انقر، حمّل، اقتل:

نظرة على صناعة الأسلحة السيبرانية في منطقة غرب آسيا وشمال أفريقيا

SMEX

شكر وتقدير

أنجزت منظمة "سمكس" هذا البحث بدعم من منظمتَيْ FIND (find[.]ngo) و"أكسس ناو" (Access Now). يعرب مؤلّفو هذا التقرير عن بالغ امتنانهم لستيفن فيلدستاين وجيمس شايرز و"V" على ملاحظاتهم وإرشاداتهم القيمة التي ساهمت في إعداد هذا العمل.

"سمكس" منظمةٌ غير ربحية تُكرّس عملها لحماية حقوق الإنسان في الفضاءات الرقمية في منطقة غرب آسيا وشمال أفريقيا. ونحن نسعى إلى ضمان وصولٍ آمنٍ وغير خاضعٍ للرقابة إلى الإنترنت وخدمات الهاتف المحمول والفضاءات الشبكية في المنطقة وخارجها.

نُشر هذا البحث في العام 2025 من قبل "سمكس".

للمزيد من المعلومات، زوروا موقع www.smex.org.

الملخص التنفيذي

مع تزايد الوقت الذي نقضيه على الإنترنت، أصبحت الخصوصية، وهي أحد حقوق الإنسان الأساسية المنصوص عليها في القانون الدولي، أكثر أهمية من أي وقت مضى.[1] ومع ذلك، يظل الحق في الخصوصية معرضاً للانتهاك باستمرار.

على الرغم من تغيّر مفهوم "الحق في الخصوصية" مع مرور الزمن، قدّم صاموئيل د. وارن ولويس د. براندیز في العام 1890 تعريفاً راسخاً للخصوصية باعتبارها "الحق في أن يُترَك الإنسان وشأنه".[2] غير أن مستخدمي الإنترنت اليوم يواجهون صعوبةً في الشعور بأنهم متروكون فعلاً وشأنهم. صحيح أن بعض التقنيات المتمحورة حول الخصوصية، مثل خدمات الدردشة المشفّرة من طرف إلى طرف، تَعِدُ بمستويات أعلى من سرية البيانات، إلا أن العديد من شركات التكنولوجيا الكبرى تجمع البيانات الشخصية للمستخدمين وتبيعها لمن يدفع الثمن الأعلى،[3] في حين تمارس الحكومات في مختلف أنحاء العالم مراقبة واسعة النطاق،[4] وتلجأ دول عدة إلى فرض الرقابة والتلاعب في المحتوى المنشور على شبكة الإنترنت.[5] ومن أبرز المخالفين في هذا المجال بائعو برامج التجسس التجارية، أي الشركات التي تقوم بتصميم أو تسويق أو بيع برامج تجسس لجهات مختلفة حول العالم بغرض تحقيق الربح. في هذا التقرير، تتناول منظمة "سمكس" بعضاً من أبرز البائعين الرئيسيين لبرامج التجسس في منطقة غرب آسيا وشمال أفريقيا.

برامج التجسّس هي شكل من أشكال البرمجيات الخبيثة التي تمكّن الجهات المهدّدة من التجسّس سراً على الضحايا. عند نجاح الاختراق، يمكن لمشغّل برنامج التجسّس مراقبة وسرقة جميع أنواع البيانات الخاصة بالشخص تقريباً من رسائله ومكالماته وسجلّ بحثه، وصولاً إلى استخدام الكاميرا والميكروفون دون علمه.[6] وبسبب هذا التجسّس غير المصرح به، تنتهك برامج التجسّس حقّ الضحايا الأساسي في الخصوصية.

تلجأ دول عديدة حول العالم إلى قمع شعوبها بهدف الحفاظ على سيطرتها.[7] ويشير باحثون مثل ستيفن فيلدستاين إلى أنّ الأنظمة الاستبدادية تعتمد على ما يصفه ليفيتسكي وواي (2010) بأساليب الإكراه المنخفضة الشدّة، مثل فرض مراقبة

---

[1] الجمعية العامة للأمم المتحدة (1948). الإعلان العالمي لحقوق الإنسان، المادتان 12 و19. باريس.

[2] وارن ص.د.، براندیز، ل.د. (1890). الحق في الخصوصية (The Right to Privacy). Harvard Law Review، 4(5)، ص. 193-220. doi:https://doi.org/10.2307/1321160.

[3] سيباستيان برومرسما (2023). *بياناتك الشخصية تُباع لمن يدفع الثمن الأعلى – وقد يكون المشتري جاسوساً* (*Your Most Intimate Data Is Being Sold to the Highest Bidder – Who Might Be a Spy*). [متاح على الإنترنت] Follow the Money – منصة للصحافة الاستقصائية. متوفر على: https://www.ftm.eu/articles/your-intimate-data-is-being-sold. [تم الاطلاع عليه في: 11 آب/أغسطس 2025]

[4] فيلدستاين، س. (2019). *الانتشار العالمي للمراقبة باستخدام الذكاء الاصطناعي* (*The Global Expansion of AI Surveillance*). [متاح على الإنترنت] مؤسسة كارنيغي للسلام الدولي. متوفر على: https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en [تم الاطلاع عليه في: 11 آب/أغسطس 2025]

[5] أ. فانك، ك. فستينسون، وغ. بايكر. (2024) *الحرية على الإنترنت 2024: الصراع من أجل الثقة عبر الإنترنت* (*Freedom on the Net 2024: The Struggle for Trust Online*) [متاح على الإنترنت] Freedom House. متوفر على: https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online [تم الاطلاع عليه في: 11 آب/أغسطس 2025]

[6] فورتينت (Fortinet) (2024). ما هي برامج التجسس؟ التعريف، والأنواع، والحماية (What Is Spyware? Definition, Types And Protection). [متاح على الإنترنت] فورتينت (Fortinet). متوفر على: https://www.fortinet.com/resources/cyberglossary/spyware [تم الاطلاع عليه في: 11 آب/أغسطس 2025]

[7] دافنبورت، ك. (2007). قمع الدولة والنظام السياسي (State Repression and Political Order). *Annual Review of Political Science*، *10(1)*، ص. *1-23*. doi:https://doi.org/10.1146/annurev.polisci.10.101405.143216

واسعة النطاق، وعرقلة أنشطة الخصوم السياسيّين، ومضايقة المعارضة.[8] وبينما يُنظر عادةً إلى القمع على أنه عنف جسدي، يمكن أن يتخذ أيضاً شكلاً رقمياً.[9] تساهم أدوات القمع الرقمي، مثل تقنيات المراقبة، في مساعدة الدول على تتبّع المعارضين والسيطرة عليهم، وتنفيذ الإكراه المنخفض الشدّة، وفي النهاية ممارسة أشكال أكثر تطرفاً من العنف القمعي. تُعدّ برامج التجسّس، بحكم تعريفها، شكلاً من أشكال المراقبة، وهي تساعد الدول على تسريع وتيرة القمع. وعادةً ما تبيع شركات برامج التجسّس التجارية منتجاتها للعملاء الحكوميّين فقط، وتدّعي أنّها تحصر مبيعاتها بالحكومات التي تستخدم منتجاتها لأغراض "مشروعة". وقد تم توثيق حالات أظهرت أنّ بعض مستخدمي هذه البرامج يسيئون استخدامها لانتهاك حقوق الإنسان، من خلال رصد سلوكيات المواطنين غير المرغوب فيها وقمعها، وبذلك تنتهك برامج التجسّس أيضاً حق الضحايا في حرية التعبير.[10] [11] [12]

على الرغم من السمعة السيئة التي اكتسبتها برامج التجسّس مثل "بيغاسوس" (Pegasus) التابع لمجموعة "إن إس أو" (NSO) خلال العقد الماضي، ما زالت الحكومات حول العالم تُضبط وهي تستخدم – أو يُشتبه في أنها تستخدم – برامج التجسّس. وتشير مؤسسة كارنيغي للسلام الدولي إلى أنّ أكثر من ثلث دول العالم اشترت برامج تجسّس أو تقنيات مشابهة بين العامَيْن 2011 و2023 [13]. كما تبيّن أنّ جميع الدول تقريباً في منطقة غرب آسيا وشمال أفريقيا تستخدم على الأرجح برامج التجسّس، وهذا هو محور بحثنا الراهن.[14] وعلى الرغم من جهود منظمات الرصد الرقمي مثل "أكسس ناو" (Access Now)، ومنظمة العفو الدولية، و"سيتيزن لاب" (Citizen Lab)، و"سمكس" (SMEX)، لا توجد أي مؤشرات على أنّ الحكومات تقلّل من استخدامها لبرامج التجسّس.

---

[8] ليفيتسكي، س.، ل. أ. واي (2010). *الاستبداد التنافسي: الأنظمة الهجينة بعد الحرب الباردة* (*Competitive Authoritarianism: Hybrid Regimes After the Cold War*). دار نشر جامعة كامبريدج.

[9] فيلدستاين، س. (2021). *صعود القمع الرقمي: كيف تُعيد التكنولوجيا تشكيل السلطة والسياسة والمقاومة* (*The Rise Of Digital Repression: How Technology Is Reshaping Power, Politics, And Resistance*) . نيويورك، دار نشر جامعة أكسفورد.

[10] دونيا مياتوفيتش (2023). برامج التجسّس الشديدة التطفل تهدد جوهر حقوق الإنسان (*Highly Intrusive Spyware Threatens the Essence of Human Rights*) مجلس أوروبا، تعليقات حول حقوق الإنسان.
https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights

[11] سانتياغو غوميز، إ.، رودريغز رودريغز، ك. 2018. تقنيات المراقبة: مراجعة للعنف المشروع الذي تمارسه الدولة في سياقات الأمن والسيطرة (Surveillance Technologies: A review of legitimate State violence in security and control contexts))، 16 ENCRUCIJADAS REVISTA CRITICA DE CIENCIAS SOCIALES. متوفر على:
https://gateway.webofknowledge.com/gateway/Gateway.cgi?GWVersion=2&SrcApp=Summon&SrcAuth=ProQuest&DestApp=WOS&DestLinkType=FullRecord&UT=000455807000011 [تم الاطلاع عليه في: 11 آب/أغسطس 2025]

[12] بابايميتريو، ج. (2023). التصدي للاستبداد الرقمي: تنظيم انتهاكات حقوق الإنسان في صناعة برمجيات المراقبة الخاصة (Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry). *مجلة حقوق الإنسان في جامعة هارفارد. (ربيع 2023).*

[13] فيلدستاين، س.، وكوت، ب. (2023). *لماذا تستمر صناعة برامج التجسّس العالمية في الازدهار؟ الاتجاهات، والتفسيرات، وردود الفعل* (*Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*) [متاح على الإنترنت] مؤسسة كارنيغي للسلام الدولي. متوفر على:
https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en [تم الاطلاع عليه في: 13 حزيران/يونيو2025]

[14] ماركزاك، ب.، سكوت-رايلتون، ج.، ماككون، س.، عبد الرزاق، ب.، ديبرت، ر. (2018). *لعبة الغمّيضة* (*HIDE AND SEEK*)

يتمثل أحد أكبر التحديات في دراسة برامج التجسّس ومستخدميها في أنّ بائعي برامج التجسّس التجارية يتعمّدون إخفاء أنشطتهم وعملائهم، كما يعمدون إلى تضليل المعلومات المتعلّقة بهويّتهم المؤسّسية. فعلى سبيل المثال، يكشف التحقيق الذي أجرته "سمكس"، والذي يُستعرض في هذا التقرير، أنّ مجموعة "إن إس أو" تُدار من خلال ما لا يقل عن خمس طبقات من الشركات القابضة، ويقع مقرّ أعلى شركة منها في لوكسمبورغ. ونتيجة لذلك، لا تتوفر معلومات كافية حول طبيعة عمل بائعي برامج التجسّس التجارية وأماكن نشاطهم، ولا سيما في منطقة غرب آسيا وشمال أفريقيا. وفي النهاية، يهدف هذا البحث إلى سدّ هذه الفجوة من خلال تحديد بائعي برامج التجسّس التجارية الأكثر نشاطاً في هذه المنطقة.

يمكن تقدير أماكن نشاط بائعي برامج التجسّس التجارية من خلال متابعة برامج التجسّس المستخدمة فعلياً والتي يمكن ربطها بالحكومات في المنطقة. واستناداً إلى منهجية الباحثَين ستيفن فيلدستاين وبراين كوت (2023)، يعتمد هذا التقرير على المعلومات المتاحة للعامة، والمصادر الإخبارية، والمستندات القضائية، وتسريبات البيانات، والسجلات المؤسّسية لتوثيق نشاط برامج التجسّس في المنطقة. وتشير النتائج إلى أنّ مجموعة **"إن إس أو"**، **ومجموعة Cytrox/Intellexa**، **وCellebrite**، **وSaito Tech/Candiru** هي الأكثر نشاطاً في المنطقة. علاوة على ذلك، يبدو أنّ بائعي برامج التجسّس الذين تقع مقرّاتهم في إسرائيل يهيمنون على السوق في منطقة غرب آسيا وشمال أفريقيا، مع أنّ شركات أخرى مثل Hacking Team (التي أصبحت تُعرف اليوم باسم Memento Labs)، ومقرّها إيطاليا، كانت هي المفضّلة سابقاً لدى حكومات المنطقة. في هذا التقرير، تعرض "سمكس" الهيكل المؤسسي لكل من هذه الشركات الأربع التي لوحظت في المنطقة، واستراتيجيات التسويق الخاصة بها، ومنتجاتها الرئيسية، والهجمات الإلكترونية المرتبطة بها. ومن خلال ذلك، يسعى هذا البحث إلى تعزيز فهم القارئ بحوادث برامج التجسّس في المنطقة، وطريقة عملها، وتأثيراتها الإنسانية، استناداً إلى مقابلات أجرتها "سمكس".

تواصل "سمكس" مناشدة جميع الدول للتوقف فوراً عن استخدام برامج التجسّس، ودعوة جميع بائعي برامج التجسّس التجارية إلى التوقف فوراً عن بيع تقنيات المراقبة. كما ينبغي على المجتمع المدني والمدافعين عن حقوق الإنسان اتخاذ إجراءات فعّالة لحماية أنفسهم على الإنترنت، بما في ذلك استخدام وسائل اتصال مشفّرة من طرف إلى طرف، وإنشاء كلمات مرور فريدة ومعقّدة، واستخدام الشبكات الخاصة الافتراضية (VPNs)، والاستعانة ببرامج إدارة كلمات المرور.

جدول المحتويات

الجزء الأول:
الخلفية

1.1 المقدمة: ما هي برامج التجسّس؟

"لو كان للخصوصية شاهدُ قبر، لربما كُتب عليه: 'لا تقلق، فقد كان هذا من أجل مصلحتك.'" – جون تويلف هوكس [النهر المظلم (*The Dark River*) (العالم الرابع، الجزء الثاني)]

طنين. يَظهر إشعار من تطبيق "واتساب" على هاتفك –رقم لا تعرفه أضافَك إلى مجموعة وأرسَلَ إليك ملفاً بصيغة PDF. بدافع الفضول، تقرّر فتح الرسالة والاطلاع على الملف.

تساورك الشكوك عندما تكتشف أنّك لا تعرف أحداً من أعضاء المجموعة. لا بأس – فأنت تدرك جيداً أنّه لا ينبغي فتح الروابط أو المستندات العشوائية التي تُرسَل من أرقام مجهولة، فتقرّر عدم فتح الملف. غير أنّ ثغرة أمنية في آلية معالجة الملفات في تطبيق "واتساب" تؤدّي إلى قيامه تلقائياً بتحليل الملف، مطلقاً سلسلة من الأحداث التي تمكّن برمجية خبيثة مخفيّة من أن تخترق "واتساب" وتنتشر إلى تطبيقات أخرى على جهازك.[15] وخلال ثوانٍ معدودة، قد يتمكّن المهاجم من الوصول إلى ملفات هاتفك، ورسائلك، وسجل مكالماتك، والمعلومات المتعلقة بموقعك. وعلى الأرجح لن تلاحظ الأمر، لكن خصوصيتك تكون قد تعرّضت لاختراق كامل.

في حين تبدو الفكرة مخيفة، إلّا أنّها ليست من نسج الخيال، فهذا أسلوب موثّق استخدمته شركة "باراغون سوليوشنز" (Paragon Solutions Ltd) الإسرائيلية لبرامج التجسس لنشر برنامجها الخبيث "Graphite" في أواخر العام 2024 (علماً أنه تمت معالجة سلسلة الاستغلال هذه منذ ذلك الحين).[16] ويشكّل برنامج "Graphite" انعكاساً لنمط أوسع، وهو من أخطر التهديدات لحقوق الإنسان الرقمية اليوم: قيام بائعي برامج التجسّس التجارية ببيع برامجهم إلى حكومات حول العالم.

