتنا لا تعرف ما يجري خلف الكواليس.
- كل مرة ندخل فيها إلى تطبيق أو موقع، ومن دون أن تلاحظ عيوننا، تحدث عملية مفاوضات سريعة ومعقدة وعدوانية، تجسّد كل اقتصاد الإنترنت: خلال جزء من المئة في الثانية – اللحظة التي تمرّ بين الضغط حتى فتح الصفحة التي نريد – يجري مزاد تلقائي بين مئات آلاف الشركات الإعلانية المختلفة. يقاتلون على الحق في الإعلان لنا بالضبط في تلك الثانية. وكلما كانت المعلومات لديهم أكثر دقةً، وهادفة أكثر، كلما أصبح الاحتمال بأن نضغط أعلى، وهكذا يرتفع أيضاً ثمن الإعلان.
- لكن هناك مَن يعرف كيف يستغل هذه الثانية لمهمة اختراق مركّبة أكثر: إرسال إعلان خاص يبدو ساذجاً، لكنه يتضمن في داخله تطبيق تجسُّس متطور. هذا الإعلان الذي يبدو عادياً جداً، هو في الحقيقة سلاح سيبراني يستطيع اختراق الهاتف، أو الحاسوب الخاص بنا.
- سابقاً، كانت هذه القدرات محصورة في أجهزة الاستخبارات. كانت تستغل عالم الإعلانات الرقمي الذي يجب أن يكون سرياً من أجل تخطّي منظومات الحماية الخاصة بشركتيْ "آبل" و"غوغل"، ثم زرع تطبيق تجسُّس متطور فيها. وبحسب متخصص في التكنولوجيا، فإن "الحديث يدور عن قدرات تسمح بتحويل كل إعلان إلى رصاصة تكنولوجية لإصابة الجهاز."
- وإذا لم يكن هذا كافياً، فإن هذه التكنولوجيا بدأت تصل إلى الشركات التجارية. يكشف الآن تحقيق "هآرتس" ومكتب "الخدمات السرية" أنه خلال أزمة وباء كورونا، تطورت في إسرائيل صناعة سايبر وتجسُّس جديدة ومقلقة. طوّر بعض الشركات التكنولوجية الإسرائيلية تكنولوجيا تعرف كيف تستغل المنظومات القائمة لجمع المعلومات وملاحقة المواطنين، وهو ما يسمح بملاحقة مئات آلاف الأشخاص، إن لم يكن الملايين.

- التحقيق الذي يستند إلى محادثات مع أكثر من 15 مصدراً في مجال السايبر الهجومي وأجهزة الأمن والصناعات الأمنية الإسرائيلية، يكشف أن هناك مجموعة صغيرة من الشركات الكبرى تذهب أبعد من ذلك، وتستغل هذه التطبيقات بهدف الهجوم وزرع أجهزة التجسس. وبذلك، وفي الوقت الذي تنافس ملايين الإعلانات على الظهور على شاشاتنا، فإن شركات إسرائيلية تبيع تكنولوجيا تحوّل هذا الإعلان إلى سلاح يمكنه اختراق أجهزتنا.
- إحدى هذه الشركات التي يُكشف عنها هنا للمرة الأولى تُدعى إينست (Insanet). وكاسمها، هي مجنونة ببساطة، بحسب مصادر في المجال. الشركة التي أقامتها مجموعة من رجال الأعمال المعروفين في مجال السايبر، تتبع لمجموعة من المسؤولين السابقين في أجهزة الأمن، بينهم رئيس مجلس الأمن القومي سابقاً داني أرديتي. ويكشف التحقيق أن الشركة نجحت في تطوير تكنولوجيا تستغل الإعلانات بغرض التجسس. وليس اعتباطاً، منحت الشركة المنتوج اسم "شارلوك".
- أصحاب الشركة، بعضهم له علاقات قديمة وعميقة مع أجهزة الأمن، نجحوا في الحصول على تصريح من وزارة الدفاع لتسويق التكنولوجيا في العالم. عملياً، الشركة باعت التكنولوجيا والقدرات لدولة غير ديمقراطية.
- وبحسب نتائج التحقيق، هذه أول حالة في العالم فيها منظومة كهذه تباع كتكنولوجيا. شركة إسرائيلية أُخرى، تدعى ريزون، نجحت في تطوير منتوج مشابه، وحصلت هذا العام على مصادقة مبدئية لبيعه لزبائن في دول غربية، لكنه لم يُبَع بعد.
- الحقيقة المقلقة جداً هي أنه اليوم، لا يمكن حماية النفس من هذه التكنولوجيا، ومن غير الواضح ما إذا كان هناك طريقة لإيقافها. شركات التكنولوجيا، وعلى مدار السنوات، أغلقت الطريق أمام المئات من الاختراقات التي استطاعت شركات تجسُّس كـ"بيغاسوس" الدخول عبرها. هذا الأسبوع فقط، تم الكشف عن اختراق، وجرى إغلاقه في المحفظة الرقمية التابعة لـ"آبل" لزرع كود تجسُّس. ولكن حتى أكثر منظومات الدفاع المتطورة والذكية كتلك التي لدى "آبل"، أو "غوغل"، أو "مايكروسوفت"، لا