برامج التجسّس (Spyware) مصطلح مُركّب في اللغة الإنكليزية من كلمتَيspy (تجسّس) وsoftware (برمجيات)، ويُطلَق على فئة من البرمجيات الخبيثة التي تتيح للمهاجمين مراقبة الضحايا والتجسّس عليهم من دون علمهم. وبحسب توصيف الباحث أجاي تشاولا، تُعَدّ هذه البرمجيات "قاتلة للخصوصية".[17] أمّا بائعو برامج التجسّس التجارية فهم شركات متخصّصة في بيع البرمجيات الخبيثة التي تُستخدم لمراقبة فئة سكانية مستهدفة. وتمثّل هذه الشركات قطاعاً متنامياً؛ فمع أنّ التقديرات الدقيقة لحجم هذا القطاع وقيمته تختلف، تشير بيانات صادرة عن مؤسّسة كارنيغي للسلام الدولي إلى أنّ أكثر من ثلث دول العالم اشترت برامج تجسّس أو تقنيات مشابهة من بائعين تجاريين خلال الفترة الممتدة بين العامَيْن 2011 و2023.[18] وخلال هذه الفترة، تبيّن أنّ معظم دول منطقة غرب آسيا وشمال أفريقيا – وهي إحدى البؤر الرئيسية لانتشار برامج التجسّس – إمّا استخدمت هذه البرامج أو كانت ضحية لهجماتها (باستثناء موريتانيا والصومال والصحراء الغربية).[19] كما أنّ العديد من الوكالات الحكومية حول العالم تبرم عقوداً مع بائعي برامج التجسّس التجارية. ومن الأمثلة البارزة والحديثة

---

[15] ماركزاك، ب. (2025). *فضيلة أم رذيلة؟ نظرة أولى على توسّع عمليات برامج التجسّس لشركة Paragon* (*Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations*) - *The Citizen Lab*. [متاح على الإنترنت]. The Citizen Lab. متوفر على: https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/

[16] The Hacker News (2025). "ميتا" تؤكّد تعرّض 90 صحافياً وناشطاً لهجوم تجسّسي عبر واتساب بدون أيّ نقرة (*Meta Confirms Zero-Click WhatsApp Spyware Attack Targeting 90 Journalists, Activists*). [متاح على الإنترنت]. The Hacker News. متوفر على: https://thehackernews.com/2025/02/meta-confirms-zero-click-whatsapp.html

[17] تشاولا، أ. (2021). برنامج التجسّس بيغاسوس – "مدمّر للخصوصية" ('Pegasus Spyware – 'A Privacy Killer). مجلة SSRN الإلكترونية. doi:https://doi.org/10.2139/ssrn.3890657

[18] فيلدستاين، س.، وكوت، ب. (2023). *لماذا تستمر صناعة برامج التجسّس العالمية في الازدهار؟ الاتجاهات، والتفسيرات، وردود الفعل* (*Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*)

[19] ماركزاك، ب.، سكوت-رايلتون، ج.، ماككون، س.، عبد الرزاق، ب.، ديبرت، ر. (2018). *لعبة الغمّيضة* (*HIDE AND SEEK*): تتبع عمليات برنامج بيغاسوس من شركة NSO في 45 دولة. [متاح على الإنترنت]. The Citizen Lab. متوفر على: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries

على ذلك، أنّ وكالة إنفاذ قوانين الهجرة والجمارك الأميركية جدّدت عقدها مع شركة "باراغون" في أيلول/سبتمبر 2025.[20]

يبيع بائعو برامج التجسّس التجارية منتجاتهم في الغالب إلى الحكومات، وبدرجة أقل بكثير إلى الشركات الخاصة، وذلك من خلال عقود تحدّد الفترة الزمنية وعدد برمجيات الاستغلال التي يطلبها العميل. وتُظهر وثيقة مسرّبة من شركة Intellexa في العام 2022 ذلك بوضوح؛ إذ تضمّن نموذج الطلب أنواعاً مختلفة من برمجيات الاستغلال لعدد محدّد من الاختراقات – في هذه الحالة، عشر حالات اختراق متزامنة على نظامَيْ iOS وAndroid مقابل ثمانية ملايين يورو، مع ضمان لمدّة 12 شهراً.[21]

على الرغم من أنّ جميع دول منطقة غرب آسيا وشمال أفريقيا تشارك في مؤتمرات واتفاقيات دولية متعدّدة لحقوق الإنسان، فإنها تنتهك الحقوق الرقمية بشكل متكرّر، وتراقب مواطنيها، وتفرض قيوداً على تداول المعلومات بين السكان.[22] وتُعَدّ دول الخليج من أبرز الجهات المشترية من بائعي برامج التجسّس التجارية، ومع ذلك فقد صادقت أكثر من نصف دول مجلس التعاون الخليجي على المعاهدات العشر الأساسية لحقوق الإنسان الصادرة عن الأمم المتحدة. غير أنّ هذه الالتزامات تبقى، في أحسن الأحوال، موضع شك، وفي أسوأها مجرّد ادّعاءات زائفة.[23] يزعم عدد كبير من أبرز بائعي برامج التجسّس التجارية أنهم يلتزمون بمعايير حقوق الإنسان بحذافيرها، مؤكّدين أنهم لا يبيعون منتجاتهم للأنظمة الاستبدادية، ويعتمدون على خطاب مدروس بعناية للادعاء بأنّ نشاطهم يقتصر على مكافحة الجرائم الخطيرة فقط. فعلى سبيل المثال، تسوِّق مجموعة "إن إس أو" منتجاتها بوصفها "استخبارات سيبرانية من أجل تعزيز الأمن والاستقرار العالمي".[24] وبعد أن تعرّضت الشركة لانتقادات بسبب سجلّها في مجال حقوق الإنسان، أفادت صحيفة "نيويورك تايمز" عام 2019 بأنّ الشركة زعمت بيع منتجاتها فقط لحكومات تكافح الجريمة أو الإرهاب.[25] مع ذلك، كشف مختبر "سيتيزن لاب" في العام 2018 أنّ بعض الحكومات الاستبدادية، مثل السعودية ومصر، استخدمت على الأرجح منتجات مجموعة "إن إس أو".[26] ووفقاً لـ"سيتيزن لاب"، فقد تمّ رصد برنامج التجسّس الشهير "بيغاسوس" التابع لمجموعة "إن إس أو" في معظم دول منطقة غرب آسيا وشمال أفريقيا، كما من المحتمل أن يكون برنامج التجسّس التابع لشركة "كوادريم" (QuaDream) قد استُخدم أيضاً في عدد من دول المنطقة.[27] [28] علاوة على ذلك، ووفقاً لمؤسسة كارنيغي للسلام الدولي، فإن 44 من أصل 74 حكومة

---

[20] فرانشيسكي-بيتشيري، ل.. (2025 أ). *وكالة إنفاذ قوانين الهجرة والجمارك الأميركية تجدّد عقدها مع شركة باراغون لتطوير برامج التجسّس* (*ICE Reactivates Contract with Spyware Maker Paragon*) | *TechCrunch*. [متاح على الإنترنت] TechCrunch . متوفر على: https://techcrunch.com/2025/09/02/ice-reactivates-contract-with-spyware-maker-paragon/ [تم الاطلاع عليه في: 3 أيلول/سبتمبر2025]

[21] مجموعة تحليل التهديدات في غوغل (2024). *شراء برامج التجسّس: رؤى حول بائعي برامج المراقبة التجارية*(*Buying Spying: Insights into Commercial Surveillance Vendors*). [متاح على الإنترنت] ص.17.

[22] شايرز، ج. (2021). سياسة الأمن السيبراني في الشرق الأوسط (*The Politics of Cybersecurity in the Middle East*).

[23] هوراك، غ. (2023). الكشف عن البيانات الشخصية: برامج التجسّس وحقوق الإنسان في منطقة الشرق الأوسط وشمال أفريقيا (*Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa*). أطروحة ماجستير، قسم التعليم المستمر، جامعة هارفارد.

[24] مجموعة "إن إس أو" (2019). مجموعة *"إن إس أو" - استخبارات سيبرانية من أجل تعزيز الأمن والاستقرار العالمي* (*Cyber intelligence for global security and stability*) [متاح على الإنترنت]. مجموعة "إن إس أو". متوفر على: https://www.nsogroup.com/ [تم الاطلاع عليه في: 21 آب/أغسطس 2025]

[25] غويل، ف.، بيرلروث، ن.. (2019) شركة برامج التجسّس NSO تَعِدُ بالإصلاح لكنها تواصل التجسّس (Spyware Maker NSO Promises Reform but Keeps Snooping). نيويورك تايمز [متاح على الإنترنت]. 9 تشرين الثاني/نوفمبر. متوفر على: https://www.nytimes.com/2019/11/09/technology/nso-group-spyware-india.html

[26] ماركزاك، ب.، سكوت-رايلتون، ج.، ماككون، س.، عبد الرزاق، ب.، ديبرت، ر. (2018). *لعبة الغمّيضة* (*HIDE AND SEEK*)

[27] ماركزاك، ب.، سكوت-رايلتون، ج.، ماككون، س.، عبد الرزاق، ب.، ديبرت، ر. (2018). *لعبة الغمّيضة* (*HIDE AND SEEK*)

[28] ماركزاك، ب.، سكوت-رايلتون، ج.، بيري، أ.، الجيزاوي، ن.، أنستيس، س.، بانداي، ز.، ليون، إ.، عبد الرزاق، ب.، ديبرت، ر. (2023) *Sweet QuaDreams*.

معروفة اشترت برامج تجسّس بين العامين 2011 و2023 كانت أنظمة استبدادية.[29] وبينما تزعم شركات تطوير برامج التجسّس أنّها تساهم في تعزيز الأمن العالمي، مؤكدةً أن تقنياتها تمنع وقوع أحداث ضارّة، فإنّ العديد من عملائها يستخدمون هذه التقنيات لمراقبة المعارضين والأقليات والخصوم السياسيّين.

هناك فجوة كبيرة في المعرفة بشأن الجهات التي تشتري من شركات برامج التجسّس التجارية، والمنتجات التي تقدمها تلك الشركات، بالإضافة إلى كيفية هيكلة هذه الشركات، ولا تتوفّر أصلاً معلومات كافية حول شركات برامج التجسّس التجارية الكبرى العاملة في منطقة غرب آسيا وشمال أفريقيا. ويشير باحثون في المجلس الأطلسي إلى أنّ أحد أكبر تجمعات هذه الشركات في المنطقة يقع في إسرائيل، إلا أنّ المعلومات المتاحة حول الأماكن الفعلية لاستخدام هذه البرمجيات محدودة. كما أن الأبحاث المتعلقة ببرامج التجسّس الأكثر استخداماً في كل دولة من دول المنطقة قليلة جداً.

يهدف هذا البحث إلى البدء في سد هذه الفجوة، مع التركيز أيضاً على عمليات هذه الشركات واستراتيجياتها، ومصادر تمويلها، وتأثيرها على حقوق الإنسان في المنطقة.

لفهم وضع برامج التجسّس في منطقة غرب آسيا وشمال أفريقيا بصورة أفضل، يطرح هذا البحث الأسئلة الآتية:

1. ما هي أبرز شركات بيع برامج التجسّس التجارية العاملة في المنطقة، وما هي استراتيجياتها التشغيلية؟
2. من يموّل هذه الشركات، وما هي تداعيات هذه العلاقات بين الممول وشركات التجسس؟
3. كيف تؤثر عمليات برامج التجسّس على البُنى الجيوسياسية والاجتماعية في منطقة غرب آسيا وشمال أفريقيا؟

من خلال الإجابة على هذه الأسئلة، يهدف هذا التحليل إلى تلخيص المعلومات، واختصارها، وتقديم نتائج بحثية جديدة حول برامج التجسّس المستخدمة في المنطقة.

1.2 مراجعة الأدبيات

الخصوصية وحقوق الإنسان الرقمية

يشهد عالمنا تطوّراً متزايداً في مجال التكنولوجيا. فقد تجاوز عدد الأجهزة المحمولة المتصلة بالإنترنت في جميع أنحاء العالم 18 مليار جهاز، وبحلول شباط/فبراير 2025 سيصل عدد مستخدمي الإنترنت إلى أكثر من 5.56 مليارات شخص

[29] فيلدستاين، س.، وكوت، ب. (2023). *لماذا تستمر صناعة برامج التجسّس العالمية في الازدهار؟* (*Why Does the Global Spyware Industry Continue to Thrive?*)

حول العالم.[30] [31] ومع تزايد عدد المستخدمين واعتمادهم على المزيد من الأجهزة، تتّسع "رقعة الهجوم" الخاصة بهم، أي عدد التهديدات الرقمية المحتملة التي قد يتعرضون لها. ويتيح هذا الأمر للمهاجمين، سواء كانوا شركات تجارية أو جهات حكومية أو أفراداً مستقلين، فرصة الوصول إلى بيانات المستخدمين وانتهاك خصوصيتهم. لكن ما المقصود بالخصوصية، ولماذا ينبغي أن نهتم بها؟

تُشكّل الخصوصية، والحق في التمتّع بها، عنصراً أساسياً في فهم التهديد الذي تطرحه برامج التجسّس. غير أنّ مفهوم الخصوصية، بما في ذلك كيفية تعريف المجتمعات له وتحديد ما ينبغي اعتباره شأناً خاصاً، قد تبدّل عبر الزمن، وهو في جوهره مفهوم متغيّر. وقد كتبت الفيلسوفة جوديث جارفيس طومسون: "ربما أكثر ما يلفت الانتباه بشأن الحق في الخصوصية هو أنّ أحداً لا يمتلك فكرة دقيقة تماماً عمّا يعنيه".[32] وكان وارن وبراندیز من أوائل من تناولوا هذا الموضوع في مقالتهما الشهيرة "الحق في الخصوصية" في العام 1890، حيث قدّما تعريفاً راسخاً للخصوصية باعتبارها "الحق في أن يُترَك الإنسان وشأنه".[33]

يذكر دانيال سولوف، وهو أحد أبرز الباحثين في مجال الخصوصية، في كتابه *"فهم الخصوصية" (Understanding Privacy)* أنّ كثيرين يعرّفون الخصوصية باعتبارها حقاً يتجلّى في أشكال مختلفة مثل "حرية التفكير، والسيطرة على الجسد، والعزلة في المنزل، والتحكم في المعلومات الشخصية، والتحرّر من المراقبة، وحماية سمعة الفرد، والحماية من عمليات التفتيش والاستجواب".[34] ويضيف سهيل آفتاب (2024) إلى ذلك في *"مفهوم الحق في الخصوصية"* (The Concept of the Right to Privacy)، مشيراً إلى أنّه من الصعب جداً تحديد تعريف شامل لمفهوم الخصوصية نظراً لتنوّع التعريفات عبر التاريخ، مثل: الحق في العزلة، والحق في أن يُترك الإنسان وشأنه، والحق في إخفاء الأسرار، والحق في عدم السماح بالوصول، والحق في التحكم في البيانات الشخصية. ويؤكّد آفتاب أنّ كلّ تعريف للخصوصية كحق يستند، في جوهره، إلى مبدأَي الكرامة والاستقلالية.[35] كما يشير الباحث وودرو هارتزوغ إلى أنّ سولوف يرى أنّ الأهم هو التركيز على "الغاية من الخصوصية" بدلاً من محاولة تعريفها بدقة.[36]

تُعدّ الأمم المتحدة من أولى المؤسّسات الدولية التي كرّست حق الإنسان في الخصوصية، وذلك عبر إصدار الإعلان العالمي لحقوق الإنسان. تنص المادة 12 من الإعلان على أنه "لا يجوز تعريض أحد لتدخّل تعسّفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسّ شرفه وسمعته"، بينما تنص المادة 19 على "حقّ التمتّع بحرّية الرأي والتعبير... [ويشمل هذا الحقّ] حرّيته في اعتناق الآراء دون مضايقة".[37] ويكرّر العهد الدولي الخاص بالحقوق المدنية

---

[30] لاريتشيا، ف. (2023). عدد الأجهزة المحمولة حول العالم 2019-2023. (Number of mobile devices worldwide 2019-2023). [متاح على الإنترنت]. Statista. متوفر على: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/

[31] بيتروسيان، آ. (2025). السكان الرقميون حول العالم 2025 (Worldwide Digital Population 2025). [متاح على الإنترنت]. Statista. متوفر على: https://www.statista.com/statistics/617136/digital-population-worldwide/

[32] طومسون، ج. ج.، 1975. الحق في الخصوصية (The right to privacy). *Philosophy & Public Affairs*، *ص. 295-314*.

[33] وارن، ص.د.، براندیز، ل.د. (1890). الحق في الخصوصية (The Right to Privacy). Harvard Law Review، 4(5)، ص. 193-220. doi:https://doi.org/10.2307/1321160

[34] دانيال ج. سولوف (2008). فهم الخصوصية (*Understanding Privacy*).

[35] آفتاب، س. (2024). مفهوم الحق في الخصوصية (The Concept of the Right to Privacy). في كتاب: وجهات نظر مقارنة حول الحق في الخصوصية (Comparative Perspectives on the Right to Privacy). سلسلة: Ius Gentium: Comparative Perspectives on Law and Justice، المجلد 109. Springer، Cham. https://doi.org/10.1007/978-3-031-45575-9_3

[36] سولوف، د. ج.، ودار نشر جامعة ييل (2011). *لا شيء لتخفيه: المفاضلة الزائفة بين الخصوصية والأمن (Nothing to Hide: the False Tradeoff between Privacy and Security)*. *نيو هافن؛ لندن:* دار نشر جامعة ييل؛ و. هارتزوغ (2021) ما هي الخصوصية؟ هذا سؤال خاطئ (*What is Privacy? That's the Wrong Question*) في The University of Chicago Law Review 1677 88. متوفر على https://scholarship.law.bu.edu/faculty_scholarship/3063

[37] الجمعية العامة للأمم المتحدة (1948). *الإعلان العالمي لحقوق الإنسان*.

والسياسية هذه المبادئ في المادتين 17 و19، مؤكّداً على أنّ الخصوصية وحرية التعبير هما من حقوق الإنسان المحمية.[38] وقد جرى تكريس مبادئ مشابهة في الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية، والاتفاقية الأميركية لحقوق الإنسان، والميثاق العربي لحقوق الإنسان. وفي العام 2015، شدّد المقرّر الخاص للأمم المتحدة المعني بالحق في الخصوصية على أهمّية هذا الحق في تقريره المعنون "الحق في الخصوصية في العصر الرقمي"، موضحاً أنّ الخصوصية "مهمّة من أجل إعمال الحق في حرية التعبير وحرية اعتناق الآراء دون مضايقة".[39] ومن هذا المنظور، يعرّف المقرّر الخاص الخصوصية باعتبارها مرتبطة ارتباطاً وثيقاً بسائر حقوق الإنسان.

لطالما وُجدت أُطر مختلفة للحقوق الرقمية، إلا أنّه في العام 2015 أنشأ مجلس حقوق الإنسان التابع للأمم المتحدة أوّل ولاية رسمية تُعنى بالخصوصية. ويقوم المقرّر الخاص المعني بالخصوصية بإعداد تقارير دورية حول القضايا والأُطر المتعلقة بحماية الخصوصية الرقمية على مستوى العالم.[40] واتّخذ التحالف العالمي للحقوق الرقمية، برعاية الأمم المتحدة، خطوة إضافية في العام 2022 في مجال تعريف حقوق الخصوصية، من خلال الدعوة إلى وضع إطار عالمي للحقوق الرقمية يكرّس مبادئ أكثر صلابة في مجال حقوق الإنسان الرقمية، مثل: الحقوق الرقمية الشاملة والمتساوية، والسلامة الشخصية وخصوصية البيانات، وتقرير المصير الرقمي، والوصول الرقمي الشامل.[41] وظهر اقتراح جديد يهدف إلى دمج أُطُر حقوق الإنسان الدولية مع التقنيات الرقمية، وتمثّل ذلك في إطار حوكمة الحقوق الرقمية الذي يقترح إنشاء نظام حوكمة تقوده المدن، يعتمد على قواعد وهياكل وأدوات محلية لحماية الحقوق الرقمية. وقد صدرت المسوّدة الأولية لهذا الإطار في كانون الأوّل/ديسمبر 2021.[42] وتحظى كل هذه الاتفاقيات والأُطر بدعم منظمات دولية غير حكومية تعمل في مجال الدفاع عن حقوق الإنسان الرقمية، مثل "أكسِس ناو"، ومؤسّسة "الحدود الإلكترونية" (Electronic Frontier Foundation)، و"سمكس"، والتي تتصدّى قانونياً للانتهاكات في مختلف أنحاء العالم وتقدّم المساعدة في حالات الطوارئ الرقمية.

يُعرِّف مكتب الأمم المتحدة المعني بالمخدّرات والجريمة الخصوصية في سياق الجرائم السيبرانية على أنّها "مرتبطة بالتحرّر من التعرّف على الهوية". وترى الأمم المتحدة أنّ الخصوصية توفّر لمستخدمي التكنولوجيا "مساحة آمنة خالية من الترهيب أو الانتقام أو غيرهما من أشكال الإكراه أو العقوبة، تمكّنهم من التعبير عن أفكارهم وآرائهم ووجهات نظرهم ومعتقداتهم بحرية، ومن دون أن يُجبَروا على الكشف عن هويتهم".[43] وهذا المفهوم، أي التحرّر من الإلزام بالكشف عن الهوية والمعلومات الشخصية المحدِّدة للهوية، هو ما تنتهكه برامج التجسّس بشكل مباشر.

تقيّد برامج التجسّس، بطبيعتها، الخصوصية على نحوٍ كبير وتحدّ من حرية التعبير. فالبرمجيات التي تخترق أجهزة المستخدمين، وترسّخ وجودها خفية، وتراقب أنشطتهم، تنتهك جميع الأُطُر التي تحمي حقوق الإنسان في الخصوصية

---

[38] الجمعية العامة للأمم المتحدة (1948). *العهد الدولي الخاص بالحقوق المدنية والسياسية*، المادتان 17 و19. باريس.

[39] المقرّر الخاص للأمم المتحدة المعني بالحق في الخصوصية (2015). *A/HRC/28/`6*: تقرير المقرّر الخاص حول الحق في الخصوصية في العصر الرقمي. *مجلس حقوق الإنسان التابع للأمم المتحدة*.

[40] المقرّر الخاص للأمم المتحدة المعني بالحق في الخصوصية (2015). *تاريخ الولاية*. [متاح على الإنترنت]. مكتب مفوضية الأمم المتحدة السامية لحقوق الإنسان OHCHR. متوفر على: https://www.ohchr.org/en/special-procedures/sr-privacy/mandate

[41] التحالف العالمي للحقوق الرقمية (2023) *حماية حقوق الإنسان في عالمنا الرقمي* (*Securing Our Human Rights in Our Digital World*). [متاح على الإنترنت]. متوفر على:
https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/230203_Alliance_for_Universal_Digital_Rights.pdf

[42] لاهتينويا، ف.، دومينغيز، ه.، فاكينا، د، وستربيرغ، ب.، نكويدجي، ل.، غودوين، ه.، شيل ساغار، ع.، بيرشال، ك.، بلوك، ج.، فان إيميرين، إ.، راميريز شيكو، غ.، بيريز باتل، م.، بويت سيرانو، ب.، بيرينو، م.، بورتيي، ف.، مانسو، ج. (من دون تاريخ). *إطار حوكمة الحقوق الرقمية* (*Digital Rights Governance Framework*) [متاح على الإنترنت] برنامج الامم المتحدة للمستوطنات البشرية - من أجل مستقبل حضري أفضل. متوفر على:
https://citiesfordigitalrights.org/sites/default/files/DIGITAL%20RIGHTS%20FRAMEWORK_CONCEPT%20FOR%20FEEDBACK.pdf

[43] مكتب الأمم المتحدة المعني بالمخدّرات والجريمة (2016). الخصوصية والأمن (*Privacy and Security*). [متاح على الإنترنت]. متوفر على:
https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-10/key-issues/privacy-and-security.html [تم الاطلاع عليه في: 14 حزيران/يونيو 2025]

وحرية التعبير. ومع أنّ العديد من الحكومات، بما في ذلك في الاتحاد الأوروبي، تلتزم بالأُطُر الدولية لحقوق الإنسان وتفرض قيوداً على تصدير السلع التي تنتهك هذه الحقوق، فإنّها في الوقت نفسه تستخدم برامج التجسّس على نطاق واسع. بالإضافة إلى ذلك، غالباً ما توظّف الدول هذه البرامج لمراقبة فئات محدّدة من المواطنين ومعاقبتها، مثل الخصوم السياسيّين وأفراد مجتمع المثليّين والمتحوّلين جنسياً.[44] ويظهر عدد كبير من هذه الدول تضارباً واضحاً في المصالح بين ادّعاء "مكافحة الجريمة" (الأشخاص محلّ الاهتمام) وبين الزعم بدعم حقوق الإنسان. وبناءً على ذلك، فإنّ التصدّي لهذا التوجّه بات أمراً بالغ الأهمية، ولا سيّما في ظل سعي العديد من المجتمعات إلى ابتكار أساليب جديدة لمكافحة الجريمة.

أساليب القمع

تلجأ الحكومات، سواء كانت استبدادية أو أنوقراطية أو ديمقراطية، إلى درجات مختلفة من القمع للسيطرة على شعوبها.[45] وهذا أمر واضح تماماً وموثَّق على نطاق واسع في الدراسات الأكاديمية: عندما تتراجع سيطرة الدولة على السلطة أو تشعر بوجود تهديد لسلطتها، فإنها تمارس القمع.[46]

يُنظر إلى القمع عادةً على أنّه عنف جسدي، كالخطف والتعذيب والقتل خارج نطاق القضاء، غير أنّه قد يتخذ أشكالاً متعدّدة أخرى. وبوجه عام، يمكن فهمه بوصفه تهديداً أو إجراءات فعلية تُتّخذ لفرض أعباء على الفرد، بهدف منع تبلور أيديولوجيات أو ممارسات غير مرغوب فيها سياسياً (غولدستاين، 1978).[47]

يرى بعض الأكاديميّين أن القمع يُمارَس بوتيرة أعلى في الأنظمة الاستبدادية مقارنةً بالأنظمة الديمقراطية، نظراً لما يترتّب على ممارسته في الأنظمة الديمقراطية من عواقب سياسية جسيمة. ووفقاً لهذه النظرية، تجعل المؤسّسات الديمقراطية اللجوء إلى القمع أكثر صعوبة، إذ يستطيع الأفراد الذين يتعرّضون له التصويت لإقصاء من يمارسونه من السلطة.[48] وكما يوضح دافنبورت (2007)، تتيح هذه المؤسسات للأفراد إمكانية تحدّي مَن هم في مواقع السلطة. وتُعدّ أساليب الحكم القمعية، في جوهرها، شكلاً من أشكال السيطرة، ويبدو أنها استُخدمت تاريخياً بشكل أكبر من قِبل الأنظمة الاستبدادية مقارنةً بالأنظمة الديمقراطية.[49] وفي العام 2025، تكاد جميع دول منطقة غرب آسيا وشمال أفريقيا تكون استبدادية.[50]

في كتابه "صعود القمع الرقمي" (*The Rise of Digital Repression*) (2021)، يشير ستيفن فيلدستاين إلى أنّ الأنظمة الاستبدادية تعتمد على ما يصفه ليفيتسكي وواي (2010) بأساليب الإكراه المنخفضة الشدّة، مثل مضايقة المعارضة،

---

[44] هاجر شيزاف وجاكوبسون، ج. (2018). كشف النقاب: صناعة التجسّس السيبراني في إسرائيل تساعد دكتاتوريي العالم على ملاحقة المعارضين والمثليين – أخبار إسرائيل (*Revealed: Israel's cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays - Israel News*) [متاح على الإنترنت]. Haaretz.com. متوفر على:
https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000 [تم الاطلاع عليه في: 13 آب/أغسطس 2025]

[45] دافنبورت، ك. (2007). قمع الدولة والنظام السياسي (State Repression and Political Order).

[46] دافنبورت، ك. (2007). قمع الدولة والنظام السياسي (State Repression and Political Order).

[47] غولدشتاين، ر. ج.. 1978. *القمع السياسي في أميركا الحديثة: من عام 1870 إلى الوقت الحاضر* (*Political Repression in Modern America: from 1870 to the Present*). كامبريدج، ماساتشوستس: Schenkman.

[48] دافنبورت، ك. (2007). قمع الدولة والنظام السياسي (State Repression and Political Order).

[49] مولر، ج.، سكانينغ، س. إ. (2013). الأنظمة الاستبدادية والديمقراطية وانتهاك الحريات المدنية (Autocracies, democracies, and the violation of civil liberties). *Democratization، 20(1)*، ص. *82-106*. doi:https://doi.org/10.1080/13510347.2013.738863

[50] كوبيدج. م.، غيرينغ، ج.، كنوستن، ك. ه.، ليندبيرغ، س. إ.، تيوريل، ج.، ألتمان، د.، أنجيوليلو، ف.، بيرنهارد، م.، كورنيل، أ.، فيش، م. س.، فوكس، ل.، غاستالدي، ل.، جيرلو، ه.، غلين، آ.، غود غاد، آ.، غراهن، س.، هيكن، أ.، كينزلباخ، ك.، كرسل، ج.، ماركوارت، ك. ل.، ماكمان، ك.، ميشكوفا، ف.، ميدزيهورسكي، ج.، ناتسيكا، ن.، نوندورف، ن.، باكستون، ب.، بيمشتاين، د.، فون رومر، ج.، سيم، ب.، سيغمان، ر.، سكانينغ، س. إ.، ستاتون، ج.، ساندستروم، أ.، تانينبيرغ، م.، تزيلغوف، إ.، وانغ، ي.ت، ويريشت، ف.، ويغ، ت.، ويلسن، س.، زيبلات، د. (2025) قاعدة بيانات V-Dem [البلد – السنة/البلد - التاريخ] الإصدار 15. مشروع Varieties of Democracy (V-Dem)، doi: 10.23696/vdemds25.

وفرض مراقبة واسعة النطاق، واحتجاز المعارضين، وإعاقة كل من يقف في طريق أصحاب السلطة.[51] [52]
وفي الوقت الحاضر، بات القمع يأخذ شكلاً رقمياً في كثير من الأحيان، حيث تساعد أدوات القمع الرقمي الدول على تنفيذ هذه الأساليب المنخفضة الشدّة.

يُصوّر فيلدستاين القمع الرقمي على أنّه سلسلة من المناورات الرقمية التي تُساهم في تنفيذ أشكال القمع الجسدي التقليدية. ويقسّم القمع الرقمي إلى خمس فئات: الرقابة على الإنترنت، والتلاعب الاجتماعي ونشر المعلومات المضلِّلة، وحجب الإنترنت، والاضطهاد الموجَّه ضدّ مستخدمي الإنترنت، والمراقبة. وتُعد برامج التجسّس إحدى أدوات المراقبة.

دور برامج التجسّس

تُستخدم برامج التجسّس بشكل خاص لأغراض المراقبة الموجَّهة، أو المراقبة التي تنطوي على اختراق رقمي لانتهاك السرية والوصول إلى معلومات المستخدِم (فيلدستاين 2021). وتعمل برامج التجسّس كأداة للإكراه المنخفض الشدّة، إذ تراقب سراً وتجمع المعلومات عن أفراد أو منظمات يُعتقد أنهم يرتكبون أفعالاً تشكّل تهديداً للدولة. وتعتمد شركات برامج التجسّس في استراتيجياتها التسويقية على تقديم منتجاتها الرقابية باعتبارها منتجات أمنية "مشروعة". لكن، كما يتساءل كثير من المراقبين: مشروعة بالنسبة لِمَن؟ الجواب يعتمد على الحكومة.

وفقاً لغوميز ورودريغز (2018)، وفيلدستاين وكوت (2023)، وبابايميتريو (2023)، تبرّر الحكومات استخدام أدوات المراقبة الجماعية وبرامج التجسّس بما تعتبره حالات استخدام مشروعة، وغالباً ما تشمل مكافحة الجريمة، أو الإرهاب، أو إدارة الأزمات.[53] [54] ويؤكّد ذلك طبيعة برامج التجسّس كمنتج مزدوج الاستخدام، إذ يمكن توظيفه لأغراض عسكرية ومدنية على حدّ سواء.[55] وفي هذا السياق، يتم تنظيم تصدير المنتجات ذات الاستخدام المزدوج بموجب اتفاق واسينار، وهو اتفاق تم التوصل إليه في العام 1996 بين 42 دولة للتحكّم بالمنتجات التي يمكن استخدامها لانتهاك حقوق الإنسان (إلى جانب استخداماتها الأمنية "المشروعة"). وقد تم تعديله في العام 2013 ليشمل بعض أشكال برامج المراقبة وتقنيات فحص الحزم العميق. والجدير بالذكر أنّه في حين وقّعت الولايات المتحدة والمملكة المتحدة على الاتفاق (باعتبارهما من كبار مصدّري تكنولوجيا المراقبة)، لم توافق أي دولة في منطقة غرب آسيا وشمال أفريقيا على هذا الاتفاق.[56] كما أنّ إسرائيل، التي هي مقرّ جميع شركات بيع برامج التجسّس التجارية المذكورة في هذا التقرير، ليست من الدول الموقّعة عليه، رغم أنّها تدّعي أنّها تبنّت بعض بنود الاتفاق ضمن قانون مراقبة الصادرات الدفاعية الإسرائيلية رقم 5766-2007.[57]

مع ذلك، أشار المقرّر الخاص للأمم المتحدة المعني بالحق في الخصوصية إلى أن الدول غالباً ما تُمارس المراقبة من دون أي أساس قانوني، نظراً لغياب القوانين التي تحدّد أهداف المراقبة المشروعة في العديد من الدول. وفي تقريرٍ للأمم المتحدة

---

[51] ليفيتسكي، س. ، واي، ل. أ. (2010). *الاستبداد التنافسي: الأنظمة الهجينة بعد الحرب الباردة* (*Competitive Authoritarianism: Hybrid Regimes After the Cold War*).

[52] س. فيلدستاين (2021). *صعود القمع الرقمي: كيف تُعيد التكنولوجيا تشكيل السلطة والسياسة والمقاومة* (*The Rise Of Digital Repression: How Technology Is Reshaping Power, Politics, And Resistance*) .

[53] سانتياغو غوميز، إ.، رودريغز رودريغز، ك.، 2018. تقنيات المراقبة (Surveillance Technologies).

[54] بابايميتريو، ج. (2023). التصدي للاستبداد الرقمي (Disrupting Digital Authoritarians).

[55] الاتحاد الأوروبي (من دون تاريخ). *تصدير المواد ذات الاستخدام المزدوج* (*Exporting dual-use Items*) متوفر على:
https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en

[56] شايرز، ج. (2022). *سياسة الأمن السيبراني في الشرق الأوسط* (*The Politics of Cybersecurity in the Middle East*). دار نشر جامعة أكسفورد، ص.8.

[57] ديلباري، د. (2019). *الرقابة على الصادرات الإسرائيلية وصفقات الدمج والاستحواذ/الاستثمار* (*Israeli Export Controls and M&A/Investment Transactions*). [متاح على الإنترنت]. مكاتب المحاماة Goldfarb Seligman، ص. 7-7. متوفر على:
https://www.goldfarb.com/pdf1/%D7%9E%D7%A6%D7%92%D7%AA%20%D7%93%D7%A0%D7%99%20%D7%93%D7%99%D7%9C%D7%91%D7%A8%D7%99%20%D7%9C%D7%9B%D7%A0%D7%A1%2010.9.19.pdf
[تم الاطلاع عليه في: 10 آب/أغسطس 2025].