تعرف كيف يمكنها وقف تجسُّس من هذا النوع. أنظمة الإعلانات الخاصة بها كانت تُعتبر محمية تماماً حتى اليوم، يبدو هذا خطأً.

- هذه قصة تكنولوجيا تعرف كيف تحوّل الإعلان إلى أداة حرب في المعركة التكنولوجية. قصة منظومة تعرف كيف تتخطى قيود الحماية والخصوصية لـ"آبل" و"غوغل"، وتخترق الهاتف عبر استعمال معلومات إعلانية. هذه قصة عن العلاقة الخطِرة بين عالم الاستخبارات والسوق الخاصة: نموذج واضح مما يسمى "رأسمالية الملاحقة" – كيف يتم استغلال معلومات جمعتها جهات تجارية لأهداف استخباراتية، ويتحول – بمساعدة رجال أعمال إسرائيليين في مجال التكنولوجيا العالية الدقة – إلى منتوج أمني. هذه قصة عن الطريقة التي يتم فيها تسريب معرفة موجهة إلى القطاع الخاص، بشكل يحوّلها إلى سلاح ضد المواطنين، من دون رقابة ومحاسبة.

* * *

- في البداية، تمت صناعة اللافتة "البانر". في سنة 1994، اشترت شركة AT&T الإعلان الأول على الإنترنت من موقع Hot wired. وسأل الإعلان "هل ضغطت مرة بالماوس هنا؟ الآن ستضغط". النموذج كان فعالاً. وبحسب المعلومات التي جمعها الموقع لمصلحة المعلنين، فإن نصف الذين رأوا الإعلان ضغطوا وحققوا الهدف.
- بعد ذلك بثلاثين عاماً، لا نزال نضغط، لكن عالم الإعلانات اختلف كلياً. اليوم، يستند الإعلان إلى الهاتف الذكي، وهو بعيد كل البعد عن المصادفة. الإعلانات تعرف عنا الكثير جداً، وتستطيع مثلاً رصد مكاننا حتى الشارع الذي نحن فيه، إن لم يكن أمتاراً قليلة – وإحالة المعلومة على تاريخ البحث الخاص بنا.
- تحوّل عالم الإعلانات التكنولوجية عبر السنوات ليصبح وحشياً من حيث الحجم: آلاف الشركات، عشرات آلاف الأنواع لجمع المعلومات، والتحليل، والتصفية، وزيادة الجودة، ثم الاستهداف. وحول الإعلانات، بُنيَ اقتصاد موازٍ ضخم – هذه بورصات الإعلانات على الهواتف الذكية الخاصة

بآيفون وغوغل، والتطبيقات الكثيرة والمختلفة التي تُركّب عليها، حيث يتنافس المعلنون هناك طوال الوقت على الظهور على شاشاتنا.