حول الحق في الخصوصية في العصر الرقمي، تُحدّد الأمم المتحدة تعريفاً واضحاً لما يُعتبر "مشروعاً" بموجب القانون الدولي: التدابير المُستخدمة فقط للتحقيق في "أخطر الجرائم أو التهديدات".[58] [59] في ذلك التقرير، تُطالب الأمم المتحدة الدول بالسعي إلى ضمان تحقيق الشروط التالية للمراقبة:

1. "أن ينصّ القانون عليها، وأن تفي بمعيارَيْ الوضوح والدقة الكافيَيْن لضمان إخطار الأفراد مسبقاً بها وإمكانية توقّعهم تطبيقها؛
2. أن تكون ضرورية على نحو محدّد وظاهر لتحقيق غرض شرعي؛
3. أن تتقيّد بمبدأ التناسب وألا تُستخدم عندما تكون التقنيات الأقل اقتحاماً متاحة أو لم تُستنفد بعد".[60]

ولكنّ المراقبة التي تُمارَس من قبل الدولة تُستَخدم لأغراض غير مشروعة، مثل التجسّس على المعارضين، والأقليات، والخصوم السياسيين، وغيرهم ممّن تصنّفهم السلطات كأهداف للمراقبة.[61] ووفقاً للمقرّر الخاص السابق للأمم المتحدة المعني بحرية الرأي والتعبير، تفاقم وضع المراقبة الحكومية إلى حدّ "أن الدول تُقدم على أعمال غير مشروعة في مجال المراقبة دون الخوف من التبعات القانونية".[62] وفي حين أنّ الحكومات التي تمتلك أجهزة متقدّمة للأمن السيبراني لديها تاريخ طويل في تطوير أسلحتها السيبرانية الخاصة (كما هي الحال في إسرائيل والولايات المتحدة مع "ستوكسنت"[63])، تشجّع دول أخرى بنشاط الجهات التجارية على تطوير برمجيات الاستغلال وبيعها.[64]

كما يوضح الباحث جورج باباديميتريو في مقالته "التصدي للاستبداد الرقمي"، هناك سببان يدفعان الجهات الحكومية إلى استخدام برامج التجسّس على الرغم من التهديد الواضح الذي تشكّله على حقوق الإنسان الرقمية. أوّلاً، يشكّل العدد الهائل من الأجهزة المستخدمة حول العالم فرصة استخباراتية لا يمكن للحكومات التغاضي عنها، إذ يُعدّ مصدراً لا حدود له تقريباً من المعلومات عن كل شخص قد يكون محل اهتمام.[65] ثانياً، تعتمد معظم المعايير التقنية الرئيسية اليوم على التشفير من طرف إلى طرف، كما أنّ عدداً كبيراً من شركات التكنولوجيا الكبرى تستخدم هذا النوع من التشفير في منتجاتها (مثل بروتوكول التشفير الخاص بـ"سيغنال" (Signal) الذي اعتمده "واتساب"، وiMessage من "آبل"، إلخ.). وهذا يضع الحكومات الساعية إلى مراقبة أهدافها أمام معضلة حقيقية، إذ إنّ خوارزميات التشفير الحديثة بالغة التعقيد ومن الصعب جداً اختراقها. فعلى سبيل المثال، قد يستغرق "فوغاكو" (Fugaku)، وهو أحد أقوى الحواسيب الخارقة في العالم، نحو 12

---

[58] المفوض السامي للأمم المتحدة لحقوق الإنسان (2018). *A/HRC/39/29*: الحق في الخصوصية في العصر الرقمي. *تقرير المفوض السامي للأمم المتحدة لحقوق الإنسان* (*The right to privacy in the digital age*). *مجلس حقوق الإنسان التابع للأمم المتحدة*.

[59] تجدر الإشارة إلى أنّ تعريف الفعل في نهاية المطاف كجريمة أو تهديد قد يكون غامضاً وقابلاً للتأويل، ويختلف من دولة إلى أخرى.

[60] لا رو، ف. (2013). *A/HRC/23/40*: تقرير المقرّر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير. *مجلس حقوق الإنسان التابع للأمم المتحدة*.

[61] دونيا مياتوفيتش (2023). *برامج التجسّس الشديدة التطفل تهدد جوهر حقوق الإنسان*(*Highly Intrusive Spyware Threatens the Essence of Human Rights*) مجلس أوروبا، تعليقات حول حقوق الإنسان.
https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights

[62] *المقرّر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير (2019). A/HRC/41/35*: المراقبة وحقوق الإنسان. تقرير المقرّر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير. *مجلس حقوق الإنسان التابع للأمم المتحدة*.

[63] موسوعة "بريتانيكا" (2024). ستوكسنت | دودة حاسوبية. في: *موسوعة "بريتانيكا"*. [متاح على الإنترنت]. متوفر على:
.https://www.britannica.com/technology/Stuxnet

[64] نيكول بيرلروث (2021). *هكذا يقولون إنّ العالم سينتهي: سباق التسلّح السيبراني* (*This Is How They Tell Me The World Ends: The Cyber-Weapons Arms Race*)، 389-90.

[65] باباديميتريو، ج.. (2023). التصدي للاستبداد الرقمي (Disrupting Digital Authoritarians).

ترليون سنة لفك تشفير المعيار AES-128 المعتمد من قبل الحكومة الأميركية لحماية المعلومات المصنّفة على أنها "سرّية".[66] [67] [68]

يقدّم بائعو برامج التجسّس التجارية حلاً بديلاً. فبدلاً من الاضطرار إلى اختراق خوارزميات التشفير من طرف إلى طرف المستخدمة على نطاق واسع وفكّ تشفير البيانات أثناء تنقّلها بين المستخدمين، يمكن للحكومات استخدام برامج التجسّس للسيطرة على الأجهزة التي تتلقى اتصالات مشفّرة.[69] فبمجرد وصول الاتصالات المشفّرة إلى تطبيق المستخدم النهائي، مثل "سيغنال" أو "واتساب" أو iMessage، يتم تفكيك شيفرتها ليتمكن المستخدم من قراءتها والتفاعل معها.[70]

بالإضافة إلى ذلك، يتيح شراء واستخدام برامج التجسّس التي يطوّرها بائعو برامج التجسّس التجارية للحكومات فرصة التنصّل علناً من المسؤولية والتمتّع بهامش من الإنكار المعقول. وقد ظهر ذلك بوضوح عندما فرضت وزارة التجارة الأميركية عقوبات على شركة بيع برامج التجسّس الإسرائيلية، مجموعة "إن إس أو"، بسبب برنامجها التجسّسي الرئيسي "بيغاسوس"، على الرغم من أنّ الولايات المتحدة كانت قد أبرمت سراً عقداً مع الشركة قبل خمسة أيام من إعلان هذه العقوبات.[71] ويؤدي هذا النوع من الاستخدام إلى نشوء دورة من العرض والطلب على برامج التجسّس، ويحفّز بائعي برامج التجسّس التجارية على تطوير المزيد منها.

عندما تتمكّن الجهات التي تشغّل برامج التجسّس من جمع ما يكفي من الأدلّة، يمكنها حينها اللجوء إلى أشكال تقليدية من العنف القمعي. وفي نهاية المطاف، ليس من قبيل الصدفة أنّ معظم بلدان منطقة غرب آسيا وشمال أفريقيا تُعدّ أنظمة استبدادية، إذ تبيّن تورّطها في استخدام برامج التجسّس أو ارتباطها بها. فهذه البرامج، باعتبارها أداة متقدّمة لممارسة أساليب الإكراه المنخفضة الشدة، تمكّن الحكومات من مراقبة السكان والتحكّم بهم وقمعهم.

كيف تعمل برامج التجسّس والشركات التي تبيعها

يمكن فهم طريقة عمل برامج التجسّس من خلال تحليل ما يُعرف بـ"سلسلة القتل" (kill chain)، وهي سلسلة من الإجراءات التي تمكّن البرمجيات الخبيثة من استغلال الجهاز المستهدف واستخراج بياناته بنجاح. وقد روّجت شركة "لوكهيد مارتن" (Lockheed Martin) للصناعات الدفاعية لهذه الفكرة من خلال تطوير "سلسلة القتل السيبرانية" (Cyber Kill Chain)، وهي نموذج لتحليل الهجمات الإلكترونية يقسّم الهجوم إلى المراحل التالية: الاستطلاع، والتسليح، والتسليم، والاستغلال، والتثبيت، والقيادة والسيطرة، وتحقيق الأهداف.[72]

---

[66] فريق Proton (2021). فك تشفير الخصوصية #3: هل يمكن فك التشفير؟ (Privacy Decrypted #3: Can encryption be broken?). *Privacy guides*. متوفر على: https://proton.me/blog/can-encryption-be-broken

[67] لين هاثاواي (2003). *السياسة الوطنية لاستخدام معيار التشفير المتقدم (AES) لحماية أنظمة الأمن القومي ومعلومات الأمن القومي* (*National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*). المعهد الوطني للعلوم والتكنولوجيا.

[68] تتطلب المعلومات الاستخباراتية "البالغة السرية" استخدام تشفير AES-192 أو AES-256.

[69] بابادیمیتریو، ج.. (2023). التصدي للاستبداد الرقمي (Disrupting Digital Authoritarians).

[70] كولير، ك. (2025). *لماذا يُمكن لتطبيق "سيغنال" الذي كان محور تسريب رسائل ضربات اليمن، أن يترك ثغرة يمكن للمخترقين استغلالها؟* (*Why Signal, the App at the Center of the Leaked Yemen Strikes Messages, Can Leave the Door Open for Hackers*). [متاح على الإنترنت]. NBC News. متوفر على: https://www.nbcnews.com/tech/security/signal-app-used-hegseth-can-leave-door-open-hackers-rcna197956 [تم الاطلاع عليه في: 14 حزيران/يونيو 2025].

[71] وزارة التجارة الأميركية (2021). *وزارة التجارة تدرج مجموعة "إن إس أو" وشركات أجنبية أخرى في قائمة الكيانات المحظورة بسبب أنشطة إلكترونية خبيثة* (*Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*) [متاح على الإنترنت] وزارة التجارة الأميركية. متوفر على: https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list [تم الاطلاع عليه في: 11 آب/أغسطس 2025].

[72] لوكهيد مارتن (2025). *سلسلة القتل السيبراني* (Cyber Kill Chain) [متاح على الإنترنت] لوكهيد مارتن. متوفر على: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

يقسّم باحثو استخبارات التهديدات في مجموعة تحليل التهديدات التابعة لـ"غوغل" سلسلة القتل في برامج التجسّس إلى خمس مراحل محدّدة:

1. التسليم إلى المستخدم المستهدَف: كيف يقوم بائعو برامج التجسّس التجارية بتسليم البرمجيات الخبيثة التي تطلق سلسلة القتل، مثلاً عبر بريد إلكتروني، أو رسالة "واتساب"، أو رسالة نصية.
2. الاستغلال: كيف يستغل المهاجمون ثغرات البرامج للوصول إلى بيانات الجهاز المستهدف.
3. تثبيت برامج التجسُّس: كيف يتمكّن المهاجمون من الحصول على وصول كامل (صلاحيات الجذر) إلى الجهاز وتنزيل برامج التجسس بشكل سرّي.
4. جمع المعلومات: كيف تقوم برامج التجسّس بمراقبة الضحية وجمع المعلومات والبيانات.
5. استخراج البيانات: كيف يتحكم المهاجمون عن بُعد في الجهاز، ثم يرسلون البيانات المجمّعة لأنفسهم.[73]

من خلال هذه المراحل الخمس، تقوم برامج التجسّس بسرقة بيانات الضحايا. ووفق ما تُظهره تقارير "سيتيزن لاب"، فإنّ برامج التجسّس التي يوفّرها بائعو برامج التجسّس التجارية، مثل "بيغاسوس" التابع لمجموعة "إن إس أو"، أو "راين" (Reign) و"كينغسباون" (Kingspawn) التابعين لشركة "كوادريم"، قادرة على تتبّع المستخدمين، والوصول إلى الرسائل في تطبيقات المراسلة المختلفة، والتسجيل من الميكروفون والكاميرا الأمامية والخلفية، بالإضافة إلى النقل غير المصرّح عنه للمعلومات الأخرى. وكما تُبرز شركة "فورتينت" (Fortinet)، فإن برامج التجسّس على الأجهزة المحمولة قادرة على الوصول إلى جميع معلومات المستخدم تقريباً، بما في ذلك سجلات المكالمات، وسجل التصفّح، وتتبّع الموقع عبر نظام تحديد المواقع العالمي (GPS)، واستخدام الميكروفون والكاميرا، وضغطات المفاتيح.[74]

تشمل بعض أنواع برامج التجسّس الشائعة برمجيات الإعلانات (Adware)، وبرامج سرقة المعلومات (Infostealer)، وبرامج رصد لوحات المفاتيح (Keylogger)، وبرامج أدوات التأصيل (Rootkit)، وبرامج تتبع البيانات (Red Shell)، وأدوات مراقبة النظام (System monitors)، ومتتبّعات ملفات تعريف الارتباط (Cookie trackers)، وأحصنة طروادة (Trojan horses).[75] وتتجسّس جميع أنواع هذه البرامج على المستخدم من دون موافقته لنقل البيانات بشكل غير مصرّح به وإرسالها إلى المهاجم. وفي حين أن معظم برامج التجسّس تستهدف الأجهزة التي تعمل بنظامَي "ويندوز" و"أندرويد" نظراً لهيمنتهما على السوق العالمية (حيث بلغت حصة "أندرويد" في السوق العالمية 71.88%[76] و"ويندوز" 72% في العام 2025[77])، فإن بعض الإصدارات المستحدثة من برامج التجسّس تستهدف أيضاً أجهزة "آبل" أو "لينُكس". ومن الأمثلة الشهيرة التي تُبرز ذلك ما حدث في العام 2016، حين أفادت منظمة "سيتيزن لاب" بأن الإمارات العربية

---

[73] مجموعة تحليل التهديدات التابعة لغوغل (2024أ). *شراء برامج التجسّس: رؤى حول بائعي برامج المراقبة التجارية* (*Buying Spying: Insights into Commercial Surveillance Vendors*). [متاح على الإنترنت] ص. 16.

[74] فورتينت (2024) (Fortinet). ما هي برامج التجسس؟ التعريف، والأنواع، والحماية (What Is Spyware? Definition, Types and Protection).

[75] فورتينت (2024) (Fortinet). ما هي برامج التجسس؟ التعريف، والأنواع، والحماية (What Is Spyware? Definition, Types and Protection).

[76] شريف، أ. (2025). *الحصة السوقية لأنظمة تشغيل الأجهزة المحمولة في العالم من عام 2009 إلى عام 2025، حسب الربع السنوي* (*Market share of mobile operating systems worldwide from 2009 to 2025, by quarter*). [متاح على الإنترنت] متوفر على: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

[77] شريف، أ. (2025). *الحصة السوقية العالمية لأنظمة تشغيل أجهزة الحاسوب المكتبي من كانون الثاني/يناير 2013 وحتى آذار/مارس 2025* (*Global market share held by operating systems for desktop PCs, from January 2013 to March 2025*). [متاح على الإنترنت] متوفر على: https://www.statista.com/statistics/218089/global-market-share-of-windows-7/

المتحدة اشترت برنامج "بيغاسوس" من مجموعة "إن إس أو"، واستغلّت ثغرات في نظام iOS على أجهزة "آيفون" لاستهداف المُدافع عن حقوق الإنسان أحمد منصور.[78]

تُباع برامج التجسُّس كغيرها من البرمجيات. فتُصنّع الشركة منتجاً، وتُسوّقه، وتلتقي بعملائها لعرض آلية عمله، ثم تبيعه بموجب عقود. مع ذلك، وبما أن بائعي برامج التجسّس متخصّصون في برمجيات تُستخدم كأسلحة سيبرانية ويبيعون منتجاتهم لجهات حكومية غالباً ما تنتهك حقوق الإنسان، فإن هذه الشركات تعمل بطريقةٍ مختلفة إلى حدٍّ ما.

يعمل بائعو برامج التجسّس في دورةٍ تتألّف من ثلاث مراحل رئيسية:[79]

1. تحديد الثغرات وتطوير برمجيات استغلال مخصَّصة لها، أو شراء برمجيات الاستغلال من البائعين.
2. تطوير منتج مراقبة يعتمد على تلك الثغرات الأمنية أو برمجيات الاستغلال.
3. تسويق وبيع منتجات برامج التجسّس الجاهزة للعملاء (وبالدرجة الأولى جهات حكومية).

وجد باحثو فريق تحليل التهديدات في "غوغل" في العام 2024 أن 50٪ من برمجيات استغلال يوم الصفر (zero-day exploits) التي استهدفت أجهزة ومنتجات "غوغل" كانت من صُنع شركات برامج التجسّس.[80] ومع ذلك، لا توجد طريقة لمعرفة عدد هذه المنتجات التي تم تطويرها داخلياً مقابل تلك التي تم شراؤها من بائعين خارجيّين. وكما هي الحال عادةً في "لعبة القط والفأر" بين الجهات المهدِّدة والباحثين في مجال الأمن السيبراني، فإن بائعي برامج التجسّس يستمرّون في شراء ثغرات أمنية وبرمجيات استغلال جديدة أو البحث عنها مع قيام شركات التكنولوجيا الكبرى بسد الثغرات الموجودة.

1.3 المصطلحات

[78] ماركزاك، ب.، سكوت-رايلتون، ج. (2016). *مُعارض المليون دولار: ثغرات يوم الصفر (Zero-Days) في جهاز "آيفون" التي استخدمتها مجموعة "إن إس أو" لاستهداف مُدافع إماراتي عن حقوق الإنسان* (*The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*). [متاح على الإنترنت] The Citizen Lab. متوفر على: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[79] مجموعة تحليل التهديدات في غوغل (2024). *شراء برامج التجسّس: رؤى حول بائعي برامج المراقبة التجارية* (*Buying Spying: Insights into Commercial Surveillance Vendors*). [متاح على الإنترنت] ص.11. متوفر على: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf

[80] مجموعة تحليل التهديدات في غوغل (2024). *الخطوة التالية في نضالنا ضد برمجيات التجسّس* (The Next Step in our Fight against Spyware). موقع *The Keyword*. متوفر على: https://blog.google/outreach-initiatives/public-policy/spyware-amicus-brief/ [تم الاطلاع عليه في: 10 آب/أغسطس 2025].

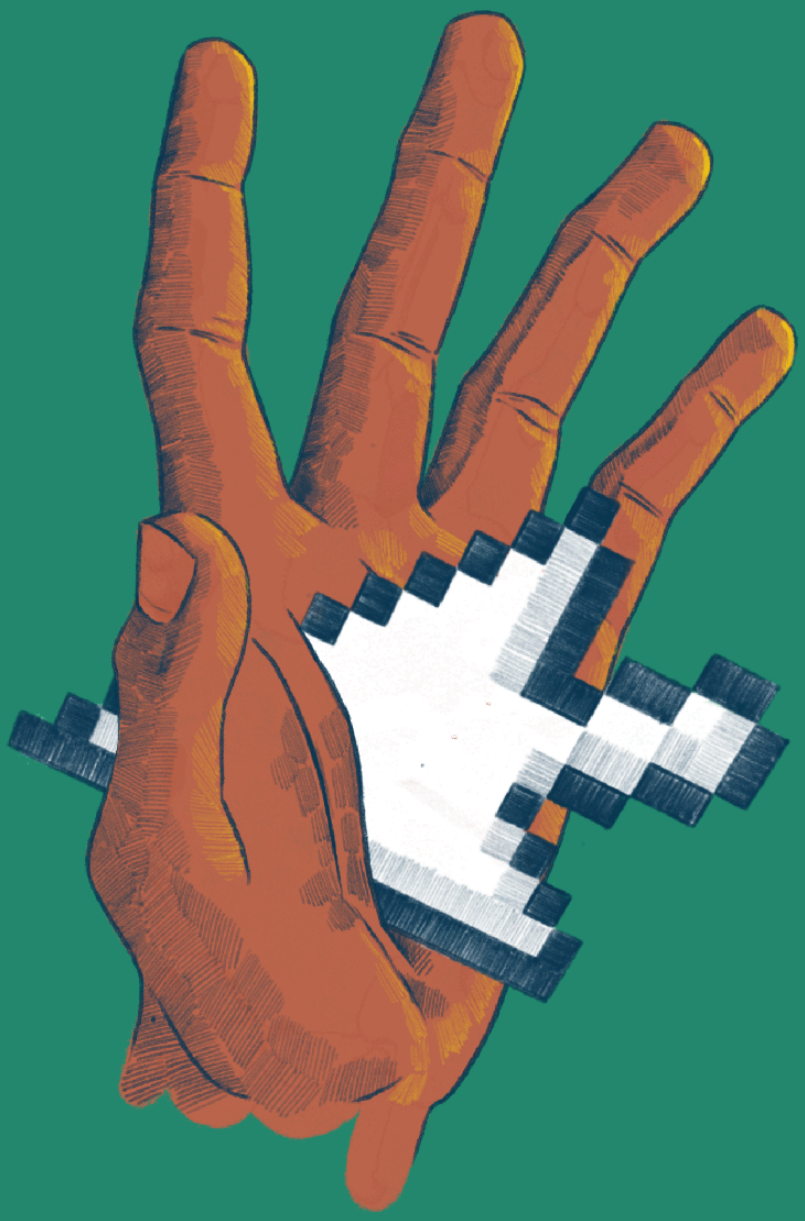
الجدول 1: المصطلحات

مصطلحات الأمن السيبراني الشائعة الاستخدام في هذا التقرير

المصطلح	التعريف
بائع برامج التجسُّس التجارية (CSV)	شركة تقوم بنتاج وتسويق و/أو بيع برامج التجسّس أو تقنيات مشابهة.
الصادرات ذات الاستخدام المزدوج	المنتجات التي يمكن استخدامها لأغراض مدنية وعسكرية على حد سواء. وتُعدّ برامج التجسّس من المنتجات ذات الاستخدام المزدوج. ينظّم اتفاق واسينار لعام 1996 تصدير هذه المنتجات. كما تُعرِّف منظمة العفو الدولية المواد ذات الاستخدام المزدوج بأنها "منتجات تتمتّع بمستوى عالٍ من القدرات التكنولوجية وتنطوي على مخاطر أمنية".
برمجية الاستغلال (Exploit)	برنامج يستفيد من ثغرة أمنية موجودة في جهاز حاسوب أو ضمن نظام حاسوبي.
شركة قابضة	شركة تمتلك حصة جزئية أو كاملة في شركة أخرى. تسيطر الشركات القابضة على شركاتها التابعة.
سلسلة القتل (kill chain)	سلسلة من الإجراءات التي تمكّن البرمجيات الخبيثة من إصابة الجهاز بنجاح.
البرمجيات الخبيثة (Malware)	مصطلح مُركّب في اللغة الإنكليزية من كلمتَي malicious (خبيث) وsoftware (برمجيات). تُشير البرمجيات الخبيثة بشكل عام إلى البرمجيات التي تهدف إلى الإضرار بالمستخدم أو أجهزته.
حقن الشبكة	تقنية تتيح للمهاجمين الوصول إلى الضحايا من خلال حزم بيانات مُعدَّلة "تُحقَن" داخل شبكة المستهدَف بغرض اعتراضها أو حجبها أو تعديلها.
الاستغلال بنقرة واحدة	ناقل تهديد يتطلب تفاعلاً من المستهدَف لتفعيل سلسلة القتل للبرمجيات الخبيثة. ومن الأمثلة الشائعة على ذلك النقر على رابط خبيث.
برامج التجسّس	مصطلح مُركّب في اللغة الإنكليزية من كلمتَيspy (تجسّس) وsoftware (برمجيات)، ويشير إلى نوع من البرمجيات الخبيثة التي تراقب الضحايا من دون علمهم.
ناقل التهديد	يُستخدم هذا المصطلح غالباً بالتبادل مع "ناقل الهجوم"، ويشير إلى الأساليب التي تستخدمها الجهات المهدِّدة لاختراق البنية التحتية للمستهدَف.
الثغرة الأمنية	يمكن اعتبار الثغرة الأمنية خللاً في أمن النظام الرقمي.
منطقة غرب آسيا وشمال أفريقيا	مصطلح جغرافي يُستخدم جزئياً لتجنّب الدلالات الاستعمارية لمصطلحات مثل "الشرق الأوسط". تشمل منطقة غرب آسيا وشمال أفريقيا الجزائر، والبحرين، وجيبوتي، ومصر، والعراق، والأردن، والكويت، ولبنان، وليبيا، والمغرب، وسلطنة عُمان، وقطر، والمملكة العربية السعودية، والصومال، والسودان، وسوريا، وتونس، وتركيا، والإمارات العربية المتحدة، والصحراء الغربية، واليمن.
برمجية الاستغلال بدون أي نقرة (Zero-click exploit)	ناقل تهديد لا يتطلّب أيّ تفاعلٍ من المستهدَف لتفعيل سلسلة القتل الخاصة بالبرمجيات الخبيثة. تستخدم هذه البرمجيات عادةً الإنترنت وتستغل الثغرات الأمنية في تطبيقات الهاتف المحمول، مثل "واتساب".
يوم الصفر (Zero-day)	يوم الصفر أو ثغرات يوم الصفر هي نوع من الثغرات الأمنية غير المعروفة لمطوّري البرمجيات وليس لها حل معروف. تستخدم برمجيات استغلال يوم الصفر ثغرات يوم الصفر لاستهداف الأنظمة التي تحتوي على هذا النوع من الثغرات البرمجية.

الجدول: "سمكس": المصدر: قائمة مصطلحات مختبر الأمن التابع لمنظمة العفو الدولية: "ما هي برمجية الاستغلال؟" (Cisco)؛ "ما هي ناقلات الهجوم؟" (CrowdStrike)؛ "ما هي البرمجيات الخبيثة؟" (Malwarebytes). تم إعداده باستخدام Datawrapper.

الجزء الثاني: المنهجية



2.1 مصادر البيانات والنطاق

يهدف هذا التقرير إلى تسليط المزيد من الضوء على أنواع برامج التجسّس التي يستخدمها بعض من أكبر بائعي هذه البرامج في منطقة غرب آسيا وشمال أفريقيا. ولكن كيف يمكن تحديد بائعي برامج التجسّس المؤهّلين لإدراجهم في الدراسة؟ إنّ البحث في مجال بائعي برامج التجسّس والبرامج نفسها أمر معقّد بطبيعته، ويعود ذلك للطابع السري الذي تتّسم به هذه الشركات. ونظراً إلى أنهم يبيعون منتجاتهم لجهات حكومية ويخضعون لضوابط التصدير في العديد من الدول لأن تلك المنتجات تعتبر ذات استخدام مزدوج، يعمل بائعو برامج التجسّس عادةً بسرية تامّة ويقيمون علاقات مؤسَّسية معقَّدة عمداً. ونتيجة لذلك، لا تتوفر معلومات كافية عن أماكن نشاط هؤلاء البائعين.

كان فيلدستاين وكوت (2023) من أوائل الباحثين الذين تصدّوا لهذا الاتجاه، حيث قاما بإنشاء مجموعات بيانات لتصنيف وتتبّع الحوادث الكبرى المرتبطة بالتجسّس حول العالم من العام 2011 إلى العام 2023. واستند فيلدستاين وكوت في إعداد هذه المجموعات إلى النتائج التي توصلت إليها وسائل الإعلام، والمبلّغون عن المخالفات، ومنظمات المراقبة، والمدافعون الدوليون عن حقوق الإنسان مثل منظمة العفو الدولية، و"سيتيزن لاب"، و"هيومن رايتس ووتش"، و"سمكس". يُعَدّ مختبر "سيتيزن لاب" في جامعة تورنتو من أبرز المختبرات البحثية التي ساهمت في تعميق فهمنا لبرمجيات التجسّس. وقد أصدر المركز عدداً من التقارير التي كشفت عن الأنشطة والتكتيكات والتقنيات والإجراءات المرتبطة ببائعي برامج التجسّس التجارية في منطقة غرب آسيا وشمال أفريقيا، وأبرزها "بيغاسوس" التابع لمجموعة "إن إس أو"، بالإضافة إلى "هاكينغ تيم" (Hacking Team)، و"باراغون"، و"سايتروكس" (Cytrox) و كوادريم".[81] [82] تُتيح المعلومات المتاحة للجمهور سبيلاً للتوصل إلى فهم أفضل لبرامج التجسس المُستخدمة وأماكن استخدامها. ويتبع هذا التقرير خطى فيلدستاين وكوت، ويعتمد على بياناتٍ صادرة عن أو مُصنّفة من قِبَل منظمات بارزة في مجال المراقبة وحقوق الإنسان - بما في ذلك منظمة العفو الدولية، و"سيتيزن لاب"، ومؤسسة كارنيغي للسلام الدولي، و"هيومن رايتس ووتش" - بالإضافة إلى تتبّع وسائل الإعلام المرموقة، ووثائق المحاكم، وسجلات الشركات. وأخيراً، أجرت منظمة "سمكس" مقابلات مع عدد من ضحايا برامج التجسّس/البرمجيات الخبيثة الذين تواصلوا مع منصة دعم السلامة الرقمية التابعة لها. وفي هذا السياق، يطرح هذا البحث السؤال التالي: من هم بائعو برامج التجسّس التجارية العاملون في منطقة غرب آسيا وشمال أفريقيا؟

بعد آخر تحديث لبيانات فيلدستاين وكوت حول حوادث برامج التجسّس في أوائل العام 2023، سيعتمد هذا التقرير على مجموعتهما من البيانات لتتبع حالات استخدام برامج التجسّس المعلنة في منطقة غرب آسيا وشمال أفريقيا خلال الفترة الممتدة بين أوائل 2023 وحتى 2025. تمتد منطقة غرب آسيا وشمال أفريقيا من المغرب والصحراء الغربية وموريتانيا، إلى مصر والسودان وجيبوتي والصومال في أفريقيا، وتشمل أيضاً دول الخليج وبلاد الشام والعراق وتركيا في الشمال.[83] يحلل هذا التقرير بائعي برامج التجسّس الناشطين الذين تم الإبلاغ عن استخدام برامجهم من قبل دول في منطقة غرب آسيا وشمال أفريقيا بشكل متكرر. كما يقدّر التقرير نشاط بائعي برامج التجسّس التجارية اعتماداً على حوادث برامج التجسّس المبلّغ عنها، بهدف تحديد الشركات الأكثر نشاطاً، أي تلك التي يبدو أن لديها عدداً أكبر من العقود، وإيرادات أعلى، وعدداً أكبر من الأهداف. وبالترتيب التنازلي، تظهر هذه الشركات كما يلي.

---

[81] سيينا أنستيس (2018). التقاضي والشكاوى الرسمية الأخرى المتعلقة ببرمجيات التجسّس التجارية (Litigation and other formal complaints related to mercenary spyware) - "سيتيزن لاب" (Citizen Lab). [متاح على الإنترنت] ."سيتيزن لاب" (Citizen Lab). متوفر على: https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-th e-digital-surveillance-industry/ [تم الاطلاع عليه في: 14 حزيران/يونيو 2025].

[82] ماركزاك، ب.، سكوت-رايلتون، ج.، بيري، أ.، الجيزاوي، ن.، أنستيس، س.، بانداي، ز.، ليون، إ.، عبد الرزاق، ب.، ديبرت، ر. (2023). Sweet QuaDreams: نظرة أولية على برمجيات الاستغلال والضحايا والعملاء لدى شركة بيع برامج التجسّس "كوادريم" (Sweet) (QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers). [متاح على الإنترنت] ."سيتيزن لاب" (Citizen Lab). متوفر على: https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

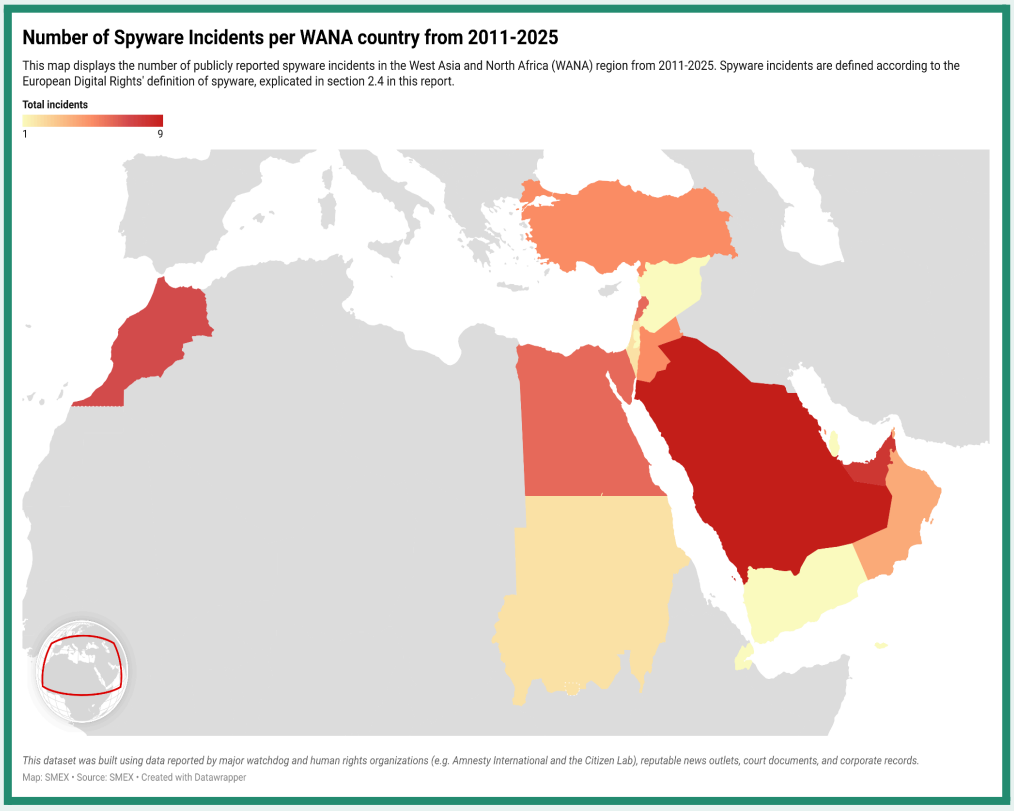
[83] في المجمل، تشمل هذه المنطقة الجزائر، والبحرين، وجيبوتي، ومصر، والعراق، والأردن، والكويت، ولبنان، وليبيا، والمغرب، وسلطنة عُمان، وقطر، والمملكة العربية السعودية، والصومال، والسودان، وسوريا، وتونس، وتركيا، والإمارات العربية المتحدة، والصحراء الغربية، واليمن.

Table 2: Most Active CSVs in SWANA Region

Commercial surveillance vendor ▲	Number of SWANA countries suspected of being customers	Number of employees	Annual Profit	Number of customers across the world
Cellebrite	At least 5	1,167 as of 2024	$56.9 million in 2024	Customers in more than 100 countries
Cytrox/Intellexa	At least 4	26 in 2021 via Thalestris	$7,649,829 in 2021	At least 14; the US Treasury claims it has a “global” customer base
NSO Group	At least 12	Approximately 350 in 2025	Allegedly ~$12 million in 2024	54 customers in 31 countries as of 2024
Saito Tech	At least 6	Between 70 and 150	$20 million in 2017	Customers in over 60 countries, as of 2017

Sources: "WhatsApp Inc. v. NSO Group Technologies Limited," NSO Group's 2024 Transparency and Responsibility Report, Feldstein and Kot's "Why Does the Global Spyware Industry Continue to Thrive?," US Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium, and "Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed" •

Annual profit in this table records the most recent reporting for each respective company's or group's profit in a given year.