- وكما قيل كثيراً: إذا كان هذا مجانياً؛ فنحن المنتوج. بورصات الإعلانات وأسواق المعلومات التي تقف خلفها هي سوق، نحن مَن يتاجرون بنا فيها.
- إلا إن هذه المعلومات التي لا تنتهي لا تُستعمل فقط على يد المعلنين. قبل عدة أعوام، اكتشف موظفون في هذا المجال أنه يمكن استعمال هذه البورصات أيضاً، بهدف استهدافنا للملاحقة والاستخبارات. هذا مجال غير معروف، ويُدعى (AD intelligence) Adlnt– استخبارات الإعلانات. الهدف منه تحويل المعلومات التي تم جمعها من أجل الإعلان إلى معلومات استخباراتية.
- بحسب مصدر يشغّل إحدى هذه الشركات، فإن "غوغل وآبل خلقتا سوقاً تجسُّسية." مضيفاً "كانوا يأملون بأن الناس لن يفهموا أن المعلومات التي يجمعونها هي بمثابة كنز ذهبي للاستخبارات. طريقة أُخرى لفهم الموضوع، هي أن آبل وغوغل هما بالأساس نوع من أنواع شركات التجسّس. ببساطة، هناك مَن يعرف كيف يستغل هذا."
- وبسبب الحساسية في هذه المعلومات، وبشكل خاص تلك المرتبطة بهاتفنا، يجب أن تكون المعلومات سرية. لكل هاتف ذكي هناك رقم هوية إعلانية، ويكون ربطه برقم الهاتف أو اسم الشخص مستحيلاً. الهدف واضح: عدم السماح بالتجسس على الهاتف وملاحقة أشخاص معينين، وعدم السماح لشركات الإعلانات باستغلال هذه المعلومات عنا. حتى أن قانون الخصوصية الأوروبي (GDPR) يمنع ذلك بشكل واضح.
- ولكن حتى المعلومات من دون اسم الشخص يمكن أن يكون لها قيمة كبيرة. مثلاً، من خلال تكنولوجيا الإعلانات، يمكن رصد كل الأشخاص الذين مروا من مطار معين في وقت معين. هذه الأداة يمكن استعمالها من أجل ملاحقة سلسلة العدوى ووقفها خلال انتشار وباء. أولاً، يتم جمع جميع الهويات الإعلانية التي كانت في المطار. هذه حركة بسيطة جداً: في كل مرة نفتح الهاتف وندخل إلى تطبيق يطرح إعلاناً، يرسل الهاتف إلى المعلن معلومات عن مكان وجودنا، بهدف زيادة نجاعة الإعلان المطروح

أمامنا. رصد هذه الهويات يخلق قائمة أشخاص كانوا في المطار لوقت معين. صحيح أن المعلنين لا يستطيعون معرفة أسماء هؤلاء الأشخاص، لكنهم يستطيعون تشخيصهم كأهداف يمكن الاستمرار في استهدافها. يبدأون بنشر الإعلان، وبذلك يلاحقون تنقلاتهم في العالم.

- وبذلك، بدأت خلال أزمة كورونا صناعة جديدة تسمى استخبارات الإعلانات الجماعية. شركة أقامها أريك بينون مثلاً، من الرياديين في مجال السايبر الهجومي الإسرائيلي، اقترحت على "الشاباك" خدمات تحديد الموقع والملاحقة المبنية على الإعلانات. وكما نشر غور مغيدو في "ذا ماركر"، فإن الفكرة كانت القيام بهندسة عكسية للمعلومات عن المتصفّحين في شركات الإعلانات الكبيرة، لأهداف استخباراتية. في هذه الحالة، كان الحديث يدور عن رصد جماعي لملاحقة انتشار الوباء.
- الشركة التي نتحدث عنها تُدعى Intelos، تسوّق منتوجاً استخباراتياً يستند إلى الإعلانات، يُدعى AdHoc لمصلحة شركات فرض القانون وزبائن تجاريين. منتوجاتها لا تخضع للرقابة، ولا تُعَد أمنية. هناك صناعة كاملة لشركات شبيهة. وكقاعدة، فإن الملاحقة العامة عبر الإعلانات غير مراقَبة من وزارة الدفاع لأنها تستند إلى معلومات يمكن شراؤها تجارياً. لكن يمكن تفعيل هذه التكنولوجيا أيضاً لأهداف أمنية – بالأساس لملاحقة أهداف مشتبَه فيها حتى من دون معلومات شخصية. مثلاً، يمكن تخيُّل حملة إعلانية موجهة إلى جمهور علماء في النووي من أصل إيراني من الفئتين العمريتين 35 و65 عاماً، مروا في العام الأخير من مطار طهران. وبعد تشخصيهم وحصولهم على الإعلانات الأولية، يمكن الاستمرار في استهدافهم لوقت طويل، وبذلك يعلمون إلى أين يذهبون ومتى.
- وفعلاً، ما بدأ كملاحقة مرضية ومحاولة رصد سلاسل العدوى، تحول سريعاً إلى مجالات أُخرى. فعلى سبيل المثال، بحسب وثائق وصلت إلى ملحق "هآرتس"، فإن الشركة الإسرائيلية Cobwebs، المتخصصة في مجال الاستخبارات، والتي تستند إلى معلومات علنية، ولذلك لا تحتاج إلى رقابة، تطرح تكنولوجيا تعرف كيف ترصد الموقع المحدد لهاتف عبر

معلومات إعلانية. هذه القدرة تشرح كيف يمكن ملاحقة هدف محتمل في إيران، ومن هناك، يمكن رؤية كيف تلاحق الشركة الهدف في كافة مناطق الدولة.

- نموذج إيران يشير إلى خصوصية استخبارات الإعلانات هذه: في الوقت الذي تستند أغلبية أنواع الاستخبارات الرقمية والسايبر الهجومي إلى الوصول المباشر إلى المعلومات والشبكات والبنى – تلك الموجودة لدى الدول فقط– فإن استخبارات الإعلانات تستند إلى معلومات تكون علنية، ويمكن رصدها عبر مصادر تُعتبر مفتوحة.
- يمكن شراء المعلومات من بنوك مختلفة، أو الوصول إليها بطرق إبداعية. فمن أجل رصد موقع شخص معين مثلاً، لا حاجة إلى أكثر من المعلومات الموجودة في بورصة الإعلانات الخليوية.
- وبحسب مصادر في هذا المجال، فإن اسم اللعبة هو مقارنة ذكية بين عدد كبير من مصادر المعلومات. حتى أن مجرد المشاركة في المسار، يمكن أن يكشف للمعلنين معلومات جغرافية – وذلك من دون علاقة بكون المعلن حقيقياً، أو تستخدمه شركة استخبارات.
- وبحسب مصدر في المجال، "من أجل القيام بعمل استخبارات الإعلانات، يجب بناء شبكة ضخمة من الإعلانات." مضيفاً "أنت بحاجة إلى أن تكون مرتبطاً بشبكات الإعلانات المختلفة للقيام بما لا تريد "آبل" أو "غوغل" القيام به – أن تلاحق الأشخاص، وحتى أن تستهدف شخصاً عبر البروفايل الإعلاني الخاص به."
- لذلك، فإن الشركات في هذا المجال عموماً، ترتبط بشركات إعلانات. حتى أنها أحياناً تفعّل شركات إعلانات خاصة بها، تمنحها الغطاء لعملها الاستخباراتي، وتمنحها إمكانية الوصول إلى المعلومات التي تحتاج إليها.
- يبدو من التحقيق أنه توجد سلسلة من الشركات الإسرائيلية التي تطرح خدمات الاستخبارات من هذا النوع لأنواع مختلفة من الزبائن. إحداها هي شركة ريزون، التي تُعتبر ريادية في هذا المجال، حتى انها اخترعت مصطلح Adlnt. المنتوج الخاص بها يُسمى Echo، ولا يخضع للرقابة

لأنه يستخدم معلومات علنية، ويتم بيعه لجهات خاصة، وأيضاً لجهات رسمية في الدولة، معنية بالشراء لملاحقة الفلسطينيين في البلد.