الجدول 2: أكثر بائعي برامج التجسّس التجارية نشاطاً في منطقة جنوب غرب آسيا وشمال أفريقيا

بائع برامج التجسّس التجارية	عدد دول منطقة جنوب غرب آسيا وشمال أفريقيا المشتبه بكونها عملاء	عدد الموظفين	الأرباح السنوية	عدد العملاء حول العالم
"سيلبرايت" Cellebrite	5 على الأقل	1,167 حتى عام 2024	56.9 مليون دولار أميركي في 2024	عملاء في أكثر من 100 دولة

بائع برامج التجسّس التجارية	عدد دول منطقة جنوب غرب آسيا وشمال أفريقيا المشتبه بكونها عملاء	عدد الموظفين	الأرباح السنوية	عدد العملاء حول العالم
"سايتروكس" (Cytrox)/"إنتلكسا" (Intellexa)	4 على الأقل	26 في 2021 عبر "ثالستريس"	7,649,829 دولار أميركي في 2021	14 عميلاً على الأقل؛ تشير وزارة الخزانة الأميركية إلى أن لديها قاعدة عملاء "عالمية"
مجموعة "إن إس أو"	12 على الأقل	حوالي 350 في 2025	يحسب التقارير -12 مليون دولار أميركي في 2024	54 عميلاً في 31 دولة حتى 2024
"سايتو تيك" (Saito Tech)	6 على الأقل	بين 70 و150	20 مليون دولار أميركي في 2017	عملاء في أكثر من 60 دولة حتى 2017

المصادر:

"قضية شركة "واتساب" ضد مجموعة "إن إس أو" المحدودة" (WhatsApp Inc. v. NSO Group Technologies Limited)، تقرير الشفافية والمسؤولية لعام 2024 الخاصة بمجموعة "إن إس أو"، مقالة فيلدستاين وكوت " لماذا تستمر صناعة برامج التجسّس العالمية في الازدهار؟" *(Why Does the Global Spyware Industry Continue to Thrive?)*، وزارة الخزانة الأميركية تفرض عقوبات على أعضاء في تحالف "إنتلكسا" لبرامج التجسس التجارية (Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium)، اختراق الهواتف المحمولة وصفقات بملايين الدولارات في الخليج: الكشف عن العمليات الداخلية لشركة إسرائيلية سريّة متخصصة في الهجمات السيبرانية (*Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*).

ترتكز الأرباح السنوية المذكورة في هذا الجدول على أحدث البيانات المبلغ عنها لكل شركة أو مجموعة في سنة محددة.

عدد حوادث برامج التجسّس لكل دولة في منطقة غرب آسيا وشمال أفريقيا خلال الفترة 2011-2025

تُظهر هذه الخريطة عدد الحوادث المُبلّغ عنها علناً والمتعلقة ببرامج التجسّس في منطقة غرب آسيا وشمال أفريقيا خلال الفترة الممتدة بين العامين 2011 و2025.
ويتم تعريف "حوادث برامج التجسّس" وفقاً للتعريف المعتمد من منظمة الحقوق الرقمية الأوروبية (EDRi)، والمبيَّن في القسم 2.4 من هذا التقرير.

إجمالي الحوادث 1 9

تم إعداد مجموعة البيانات هذه استناداً إلى المعلومات الصادرة عن منظمات المراقبة وحقوق الإنسان الكبرى (مثل منظمة العفو الدولية و"سيتيزن لاب")، بالإضافة إلى تتبّع وسائل الإعلام المرموقة، ووثائق المحاكم، وسجلات الشركات.

الخريطة: "سمكس" - المصدر: "سمكس" تم إعدادها باستخدام Datawrapper

2.2 القيود

هناك عدّة قيود على هذا النهج، ويعود ذلك أساساً إلى اعتماده على المعلومات المتاحة للعامة. ويهدف هذا التقرير، كلما أمكن، إلى التحقق من النتائج من خلال مصدَرين اثنَين على الأقل من وسائل إعلامية مختلفة. أمّا بالنسبة إلى بيانات الإصابة ببرامج التجسس، فقد اعتمدت "سمكس" على التقارير الصادرة عن مختبرات التهديدات المتخصصة، مثل "سيتيزن لاب"،

ومختبر الأمن التابع لمنظمة العفو الدولية. وفي ما يخصّ المعلومات المتعلقة بالشركات، فقد استندت "سمكس" بشكل أساسي إلى المصادر الرسمية الأولية (مثل السجلات التجارية والملفات القانونية). وفي الحالات المحدودة التي لم تكن فيها المعلومات الرسمية متاحة للعامة، استعانت "سمكس" بمجمِّعات بيانات موثوقة تابعة لجهات خارجية.

ومع ذلك، قد لا يتم إدراج بعض أكبر بائعي برامج التجسّس التجارية العاملين في المنطقة بسبب نقص المعلومات المتاحة للعامة والقابلة للتحقق (على سبيل المثال، شركة "باراغون"). كما أنّ بعض المعلومات غير متاحة أو لا يمكن التحقق منها في الوقت الراهن. ومن أبرز الأمثلة على ذلك:

- ملكية الشركات المسجّلة في ولايات قضائية منخفضة الشفافية (مثل جزر العذراء البريطانية)، ما لم يتم الكشف عن هذه المعلومات في إجراءات قانونية أو في إفصاحات الشركات ضمن ولايات قضائية أكثر شفافية.
- ملفات المشتريات التي تؤكّد شراء أيّ حكومة في منطقة غرب آسيا وشمال أفريقيا لأداة تجسّس محدّدة.
- تراخيص التصدير التي حصل عليها بائعو برامج التجسّس التجارية.

بالإضافة إلى ذلك، قد يؤدّي هذا النهج إلى حالة من الالتباس تُشبه معضلة "الدجاجة أم البيضة"، حيث يصبح من غير الواضح ما إذا كان بائعو برامج التجسّس التجاري الذين يتم تحليلهم هم الأكثر نشاطاً فعلياً في المنطقة، أم أنّهم ببساطة الأكثر عرضة للاكتشاف. وبعبارة أخرى، هل هم فعلاً يعملون أكثر من الشركات الأخرى في المنطقة ويتمّ الإبلاغ عنهم لأنّهم يستهدفون عدداً أكبر من الضحايا، أم أنهم أقلّ حذراً ويُكتشفون بشكل متكرر بسبب ارتكاب أخطاء يمكن تجنّبها؟ كلا الاحتمالين واردان. ومن الأمثلة الجيّدة على الاحتمال الأخير ما حدث في العام 2021، عندما نشرت منظمة العفو الدولية تقريراً ذكرت فيه أنّ مجموعة "إن إس أو" "ارتكبت عدّة أخطاء أمنية تشغيلية، الأمر الذي مكّن المنظمة من تطوير طريقة جنائية لتحديد برنامج التجسّس "بيغاسوس".[84]

غالباً ما يحدّد الباحثون حوادث برامج التجسّس على المستوى الجغرافي من خلال ربط مؤشرات الاختراق بمناطق معيّنة، مثل مواقع خوادم نظام أسماء النطاقات (DNS). وقد يؤدي ذلك إلى بعض الغموض عند محاولة تحديد أماكن استخدام برامج التجسّس. وكما أوضح مختبر "سيتيزن لاب" في تقريره لعام 2018 حول 45 دولة يُشتبه في إصابتها ببرنامج "بيغاسوس"، قد يؤدي استخدام مشغّلي البرنامج لشبكات افتراضية خاصة (VPN) أو لاتصالات الإنترنت عبر الأقمار الصناعية إلى حدوث أخطاء عند نسب الإصابات إلى دول معّينة.[85] بالإضافة إلى ذلك، وكما ورد في هذا التقرير، فإن بعض بائعي برامج التجسّس التجارية يوفّرون ملحقات إضافية تمكّن عملاءهم من استهداف ضحايا في دول مختلفة. لذلك، وعلى الرغم من أنّ هذا التقرير يستند إلى مصادر بيانات متعددة بهدف تحسين تحديد مواقع مشغّلي برامج التجسّس المحتملين، فإنه لا يستطيع تحديد الدول التي تستخدم برامج بائعي برامج التجسّس التجارية بدقة تامة.

في نهاية المطاف، لا يزال من غير الواضح أيّ من البائعين له بصمة أكبر في المنطقة ويمتلك أكبر عدد من العملاء والعقود، وهو ما يستدعي مزيداً من البحث والتقصّي. ونظراً لندرة البيانات في هذا المجال، يستند هذا التقرير إلى افتراضٍ مفاده أنّه يمكن استخدام حوادث التجسّس المعلَن عنها كمؤشّر تقريبي لتقدير البائعين الأكثر نشاطاً في المنطقة. ورغم أنّ مؤلّفي هذا التقرير قاموا بتحديث نتائج فيلدستاين وكوت كلّما أمكن ذلك، لا يُعتبَر هذا التقرير بأيّ حالٍ من الأحوال شاملاً أو قائمةً مكتملة بجميع حوادث برامج التجسّس وأنشطة البائعين في منطقة غرب آسيا وشمال أفريقيا.

---

[84] مختبر الأمن التابع لمنظمة العفو الدولية (2021). *تقرير منهجية التحقيق التقني الجنائي: كيف تكتشف الاختراق ببرنامج بيغاسوس التابع لمجموعة "إن إس أو"* (*Forensic Methodology Report: How to Catch NSO Group's Pegasus*). منظمة العفو الدولية. متوفر على: https://www.amnesty.org/en/documents/doc10/4487/2021/en/

[85] ماركزاك، ب.، سكوت-رايلتون، ج.، ماككون، س.، عبد الرزاق، ب.، ديبرت، ر. (2018). *لعبة الغمّيضة* (*HIDE AND SEEK*)

2.3 أهداف التقرير

تهدف هذه الورقة إلى تحقيق ثلاثة أهداف رئيسية.

1. توثيق حوادث برامج التجسّس خلال الفترة الممتدّة بين العامَين 2011 و2025. كان فيلدستاين وكوت أوّل الباحثين الذين قاموا بتوثيق الحوادث الكبرى لبرامج التجسّس على مستوى العالم، وقد حدّثا قاعدة بياناتهم آخر مرة في العام 2023. بالإضافة إلى ذلك، لم يصدر أي تقرير بحثي رئيسي يُحلّل أيّ من بائعي برامج التجسّس التجارية ينشطون أكثر في منطقة غرب آسيا وشمال أفريقيا استناداً إلى تقارير الحوادث. ويهدف هذا التقرير إلى تحديث عمل فيلدستاين وكوت في ما يخصّ دول منطقة غرب آسيا وشمال أفريقيا وتوثيق الحوادث الكبرى لبرامج التجسّس في المنطقة. واستناداً إلى هذه المعطيات، سيحلّل التقرير أيضاً بائعي برامج التجسّس الذين يبدو أنّهم ينشطون بشكل أكبر في المنطقة.
2. تقديم إسهامات جديدة لتعزيز فهم الجمهور لكيفية عمل بائعي برامج التجسّس التجارية، بدعم من منظمة "فايند" (FIND).
3. إظهار الأثر البشري لبرامج التجسّس من خلال المقابلات التي أجرتها "سمكس" مع ضحايا هذه البرامج. تنتهك برامج التجسّس حقوق الإنسان الأساسية، ويسلّط هذا التقرير الضوء على ما يعنيه ذلك يومياً للصحافيّين والمدافعين عن حقوق الإنسان والمُعارضين.

2.4 الملاحظات والتعريفات

عند النظر في الحوادث التي وقعت خلال الفترة الممتدّة بين العامَين 2011 و2025، لا بدّ من الإشارة إلى عدّة ملاحظات مهمّة. أوّلاً، إن بعض بائعي برامج التجسّس التجاريّة الأكثر نشاطاً أو شهرة في منطقة غرب آسيا وشمال أفريقيا، مثل "فينفيشر" (FinFisher) و"كوادريم"، لم يعودوا نشطين، وبالتالي لم يتمّ تضمينهم في هذا التقرير.[86] ثانياً، من الجدير بالذكر أنّه على الرغم من احتلال شركة "ميمينتو لابز" (Memento Labs) المرتبة الثانية من حيث عدد مرّات الظهور في هذه المجموعة من البيانات، فإنّ آخر حادثة أُبلِغ عنها علناً تعود إلى العام 2015. ولو تناول هذا التقرير سنوات إفصاح مختلفة، لكان ظهور هذه الشركة أقلّ تكراراً (على سبيل المثال، مرّة واحدة فقط خلال الفترة 2015–2020، أو عدم الظهور إطلاقاً خلال الفترة 2020–2025). ويعرض الملحق "أ" مزيداً من المعلومات حول أسباب عدم إدراج "ميمينتو لابز" من قبل مؤلّفي هذا التقرير. لتوثيق ما يُعتبَر "حادثة تجسّس" بدقة أكبر، يُعرِّف هذا البحث برامج التجسّس استناداً إلى تعريف منظمة الحقوق الرقمية الأوروبية (EDRi)، وذلك اعتباراً من حزيران/يونيو 2025. برامج التجسس هي "... البرامج التي تستوفي الشروط التالية":

1. تم تثبيتها أو تشغيلها على جهاز دون موافقة حرة وواعية من [المستخدِم النهائي]؛
2. تقوّض سلامة الجهاز؛
3. يتم نشرها بشكل أساسي من خلال استغلال الثغرات الموجودة أو التي تم إنشاؤها في الأنظمة الرقمية؛
4. بعد التثبيت، يتم تشغيلها تلقائياً أو عن بُعد؛
5. يمكن أن تستهدف أفراداً أو مجموعات، أو يتم نشرها بشكل عشوائي.[87]

---

[86] استناداً إلى التقارير العامة، كانت شركة "فينفيشر" (FinFisher) ثاني أكبر مورّد لبرامج التجسّس التجاريّة استخداماً في المنطقة، لكنّها أوقفت نشاطها في العام 2022 بسبب مشاكل قانونية مرتبطة بانتهاكات حقوق الإنسان. كذلك، اكتسبت "كوادريم" (QuaDream) سمعة سيئة جداً في منطقة غرب آسيا وشمال أفريقيا خلال السنوات الخمس الماضية، لكنها أوقفت نشاطها بعد ظهور جدل حول أنشطتها في العام 2023.

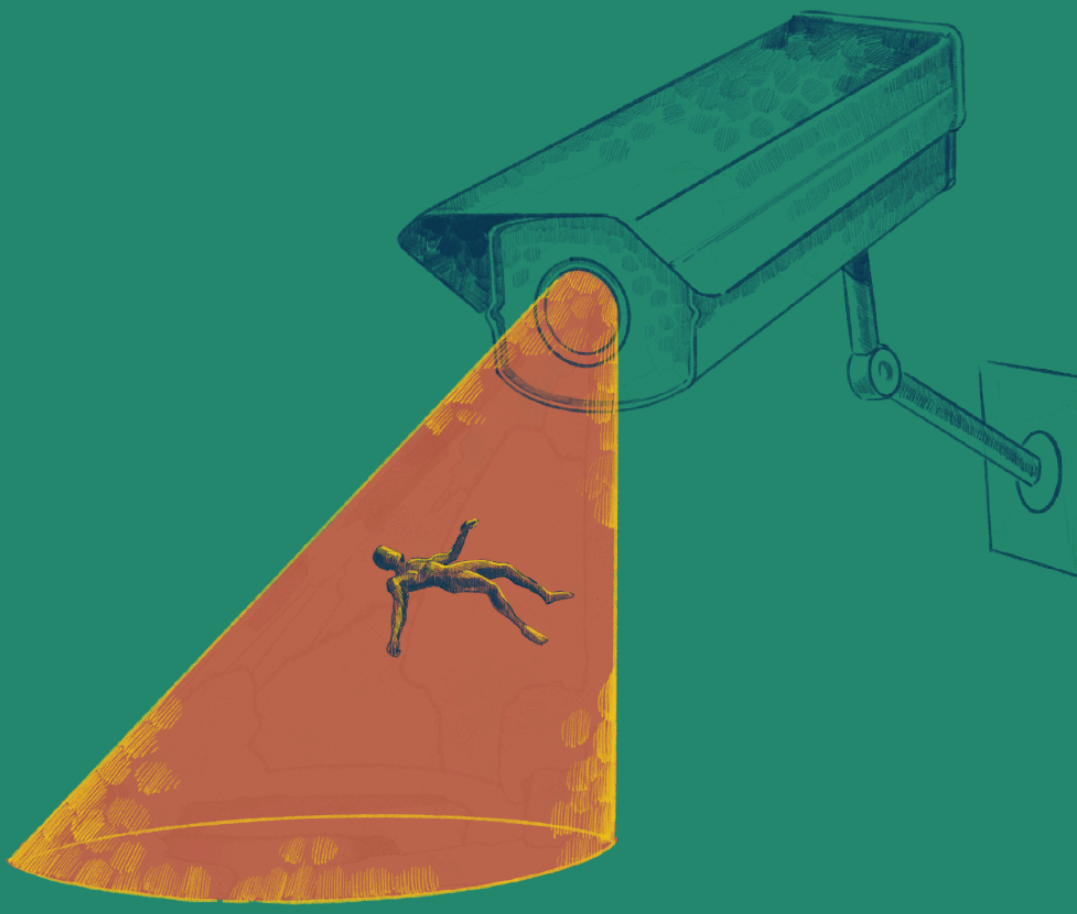
[87] بيرتيليمي، ك.، لند، ج.، لو كيريك، ب.، ريستيك، أ.، حمود، ر.، نيينهويس، ل.، ليتشتينثالير، ه.، زينغر، ر.، ناكياما شابيرو، م.، فان هولست، و. (2025). *برامج التجسّس وانتهاكات الدولة: قضية حظر على مستوى الاتحاد الأوروبي* (*Spyware and State Abuse: The Case for an*

على الرغم من أنّ شركة "سيلبرايت" لا تبيع برامج تجسّس بالمعني التقني وفقاً لهذا التعريف، فإنّ هذا التقرير يشملها لعدة أسباب رئيسية. وكما تُشير منظمة الحقوق الرقمية الأوروبية، فإنّ منتَج "سيلبرايت" الرئيسي، وهو جهاز استخراج الأدلة الجنائية العالمي (UFED)، يستوفي تقريباً جميع شروط تعريف برامج التجسّس بحسب المنظمة، باستثناء قدرته على استخراج البيانات بشكل مستمر بعد التثبيت. يتطلب جهاز استخراج الأدلة الجنائية العالمي الوصول الفعلي إلى الجهاز، على الرغم من أنّه يوفر حلولاً للتحكّم عن بُعد في البيانات المستخرجة من الأجهزة.[88] مع ذلك، وعلى غرار العديد من منتجات برامج التجسّس، فإنّ "أدوات التحليل الجنائي" الخاصة بشركة "سيلبرايت" تستغل الثغرات للوصول إلى الأجهزة، ويمكنها إنشاء نسخ كاملة من الهوية الرقمية للضحايا، بما في ذلك رسائلهم وملفاتهم واتصالاتهم، حتى على تطبيقات المراسلة المشفّرة. علاوةً على ذلك، وثّقت منظمة العفو الدولية في أواخر العام 2024 عدّة حالات استخدم فيها عملاء شركة "سيلبرايت" في صربيا منتجات جهاز استخراج الأدلة الجنائية العالمي للوصول غير المشروع إلى هواتف الضحايا من دون اتباع الإجراءات القانونية الواجبة، ثم قاموا بتثبيت برنامج التجسّس "نوفي سباي" (NoviSpy) على أجهزتهم.[89] وبناءً على ذلك، أُدرجت شركة "سيلبرايت" ضمن نطاق هذا التقرير.