- هناك شركات أُخرى مع منتوجات أقل تطوراً. إحدى هذه الشركات هي B-Sightful، التي تسوّق قدراتها لجهات خاصة تعمل في مجال الإعلانات في العالم. وبحسب مصادر في المجال، فإن عمل الشركة يستند إلى مقارنة معطيات التصفح ومصادر المعلومات الإضافية التي يمكن شراؤها، أو الوصول إليها عبر الشبكة. اشترت هذه الشركة شركة سايبر أُخرى تدعى Cognyte، التي تعرض خدمات مشابهة – لكن للدول والجيوش. بما معناه، المعلومات ذاتها والتكنولوجيا ذاتها، مع استعمالات مختلفة: واحدة تجارية، والثانية استخباراتية.
- ولكن، هناك بعض الشركات التي لا تكتفي باستخدام الإعلانات فقط لجمع المعلومات والملاحقة، وتذهب أبعد من ذلك، تبني أدوات لاختراق الهواتف والأجهزة.
- كيف تعمل هذه الأدوات؟ أولاً، تركيب بروفايل إعلاني دقيق للجمهور المستهدف. واستناداً إلى هذا البروفايل، يتم بناء حملة إعلانية مخصصة لجمهور الهدف ونشرها عبر الإعلانات. وفي المرحلة التالية، يُزرع تطبيق تجسّس أو مضمون عدائي داخل الحملة ذاتها، وعبر المعلن، أو مجموعة المعلنين، يتم رفع الإعلان التجسسي في بورصة الإعلانات. حينها، يشاركون في البورصة ويستحقون المزيد من الإعلانات. وعندما ينكشف الهدف للإعلان، يتم اختراق هاتفه.
- تقول مصادر في هذا المجال أنه كان من الواضح منذ البداية أن هذا المجال سيتحول سريعاً إلى منزلق. ويقول أحد المصادر إن "استخبارات الإعلانات هي مجال شرعي"، مضيفاً "ما دام لا يزال في منطقة الملاحقة العامة. مَن يحوّل هذا المجال إلى سلاح يلعب بالنار. كل ما يجب القيام به هو اختراق واحد، استعمال واحد سيئ، يكفي إلى حرق الأداة برمتها."

* * *

- منذ أكثر من عقد ونصف، تدور لعبة القط والفأر بين الدول وبين الشركات

التكنولوجية العملاقة، فبعد انتقال الجميع إلى الهواتف الخليوية، خسرت أجهزة الاستخبارات القدرة على التنصت على المواطنين بواسطة شبكات الهاتف الثابتة. وتحولت الهواتف الخليوية إلى هواتف ذكية ومشفرة أكثر.

- وعلى الرغم من أن شركات آبل وغوغل وميتا تتعاون مع طلبات أجهزة الاستخبارات، وخصوصاً إذا كانت آتية من الولايات المتحدة ومن دول غربية أُخرى، فإنها لا تسمح بالوصول الكامل إلى المكالمات والأجهزة التابعة لها. ويوجد تفسير أساسي تقني لذلك: لا تريد هذه الشركات السماح للدول باستخدام هواتفها لأغراض تجسّسية حتى لو كانت شرعية، بالأساس في ضوء الحوادث التي استُخدمت فيها بصورة سيئة ضد الصحافيين ومنتقدي الأنظمة ونشطاء الدفاع عن حقوق الإنسان.
- لكن أجهزة الاستخبارات في كل أنحاء العالم متعطشة إلى الوصول إلى هذه الأجهزة، والصناعة السيبرانية الهجومية تعرض سلة حلول، بالتحديد على الدول غير القادرة على تطوير هذه القدرة بنفسها. بدأ هذا قبل أكثر من عقد مع قرصنة وتعقُّب شبكة الخليوي،
- واستمر مع قرصنة شبكة الإنترنت من خلال الخط الثابت، أو الواي فاي، وتطور مع متصفّحات وتطبيقات ورسائل نصية (sms) ذات مضامين مسيئة.
- القدرات الأكثر تطوراً التي انتشرت في الفترة الأخيرة وتعرّضت لانتقادات حادة هي تلك التي طورتها شركات إسرائيلية، مثل شركة NSO وCandiro، وبواسطة برامج التجسس التي طورتها، وأشهرها بيغاسوس، أصبح في الإمكان اختراق الهواتف الخليوية بواسطة تقنية Zero Click، أي من دون أن يعرف الشخص الذي تعرّض للهجوم بذلك، وبالتالي من دون أن يقوم بأي خطوة تمنع ذلك في جهازه.
- برامج التجسس، مثل بيغاسوس، في إمكانها التسلل إلى أي جهاز هاتفي وتحويله إلى أداة تجسّس تعمل ضد صاحبه، نظراً إلى ضُعف الحماية. والمقصود هنا شيء آخر. فهذه ليست محاولة للتسلل إلى الجهاز من الباب الخلفي، بل الدخول بصورة ذكية عبر نافذة أمامية، هذه النافذة مفتوحة

على مصراعيها بفضل عالم الإعلانات القوي على الإنترنت.

- وفي الواقع، هذه التكنولوجيا تسمح بإنشاء طريق دخول جديد إلى الجهاز "vector" (باللغة المهنية) بالنسبة إلى الذين يعرفون كيفية تطوير وسائل تجسّسية خاصة بهم، أو استخدام تلك الموجودة لدى شركة مثل NSO، إذا كان هناك مَن يعتبر بيغاسوس القنبلة الموقوتة في العالم الرقمي، فإن هذه القدرات الجديدة هي الصاروخ الموجّه الذي يحمل رأساً حربياً نووياً – رقمياً متطوراً.
- ليست صدفة محاولات شركات إسرائيلية سيبرانية تطوير تقنيات تستغل الإعلانات خلال الأعوام الأخيرة، ليس فقط للمراقبة، بل أيضاً للتجسس. وفي الواقع، خلال السنوات الخمس الأخيرة، يشهد هذا المجال سباقاً بين شركات، مثل Candiro، Paragon، Nemsis، وQuadri، وNSO نفسها.
- ووفقاً لجهات مطّلعة في هذا المجال، نجحتNSO في اختراع منتوج سمّته Truman، لكن لم يُسمح لها ببيعه. وحدها شركة Insanet سُمح لها ببيع هذا المنتوج حتى الآن.
- أنشأت شركة Insanet في سنة 2019 مجموعتان من رجال الأعمال. المجموعة الأولى مخضرمة في مجال السايبر، بينهم أريئيل أزيان، وروعي لامكين، وداني أرديتي، الذين حملوا معهم الاستثمارات المالية. والثلاثة معروفون بصفتهم المسوّقين لشركات، مثل NSO وParagon في أوروبا الغربية والشرقية، ولديهم علاقات جيدة مع أجهزة الاستخبارات.
- المجموعة الثانية مؤلفة من رجال أعمال شباب، جزء منهم لديه خلفية في منظومات سيبرانية إسرائيلية، وقدموا الفكرة قبل شركة Insanet، وأسّسوا شركة إعلانات، لكنهم باعوها قبل سنوات.
- وبفضل خبرتهم في المؤسسة الأمنية وفي مجال الإعلانات، نجحوا في شركة Insanet في تطوير "شرلوك"، أداة تستغل شبكة الإعلانات من أجل قرصنة فعالة لأجهزة الكومبيوتر والهواتف الخليوية.
- ومن أجل تسويق هذا المنتوج، بحثت الشركة عن تعاوُن مع شركات سيبرانية هجومية أُخرى. في وثيقة تسويق Candiro التي نشرها أميتي زيف في "ذا ماركر" في سنة 2019، يُعرض على الزبون المحتمل شراء

"شارلوك" مع برامج تجسّس أُخرى طورتها الشركة. ويبرز في الوثيقة أن ثمن البرنامج باهظ جداً: استخدام "شارلوك" للملاحقة يكلف الزبون خمسة ملايين يورو.

- وتكشف الوثيقة أن برنامج "شارلوك" قادر على اختراق كومبيوترات Windows وهواتف آيفون وأندرويد. حتى الآن، هناك شركات تخصصت في قرصنة أجهزة مختلفة، فشركة Candiro ركزت على الكومبيوترات الشخصية، وNSO عرفت كيف تخترق آيفون، ومنافسوها تخصصوا في اختراق أندرويد. لكن مع شبكة من هذا النوع، في الإمكان الوصول إلى أي جهاز.
- يقول دونا أو سربهايل رئيس طاقم أمنستي – تك إن "هذه الأدوات خطِرة جداً. ويمكن استخدام هذه المنظومة الهجومية لاستهداف أشخاص على أساس ديموغرافي أو سلوكي، يجري جمعها من خلال الإعلانات. على سبيل المثال، يمكنك استهداف مجموعة إثنية معينة، أو أشخاصاً زاروا موقعاً إخبارياً معيناً ينتقد السلطة، وهذا تطوّر خطِر."