EU-Wide Ban). منظمة الحقوق الرقمية الأوروبية (EDRi)،
/https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper

[88] Cellebrite.com. (2024). *Inseytes* (*Inseytes by Cellebrite*) من *سيلبرايت* (*Cellebrite*). [متاح على الإنترنت]. متوفر على:
https://cellebrite.com/en/cellebrite-inseyets/ [تم الاطلاع عليه في: 12 تموز/يوليو 2025]

[89] منظمة العفو الدولية. (2024). *صربيا: السلطات تستخدم برامج التجسّس وأدوات استخراج الأدلة الجنائية من " سيلبرايت" لاختراق هواتف الصحافيين والنشطاء* (*Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists*). [متاح على الإنترنت]. متوفر على:
https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extracti on-tools-to-hack-journalists-and-activists/ [تم الاطلاع عليه في: 3 آب/أغسطس 2025]



الجزء الثالث:
النتائج: بائعو برامج التجسّس التجارية محلّ الاهتمام

غالباً ما تسعى شركات برامج التجسّس إلى إخفاء أنشطتها، وقوائم عملائها، وقدراتها التقنية من خلال شركات وهمية، واتفاقيات عدم إفصاح، وهياكل مؤسّسية معقدة.[90] [91] وكما يشير بانسال وآخرون (2024) في تقرير صادر عن المجلس الأطلسي، فإنّ الكيانات التي تصمّم وتبيع برامج التجسّس للمُستخدمين النهائيين تعمل في الغالب بالتعاون مع شركاء. وقد يعمل بائعو برامج التجسّس من خلال شركات فرعيّة، أو يعتمدون على مستثمرين مستقلّين، أو مزوّدي خدمات (مثل وسطاء الوصول الأوّلي)، وقد يكونون جزءاً من شركات قابضة. فعلى سبيل المثال، ووفقاً لأبحاثٍ أجرتها منظمة العفو الدولية، كانت مجموعة "إن إس أو" في العام 2021 مرتبطة بشكلٍ مباشر أو غير مباشر بما لا يقلّ عن أربعة مساهمين أفراد، وثلاث عشرة شركة قابضة، واثنتي عشرة شركة فرعيّة تعمل في عدّة ولايات قضائية.[92] وتعتبر هذه العلاقات المتشعّبة معقّدة عمداً، إذ تلجأ الشركات في كثير من الأحيان إلى تغيير أسمائها بشكلٍ استراتيجي، وتوسيع نطاق عملياتها عبر الحدود الدولية لتجنّب الخضوع لأنظمة أكثر صرامة.

بعد توسيع مجموعة البيانات التي أعدّها فيلدستاين وكوت (2023) وتحليل حوادث برامج التجسّس التي وقعت خلال السنوات الأخيرة في منطقة غرب آسيا وشمال أفريقيا، لاحظت "سمكس" عدّة اتجاهات رئيسيّة بين هذه الشركات:

1. كانت مجموعة "إن إس أو" الجهة الأكثر تورّطاً في حوادث برامج التجسّس ضمن مجموعة البيانات هذه، تلتها بالترتيب التنازلي من حيث التكرار كلٌّ من "سايتو تيك"، و"سيلبرايت"، و"سايتروكس"/"إنتلكسا".
2. يبدو أنّ بائعي برامج التجسّس التجارية المتمركزين في إسرائيل يهيمنون على السوق في منطقة غرب آسيا وشمال أفريقيا، رغم وجود بائعين آخرين أيضاً، مثل MSAB من السويد، وRSC Labs من إيطاليا، وMeiya Pico من الصين.
3. يبدو أن الجهات الرئيسيّة التي كانت تهيمن سابقاً على السوق في منطقة غرب آسيا وشمال أفريقيا، مثل "فينفيشر" (FinFisher) و"هاكينغ تيم" (Hacking Team) (المعروفة حالياً باسم "ميمينتو لابز" Memento Labs)، لم تعد تتمتع بحصة كبيرة في السوق، وذلك استناداً إلى التقارير العامة حول استخدام الحكومات في المنطقة لبرامج التجسّس التي تنتجها هذه الشركات.
4. تصدّرت دولة الإمارات العربية المتحدة والمملكة العربية السعودية قائمة الدول الأكثر تورّطاً في حوادث برامج التجسّس المبلّغ عنها: ثمانية حوادث على الأقل لكل منهما. كما جرى الإبلاغ بشكل متكرّر عن المغرب (سبعة حوادث)، ومصر (ستة حوادث)، والبحرين (خمسة حوادث)، والأردن (خمسة حوادث) كعملاء محتملين لبائعي برامج التجسّس التجارية.
5. ظهر بعض بائعي برامج التجسّس التجارية الأقل شهرة أيضاً ضمن مجموعة البيانات، وهناك حاجة لإجراء المزيد من الأبحاث حول البائعين الأصغر حجماً والمتخصصين في هذا المجال.

---

[90] روبيرتس، ج.، هير، ت.، بانسال، ن.، مسييه، ن. (2024.) *الوحوش الأسطورية وأين نجدها: رسم خريطة سوق برامج التجسس العالمية وتهديداتها للأمن القومي وحقوق الإنسان.* (*Mythical Beasts and Where to Find them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*) [متاح على الإنترنت].المجلس الأطلسي. متوفر على:
https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/#methods

[91] هوراك، غ. (2023). *الكشف عن البيانات الشخصية: برامج التجسّس وحقوق الإنسان في منطقة الشرق الأوسط وشمال أفريقيا* (*Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa*). [أطروحة ماجستير]. متوفر على:
https://dash.harvard.edu/server/api/core/bitstreams/cb8802b2-a4c2-4733-8229-cb0495f0c3dc/content. [تم الاطلاع عليه في: 10 آب/أغسطس 2025]

[92] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو" (Operating from the Shadows: inside NSO Group's Corporate Structure) (NSO)*. [متاح على الإنترنت]. ص.58.

في الأقسام الفرعية الأربعة التالية، يحلّل هذا التقرير أبرز بائعي برامج التجسّس التجارية وفق مجموعة البيانات الخاصة بهذا التقرير: مجموعة "إن إس أو"، و"سايتروكس"/"إنتلكسا"، و"سيلبرايت"، و"سايتو تيك"، و"كانديرو".

3.1 مجموعة "إن إس أو" (NSO)

"يُشبه *[بيغاسوس]* عمليّات التنصّت التقليديّة... لكنّه مُصمَّم ليتلاءم مع حالات الاستخدام في العالم الحديث... *[وهو]* ليس أداةً للمراقبة الشاملة".

– مجموعة "إن إس أو" (NSO)، من تقرير المساءلة والمسؤولية لعام 2024

هيكل الشركة ومواردها المالية

أسّس نيف كارمي وشاليف هوليو وأومري لافي شركة "إن إس أو غروب تكينولوجيز المحدودة" (NSO Group Technologies Ltd.) عام 2010 في إسرائيل (الرقم التعريفي للشركة: 514395409).[93] ويزعم المؤسّسون الثلاثة أنّهم أنشأوا الشركة لتطوير منتجات تكنولوجية لوكالات إنفاذ القانون والحكومات، بهدف مكافحة الجريمة ومنع الإرهاب.[94] وقد أشار هوليو إلى أنّ أحد الأهداف الأساسية لمجموعة "إن إس أو" كان تزويد وكالات إنفاذ القانون والاستخبارات بالوسائل اللازمة لتجاوز التشفير والوصول إلى الأجهزة المحمولة المطلوبة لمكافحة الجرائم.[95] [96] ويتجلّى ذلك بوضوح في تقرير الشفافية والمسؤولية لعام 2021 الصادر عن المجموعة، حيث تزعم الشركة أنّ "مجموعة "إن إس أو" تأسست... بهدف رئيسي واحد، وهو: جعل العالم مكاناً أكثر أماناً."[97] وبالطبع، فإن أفعال مجموعة "إن إس أو" خلال العقد الماضي قد روت قصّة مغايرة تماماً.

[93] تُشكّل NSO اختصاراً للأحرف الأولى من أسماء المؤسّسين الثلاثة للشركة (باللغة الإنكليزية).

[94] مجموعة "إن إس أو" (2021). من نحن. [متاح على الإنترنت] Nsogroup.com. متوفر على: https://www.nsogroup.com/about-us/ [تم الاطلاع عليه في: 3 آب/أغسطس 2025]

[95] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو" (*Operating from the Shadows: inside NSO Group's Corporate Structure*) (NSO)". ص.29.

[96] ملاحظة: يُستخدم اسم مجموعة "إن إس أو" عادةً للإشارة إلى الكيان المؤسّسي بأكمله، في حين يُقصد بـ NSO Group Technologies Ltd. الكيان الرئيسي / الشركة التشغيليّة التابعة للمقرّ الرئيسي للمجموعة في إسرائيل.

[97] مجموعة "إن إس أو" (2021). *تقرير الشفافية والمسؤولية لعام 2021* (*Transparency and Responsibility Report 2021*). [متاح على الإنترنت]. متوفر على: https://web.archive.org/web/20250408183946/https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf [تم الاطلاع عليه في: 14 تموز/يوليو 2025]

الصورة 1: شعار موقع مجموعة "إن إس أو" الإلكتروني لعام 2019.

منذ العام 2010، رسّخت مجموعة "إن إس أو" وجودها من خلال كياناتٍ في جزر العذراء البريطانية، وبلغاريا، وجزر كايمان، وقبرص، ولوكسمبورغ، وهولندا، والمملكة المتحدة، والولايات المتحدة الأميركية. ومع مرور الوقت، أُعيدت هيكلة عدد كبير من هذه الكيانات، أو تمّت تصفيتها، أو تغيّر مالكوها نتيجة انتقالها إلى مستثمرين مختلفين. وقد بدأت المجموعة بتقديم الإصدارات الأولى من برنامج "بيغاسوس" عام 2011.[98]

استحواذ شركة "فرانسيسكو بارتنرز " (Fransisco Partners)

في العام 2014، استحوذت شركة "فرانسيسكو بارتنرز" (Francisco Partners)، وهي شركة متخصصة في مجال الأسهم الخاصة، على حصة تبلغ 70% من مجموعة "إن إس أو" مقابل 115 مليون دولار أميركي.[99] وقد أشرفت الشركة خلال فترة سيطرتها على المجموعة بين العامين 2014 و2019 على عدد من التغييرات الهيكليّة الكبرى. وخلال تلك الفترة، أصبحت عدّة شركات تجارية وقابضة جزءاً من الهيكل المؤسّسي المرتبط بمجموعة "إن إس أو"، بما في ذلك:

- شركة L.E.G.D. Company Ltd. ومقرها في إسرائيل، والتي غيّرت لاحقاً اسمها إلى "كيو سايبر تكنولوجيز المحدودة" (Q Cyber Technologies ltd) (رقم التسجيل: 514971522) وأصبحت المساهم الأكبر في مجموعة "إن إس أو".[100] في العام 2019، وصف موقع مجموعة "إن إس أو" الشركة بأنها شركة تابعة لـ"كيو سايبر تكنولوجيز" (Q Cyber Technologies)؛[101]
- OSY Technologies S.à r.l. (رقم التسجيل: B184226، ومقرها في لوكسمبورغ؛[102]
- OSY Holdings Ltd. (رقم التسجيل: 284745)، شركة قابضة مقرها في جزر كايمان، وأصبحت المساهم الوحيد في OSY Technologies S.à r.l؛[103]

---

[98] بيرغمان، ر.، مازيتي، م. (2022). المعركة من أجل أقوى سلاح سيبراني في العالم (The Battle for the World's Most Powerful Cyberweapon). صحيفة نيويورك تايمز [متاح على الإنترنت] 28 كانون الثاني/يناير. متوفر على: https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html [تم الاطلاع عليه في: 10 آب/أغسطس 2025].

[99] "بلومبيرغ إل بي" (Bloomberg L.P.)، محفظة "فرانسيسكو بارتنرز III إل بي" (Francisco Partners III LP) الحالية، تم الاطلاع عليها في 28 شباط/فبراير 2019 من خلال منصة بلومبيرغ.

[100] سلطة الشركات الإسرائيلية، شهادة تأسيس شركة2 ، L.E.G.D. Company Ltd. كانون الأول/ديسمبر 2013، متاحة كمرفق رقم 6 للشكوى في "*قضية شركة واتساب ضد مجموعة "إن إس أو" المحدودة* (WhatsApp Inc. v. NSO Group Technologies Limited)، [2025] *(NSO)* [محكمة المقاطعة، المنطقة الشمالية في كاليفورنيا). متوفر على: https://www.courtlistener.com/docket/16395340/whatsapp-inc-v-nso-group-technologies-limited/ [تم الاطلاع عليه في: 10 تموز/يوليو 2025].

[101] مجموعة "إن إس أو" (2019). *من نحن - مجموعة "إن إس أو" (NSO)* [متاح على الإنترنت]. متوفر على: https://web.archive.org/web/20190215201627/https://www.nsogroup.com/about/ [تم الاطلاع عليه في: 10 آب/أغسطس 2025]

[102] سجل التجارة والشركات في لوكسمبورغ (2014). *شهادة تسجيل شركة Osy Technologies S.à r.l. : 3 شباط/فبراير 2014.*

[103] محضر اجتماع الجمعية العامة غير العادية المنعقد في 1 كانون الأول /ديسمبر 2014 (2014). [متاح على الإنترنت] Triangle Holdings. متوفر على: www.etat.lu/memorial/2014/C/Html/4019/2014197910.html. [تم الاطلاع عليه في: 2 آب/أغسطس 2025].

- "كيو سايبر تكنولوجيز ش.م.م." (Q Cyber Technologies S.à r.l) (رقم التسجيل: B203124)، كيان تأسّس في لوكسمبورغ في 8 كانون الثاني/يناير 2016، وكانت شركة OSY Technologies المساهم الوحيد فيه.[104] لاحقاً، عرّفت مجموعة "إن إس أو" شركة "كيو سايبر تكنولوجيز ش.م.م." في رسالة موجّهة إلى منظمة العفو الدولية بوصفها موزّعاً تجارياً، يتولّى بشكل أساسي إصدار الفواتير وتلقّي المدفوعات من العملاء.[105]

أدّت عمليّات الاستحواذ المتعدّدة التي نفّذتها شركة "فرانسيسكو بارتنرز" عام 2014 على عددٍ من شركات التكنولوجيا الصغيرة إلى إعادة هيكلة مجموعة "إن إس أو" عدّة مرّات، وتوسيع نطاقها لتشمل ما لا يقلّ عن 15 شركة دوليّة موزّعة على ثماني ولايات قضائيّة.[106] وشمل ذلك عدداً من الشركات في كلٍّ من قبرص وبلغاريا، من بينها:

- IOTA Holdings Ltd. في قبرص (رقم التسجيل: 337445 ؛ مسجّلة في 4 تشرين الثاني/نوفمبر 2014[107]) وهي الشركة الأم لشركة CS-Circles Solutions Ltd. التي تتخذ من قبرص مقرّاً لها؛
- CS-Circles Solutions Ltd. في قبرص (رقم التسجيل: 336847، مسجّلة في 15 تشرين الأوّل/أكتوبر 2014[108])، وهي المالكة بالكامل لشركة CI-Compass Ltd. التي تتخذ من قبرص مقرّاً لها؛
- CI-Compass Ltd. في قبرص (رقم التسجيل: 310769، مسجّلة في 23 آب/أغسطس 2012[109])؛
- Global Hubcom Ltd. في قبرص (رقم التسجيل: 323665، مسجّلة في 18 تموز/يوليو 2013 [110])؛
- MS Magnet Solutions Ltd. في قبرص (رقم التسجيل: 309073، مسجّلة في 10 تموز/يوليو 2012[111])، وهي المالكة بالكامل لشركة MI Compass Ltd. التي تتخذ من قبرص مقرّاً لها[112]؛
- MI Compass Ltd. في قبرص (رقم التسجيل: 347278، مسجّلة في 24 أيلول/سبتمبر 2015)؛
- Circles Bulgaria EOOD [113] في بلغاريا (رقم التسجيل: 175408771، مسجّلة في تموز/يوليو 2017 [114])، وهي مملوكة لشركة CS-Circles Solutions Ltd. التي تتخذ من قبرص مقرّاً لها؛

---

[104] سجل التجارة والشركات في لوكسمبورغ (2016). *شهادة تسجيل شركة "كيو سايبر تكنولوجيز " Q Cyber Technologies : 12 كانون الثاني/يناير 2016.*

[105] منظمة العفو الدولية، (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو"* (*Operating from the Shadows: inside NSO Group's Corporate Structure*). [متاح على الإنترنت]. *منظمة العفو الدولية*، ص.84.