* * *

- على الرغم من المخاوف، فإن منتوج Insanet يُباع بصورة قانونية بموافقة إسرائيل. وحصلت الشركة على تصريح متساهل من وزارة الدفاع فيما يتعلق بتقنيات سيبرانية حساسة. وبفضل هذا التصريح، نجحت الشركة في استكمال صفقة كبيرة.
- لكن بعد التصريح الأولّي، وُضعت عليه قيود كبيرة. تقول مصادر في المجال إن التغيّر نجم عن خوف حقيقي، وهو ثلاثي الأبعاد: تخوف من تسرّب القدرة، ومن الغضب الأميركي، ومن غضب شركات تكنولوجية عملاقة، الغاضبة أصلاً من الصناعة السيبرانية الإسرائيلية (على سبيل المثال، فايسبوك وآبل تقاضيان شركة NSO).
- لهذا السبب، جرى تقييد التصريح بصورة كبيرة. واليوم يمكن بيع "شارلوك" كمنتوج هجومي، لكن ضمن شروط محدودة جداً. ومن أجل بيعه لزبون محتمل في الغرب، المطلوب الحصول على موافقة محددة من وزارة

الدفاع التي لا تمنحها دائماً.

- قصة شركة Insanet وشبيهاتها هي قصة إسرائيلية كلاسيكية: روح مبادرة تكنولوجية متقدمة ومتحدية كي لا نقول استغلالية، آليات رقابة عفا عنها الزمن غير قادرة على
- مواجهة وتيرة الاختراعات وشهية العالم اللانهائية للتقنيات المتطورة. وتتخوف مصادر في هذا المجال من أن القدرة على مراقبة وكبح استخدام هذه التقنيات الخطِرة تزداد ضعفاً. وجزء يعتقد أن هذا المجال خرج عن السيطرة...
- حتى الآن، الشركات التي تعتبر أنها تعمل انطلاقاً من مصادر علنية مع زبائنها المدنيين ليست مراقبة البتة. في المقابل، الشركات العالمية في المجال السيبراني تخضع لرقابة دقيقة.
- لكن الحدود ليست واضحة دائماً، والقيود لا تعمل دائماً. مثلاً، بعد حصول شركة NSO على ترخيص لتصدير منتوجها في هذا المجال، مُنع موظفو الشركة من إخبار زبائنهم المحتملين عن وجود المنتوج، ودرست الشركة إمكانية دمج هذه التكنولوجيا في برنامج بيغاسوس...
- بمرور الوقت، ازداد إدراك وزارة الدفاع أنه من الصعب المحافظة على هذه القدرات. والدولة التي سمحت بنشاط استخباراتي إعلاني من دون رقابة، بحجة أن المقصود "استخبارات من مصادر علنية"، خسرت قدرتها على كبح السوق الهجومية التي برزت على ظهرها. ومن أجل منع حجج فلان وعلان، أخيراً قررت وزارة الدفاع هذه السنة منح شركة رايزون Raizon ترخيصاً لمنتوج اختراق فعال.
- حالة شركة رايزون تدل على مدى وحشية السباق على التسلح الدائر في هذا المجال. لسنوات طويلة، تجنبت شركة رايزون إنتاج منتوج مسيء، واقتصرت على معلومات استخباراتية تعتمد على الموقع الجغرافي ومراقبة الاتصالات غير المشفرة. بمعنى آخر، لا يمكن معرفة مَن يتحدث، ومع من، ومتى. لأن هذه خاضعة للرقابة، وهي تعتمد على جمع معلومات تُعتبر حساسة وغير علنية...
- في إسرائيل يُدرس إخضاع كل المصادر العلنية للرقابة. وفي الأشهر

الأخيرة، تجري محادثات لتغيير الرقابة في هذا المجال. وتغيير السياسة نابع من ردة فعل وزارة الدفاع على التغيير الذي طرأ على هذا المجال. وبعد أعوام، تمارس إسرائيل حالياً ضغطاً على الصناعة السيبرانية.

- وقبل عامين، قررت الدولة الاستجابة للضغط الأميركي وكبح برامج السايبر الهجومي وتقليص قائمة الدول المسموح التصدير لها. ومن قائمة تشمل 100 دولة، سُمح فقط لـ40 دولة، أغلبيتها غربية. ونتيجة ذلك، أغلقت الشركات الإسرائيلية التي كانت تعتاش من زبائن في دول العالم الثالث أبوابها.
- هذه الخطوة كانت ناجحة جزئياً، وكان لها تداعيات إشكالية على السوق، فقد دفعت عشرات الإسرائيليين إلى المغادرة إلى أوروبا والولايات المتحدة، وهناك نشأت صناعة سيبرانية هجومية مزدهرة تحاول استغلال أفضل القراصنة الإسرائيليين...
- في وزارة الدفاع، نشأ تخوف حقيقي من أن تصبح هذه القدرات التكنولوجية ملكاً لشركات أجنبية غير خاضعة للرقابة، وعلى أمل إبقاء هذا المجال الجديد في البلد وتحت الرقابة، قررت هذه السنة تنظيم المجال، بهدف إرضاء هذه الصناعة قليلاً.

* * *

- كلنا يعلم بأن هذه الأدوات للمراقبة المتطورة يمكن أن تستخدمها دول ضدنا. في السنوات الأخيرة عرف الناس أن دولاً ليست غربية، في أفريقيا، وفي الشرق، وفي أميركا الوسطى، وفي العالم العربي، حصلت على هذه القدرات، ليس بقدراتها الخاصة، بل من خلال شرائها من السوق الدولية والخاصة.
- هذه القدرات التي طورتها شركات إسرائيلية، الهدف منها منع الإرهاب والجريمة، تُستغل بصورة سيئة أيضاً من جانب دول غير ديمقراطية وغير ليبرالية. ومثل كل سلاح، إلى جانب السوق المراقبة والشرعية، تنشأ دائماً أسواق سوداء تكون الرقابة عليها قليلة، تبيع هذه التقنيات لدول مشكوك

فيها تمنع إسرائيل بيعها لها، أو لكيانات خاصة. وتحذّر مصادر في هذا المجال هذه المرة أيضاً، كما جرى في السايبر الهجومي، من حدوث تداعيات مشابهة في هذا المجال.

المصادر الأساسية:

صحيفة "هآرتس"
- النسخة المطبوعة
- النسخة الالكترونية بالعبرية http://www.haaretz.co.il
- النسخة الالكترونية بالإنجليزية http://www.haaretz.com

صحيفة "يديعوت أحرونوت"
- النسخة المطبوعة
- النسخة الالكترونية بالعبرية http://www.ynet.co.il
- النسخة الالكترونية بالإنجليزية http://www.ynetnews.com

صحيفة "معاريف"
- النسخة المطبوعة
- النسخة الالكترونية بالعبرية http://www.nrg.co.il

صحيفة "يسرائيل هيوم"
- النسخة المطبوعة
- النسخة الالكترونية بالعبرية http://www.israelhayom.co.il

المواقع الالكترونية لأهم مراكز الأبحاث في إسرائيل.

صدر حديثاً

العولمة والعبرنة في المشهد اللغوي العربي الفلسطيني في إسرائيل

تأليف: محمد أمارة
تدقيق وتحرير لغوي: نرمين عباس

محمد أمارة، محاضر وباحث في علوم اللغة الاجتماعية في العديد من الجامعات والكليات.

يفحص هذا الكتاب – بصورة معمقة تجليات العولمة والعبرنة فى المجتمع العربى الفلسطينى فى إسرائيل من ناحية، وتأثيراتها وإسقاطاتها عليه من ناحية أُخرى، ولا سيما فيما يتعلق بالهوية واللغة العربية والمشهد اللغوى. ويعاين مدى تغلغل ظاهرة العبرنة – مع كل ما تحمله من دلالات لغوية وأيديولوجية – وتشابكها مع الأسرلة والعولمة والتكنولوجيا، ثم تأثير ذلك كله فى هذا المجتمع. كذلك يرصد الكتاب مظاهر العبرنة والعولمة فى المشهد اللغوى العربى الفلسطينى فى إسرائيل من خلال عبرنة أسماء المواقع العربية، وأسماء المحال التجارية، والمشهد اللغوى فى المدارس، ومدى استعمال المواطنين الفلسطينيين للغة العبرية واللغات الأجنبية، وخصوصاً الإنكليزية. ويتناول مسألة اللغة البينية التى يُطلق عليها أيضاً: "الهجين اللغوى"، أى الخلط ما بين لغتين.

يتمحور الكتاب حول المنحى اللغوى لدى المجتمع العربى الفلسطينى فى إسرائيل الذى مر بتحولات جيو – سياسية هائلة فى أعقاب النكبة، وأصبح أبناؤه أقلية مهمشة داخل الدولة، ومروا بمجموعة من التغيرات التى مست بنيتهم الاجتماعية والاقتصادية والهوياتية، فضلاً عن لغتهم العربية ومخزونهم اللغوى.