[106] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو"* (*Operating from the Shadows: inside NSO Group's Corporate Structure*) *"(NSO)"*. [متاح على الإنترنت]. ص.31.

[107] IOTA Holdings Ltd. (بدون تاريخ). تفاصيل تسجيل IOTA Holdings Ltd. [متاح على الإنترنت] متوفر على: https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=IOTA+Holdings&number=%25&searchtype=optStartMatch&index=1&tname=%25&sc=0 [تم الاطلاع عليه في: 25 آب/أغسطس 2025].

[108] OpenCorporates (2025). CS - Circles Solutions Ltd. *OpenCorporates*. [متاح على الإنترنت] متوفر على: https://opencorporates.com/companies/cy/HE336847 [تم الاطلاع عليه في: 25 آب/أغسطس 2025].

[109] OpenCorporates (2025). CI - Compass Ltd. *OpenCorporates*. [متاح على الإنترنت] متوفر على: https://opencorporates.com/companies/cy/HE310769 [تم الاطلاع عليه في: 25 آب/أغسطس 2025].

[110] OpenCorporates (2025). Global Hubcom Ltd. *OpenCorporates*. [متاح على الإنترنت] متوفر على: https://opencorporates.com/companies/cy/HE323665 [تم الاطلاع عليه في: 25 آب/أغسطس 2025].

[111] OpenCorporates (2025). MS Magnet Solutions Ltd. *OpenCorporates*. [متاح على الإنترنت] متوفر على: https://opencorporates.com/companies/cy/HE309073 [تم الاطلاع عليه في: 25 آب/أغسطس 2025].

[112] OpenCorporates (2025ب). MI Compass Ltd. *OpenCorporates*. [متاح على الإنترنت] متوفر على: https://opencorporates.com/companies/cy/HE347278 [تم الاطلاع عليه في: 25 آب/أغسطس 2025].

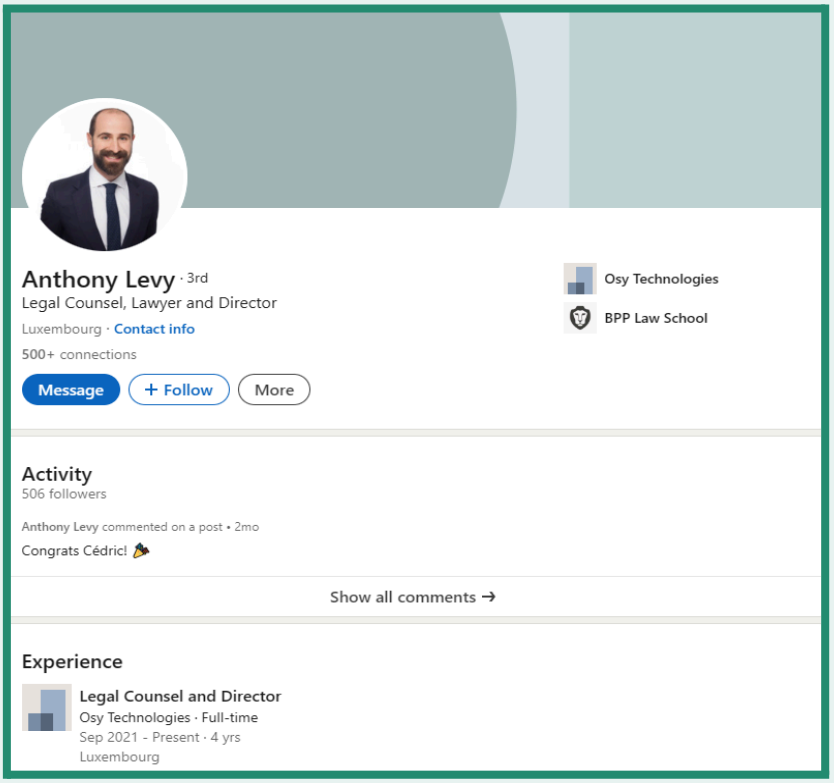
[113] جمهورية بلغاريا، وزارة العدل، هيئة السجلات (بدون تاريخ). سجل المنظمات التجارية وغير الربحية: سجل Circles Bulgaria Ltd.

[114] OpenCorporates (2025أ). Circles Bulgaria. *OpenCorporates*. [متاح على الإنترنت] متوفر على: https://opencorporates.com/companies/bg/175408771 [تم الاطلاع عليه في: 25 آب/أغسطس 2025].

- Magnet Bulgaria EOOD [115] في بلغاريا (رقم التسجيل: 203012611، مسجّلة في نيسان/أبريل 2014، وقد تمّ حلّها لاحقاً)، وهي مملوكة لشركة MS Magnet Solutions Ltd التي تتخذ من قبرص مقرّاً لها؛

تُدرج جميع الشركات الفرعية في قبرص المحامي اللوكسمبورغي أنطوني ليفي كمدير لها.[116] ويشغل ليفي حالياً أيضاً منصب المستشار القانوني لشركة OSY Technologies S.à r.l..[117] ووفقاً لمنظمة العفو الدولية، تمّ تسجيل الشركتين البلغاريتين بغرض الحصول على تراخيص تصدير من بلغاريا، غير أنّ مجموعة "إن إس أو" أوضحت في رسالة إلى المنظمة أنّ شركة Magnet Bulgaria كانت غير ناشطة في عام 2021.[118]

تمّ تنظيم ملكية مجموعة "إن إس أو" من قبل شركة "فرانسيسكو بارتنرز" عبر شركة OSY Holdings Ltd. (شركة قابضة مقرّها في جزر كايمان). كما توسّعت شبكة شركات مجموعة "إن إس أو" لتشمل ما لا يقلّ عن عشرين شركة وصندوقاً وهيكلاً قابضاً بحلول العام 2017.[119]



[115] جمهورية بلغاريا، وزارة العدل، هيئة السجلات (بدون تاريخ). سجل المنظمات التجارية وغير الربحية: سجل Magnet Bulgaria Ltd.

[116] Open Corporates. (2025). *البحث عن المسؤولين: أنطوني ليفي*. [متاح على الإنترنت] متوفر على: https://opencorporates.com/officers/cy?q=ANTHONY+LEVY&user=true [تم الاطلاع عليه في: 14 آب/أغسطس 2025].

[117] OSY Technologies S.à r.l. (2025). مستخرج من السجل التجاري. [متاح على الإنترنت] سجل التجارة والشركات في لوكسمبورغ، ص. 16، متوفر على: https://gd.lu/rcsl/85HXkB [تم الاطلاع عليه في: 14 آب/أغسطس 2025].

[118] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو" (Operating from the Shadows: inside NSO Group's Corporate Structure)* (NSO). ص.34.

[119] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو" (Operating from the Shadows: inside NSO Group's Corporate Structure)* (NSO). ص.58.

الصورة 2: يُدرج أنطوني ليفي على حسابه في "لينكد إن" صفته كمدير ومستشار قانوني لشركة OSY Technologies S.à r.l..[120]

أنطوني ليفي

مستشار قانوني ومحامٍ ومدير لوكسمبورغ. معلومات الاتصال

عدد المعارف: 500+

شركة OSY Technologies

كلية الحقوق BPP

النشاط

- 506 متابع
- آخر تعليق (منذ شهرين): "تهانينا سيدريك!"

الخبرة المهنية

مستشار قانوني ومدير

Osy Technologies – دوام كامل

أيلول/سبتمبر 2021 – حتى الآن (4 سنوات)

لوكسمبورغ

انتقال الملكية إلى شركة "نوفالبينا كابيتال" (Novalpina Capital)

في 14 شباط/فبراير 2019، استحوذت شركة "نوفالبينا كابيتال" (Novalpina Capital)، وهي شركة أسهم خاصة عالميّة، على حصة شركة "فرانسيسكو بارتنرز" في مجموعة "إن إس أو" (بما في ذلك الشركات الفرعية والشركات المرتبطة بها) لتصبح بذلك المالكة الجديدة لمجموعة "إن إس أو" وهيكلها المؤسسي.[122121] كما قامت "نوفالبينا كابيتال" بإعادة هيكلة المجموعة، وإنشاء هيكل شركات قابضة أكثر تعقيداً يمتدّ عبر بلغاريا وقبرص ولوكسمبورغ وجزر العذراء البريطانية. تجدر الإشارة إلى أنّ ملكية شركة OSY Technologies S.à r.l. انتقلت في نيسان/أبريل 2019 إلى شركة لوكسمبورغية تُدعى NorthPole Newco S.à r.l. (رقم التسجيل: B230411)، التي أصبحت لاحقاً شركة قابضة رئيسية في العام 2025.[123] في هذه المرحلة، استحوذت مجموعة "إن إس أو" على ثلاث شركات فرعية على الأقل، من بينها شركة "كونفيكسوم المحدودة" (Convexum Ltd) (رقم التسجيل: 515495554)،[124] التي تطوّر تقنيات مضادة

---

[120] ليفي، أ.. (2025) *الصفحة الشخصية لأنطوني ليفي*. [لينكد إن]. [تم الاطلاع عليه في: 14 آب/أغسطس 2025]. متوفر على: https://www.linkedin.com/in/anthony-levy-3a664522/

[121] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو" (Operating from the Shadows: inside NSO Group's Corporate Structure)* (NSO). ص.50.

[122] "نوفالبينا كابيتال" (Novalpina Capital)، استحواذ إدارة مجموعة "إن إس أو" (NSO) على الشركة (NSO Group Acquired by its Management)، 14 شباط/فبراير 2019، www.novalpina.pe/nso-group-acquired/

[123] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو" (Operating from the Shadows: inside NSO Group's Corporate Structure)* (NSO). ص.58.

[124] استحوذت مجموعة "إن إس أو" أو أصبحت المساهم الأكبر في شركة Wayout المتخصصة في تقنيات المراقبة، وشركة "كونفيكسوم " (Convexum) المزودة لتقنيات مضادة للطائرات من دون طيار في عام 2020، وشركة PFOS Technologies Ltd. البريطانية، التي تقدّم خدمات تسويقية.

للطائرات من دون طيار.[125] أمّا NorthPole Bidco S.à.r.l. (رقم التسجيل: B228505)، وهي شركة قابضة مقرّها لوكسمبورغ أدرجتها مجموعة "إن إس أو" ضمن هيكلها في العام 2018، فقد استحوذت في شباط/فبراير 2020 على شركة Goatilev Ltd. (رقم التسجيل: 516105657). وتُعدّ شركة Goalitev نفسها شركة قابضة إسرائيليّة، وقد استحوذت في العام 2020 على شركة Wayout Ltd المتخصصة في مجال تقنيات المراقبة (رقم التسجيل: 515773513).[126]

كما دفعت شركة "نوفالبينا كابيتال" مجموعة "إن إس أو" إلى تغيير معايير الحوكمة الخاصة بها، وأنشأت لجنة الحوكمة والمخاطر والامتثال لمراجعة سجلات حقوق الإنسان لدى جميع العملاء المحتملين.[127] وفي ظل إدارة "نوفالبينا كابيتال"، قدمت مجموعة "إن إس أو" سياسات جديدة للعناية الواجبة في مجال حقوق الإنسان، وبدأت تفرض إدراج بنود تتعلق بالامتثال لحقوق الإنسان في جميع عقود العملاء الجدد. ووفقاً لتقرير الشفافية والمسؤولية الصادر عن مجموعة "إن إس أو" لعام 2021، رفضت المجموعة عقوداً تجاوزت قيمتها 300 مليون دولار أميركي بعد إجراء مراجعات للعناية الواجبة في مجال حقوق الإنسان مع عملاء محتملين.[128] مع ذلك، وحتى لو كان ذلك صحيحاً، فقد صدرت تقارير قبل عامٍ ونصف تزعم أنّ الحكومة الأردنية استخدمت على الأرجح برنامج "بيغاسوس" للتجسّس على مدافعين عن حقوق الإنسان، في انتهاكٍ صارخٍ لحقوق الإنسان باستخدام منتجات مجموعة "إن إس أو".[129]

في تلك المرحلة، توسّع نطاق نشاط مجموعة "إن إس أو" ليشمل شرق آسيا أيضاً. وفي البيان المالي الصادر عن شركة CS-Circles Solutions لعام 2023، ذكرت أنها تمتلك بنسبة 100% شركة فرعية غير نشطة مقرّها هونغ كونغ، وحقّقت أرباحاً بقيمة 1,288 دولاراً أميركياً في عام 2023، وهي LI-Trade Company Limited (رقم التسجيل: 61379026).[130] وكانت LI-Trade Company Limited تُعرف سابقاً باسم World Faith Trading Limited، وتم حلّها في 10 كانون الأول/ديسمبر 2021.[131] ولا يزال دور LI-Trade Company Limited غير واضح.

---

[125] أورباش، م. (2020). مجموعة "إن إس أو" (NSO) تشتري شركة "كونفيكسوم " (Convexum) المتخصصة في التقنيات المضادة للطائرات من دون طيار. (*CTech*). NSO Buys Counter-Drone Company Convexum. [متاح على الإنترنت] 2 كانون الأول/ديسمبر. متوفر على: https://www.calcalistech.com/ctech/articles/0,7340,L-3792634,00.html [تم الاطلاع عليه في: 30 آب/أغسطس 2025]

[126] (2021 NorthPole Bidco S.à r.l.). *الميزانية العمومية: السنة المالية من 05/10/2018 إلى 31/12/2019* (*Balance Sheet: Financial Year from 10/05/2018 to 12/31/2019*.) . [متاح على الإنترنت] سجل التجارة والشركات في لوكسمبورغ، ص. 19 متوفر على: https://gd.lu/rcsl/26Qz0v [تم الاطلاع عليه في: 14 آب/أغسطس 2025]

[127] إينت فيلد، ص. (2023). *تقريرٌ بشأن التحقيق في الادعاءات المتعلّقة بالمخالفات وسوء الإدارة في تطبيق قانون الاتحاد الأوروبي في ما يخصّ استخدام برنامج "بيغاسوس" وبرامج المراقبة المماثلة للتجسس* (*REPORT of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware*). [متاح على الإنترنت] لجنة تقصي الحقائق المُكلَّفة بالتحقيق في استخدام برمجية "بيغاسوس" وبرمجيات المراقبة المماثلة للتجسس. متوفر على: https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN [تم الاطلاع عليه في: 21 آب/أغسطس 2025]

[128] مجموعة "إن إس أو" (2021 ب). *تقرير الشفافية والمسؤولية لعام 2021* (*Transparency and Responsibility Report 2021*). [متاح على الإنترنت]. ص. 20. متوفر على: https://web.archive.org/web/20250408183946/https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf [تم الاطلاع عليه في: 14 تموز/يوليو 2025]

[129] "أكسِس ناو" (2024). *بين الاختراق والمأزق: كيف يسحق برنامج "بيغاسوس" الفضاء المدني في الأردن* (*Between a hack and a hard place: how Pegasus spyware crushes civic space in Jordan*) [متاح على الإنترنت]. "أكسِس ناو". متوفر على: https://www.accessnow.org/publication/between-a-hack-and-a-hard-place-how-pegasus-spyware-crushes-civic-space-in-jordan/ [تم الاطلاع عليه في: 11 آب/أغسطس 2025]

[130] بي. إم. إيه. وشركاه محاسبون معتمدون (2023). (PMA & Co Chartered Accountants) البيانات المالية لشركة CS - Circles Solutions Limited للسنة المنتهية في 31 كانون الأول/ديسمبر 2023 (*CS - Circles Solutions Limited Financial Statements: Year Ended 31 December 2023*). ليماسول، قبرص: CS - Circles Solutions Limited

[131] حكومة منطقة هونغ كونغ الإدارية الخاصة (بدون تاريخ). سجلّ الشركات: سجل شركة LI-Trade Company [متاح على الإنترنت] متوفر على: https://www.e-services.cr.gov.hk/ICRIS3EP/system/home.do . [تم الاطلاع عليه في: 25 آب/أغسطس 2025]

بحلول العام 2020، كان هناك ما لا يقلّ عن 29 كياناً وشركةً استثماريّةً وشركةً قابضة مرتبطة بمجموعة "إن إس أو".[132] وأفادت قناة "سكاي نيوز" في 27 تموز/يوليو 2021 بأنّه كان من المقرّر تصفية شركة "نوفالبينا كابيتال" بعد خلافات داخليّة أدّت إلى نزاعٍ غير قابل للحلّ بين مديريها الثلاثة.[133] وفي العام 2021، تغيّرت ملكيّة مجموعة "إن إس أو" مجدّداً وانتقلت إلى شركة "بيركلي ريسيرتش غروب" (Berkeley Research Group)، ومقرّها كاليفورنيا.[134] وفي هذه المرحلة أُخرجت شركة OSY Holdings من الهيكل التنظيمي.[135]

قدّرت شركة "إرنست آند يونغ" (EY) قيمة مجموعة "إن إس أو" بـ2.3 مليار دولار أميركي عام 2021، لكنّ الشركة سرعان ما بدأت تتعرّض لسلسلة من الضربات الماليّة التي غيّرت مسارها بالكامل.[136] شمل ذلك تقدير قيمتها علناً بصفر دولار من قبل شركة "بيركلي ريسيرتش غروب" (Berkeley Research Group) في 2021، رغم تقدير شركة "إرنست آند يونغ" (EY)؛[137] واحتياجها إلى ضخ نقدي طارئ من شركة "بيركلي" بقيمة 10 ملايين دولار في العام ذاته؛ وكذلك إدراجها في القائمة السوداء من قبل وزارة التجارة الأميركيّة عام 2022 على خلفيّة ما تمّ كشفه عن استخدامات برنامج "بيغاسوس".[138] وبحلول نهاية عام 2021، وجّهت مجموعةٌ من دائني مجموعة "إن إس أو" رسالةً علنيّة إلى المساهمين الرئيسيّين تفيد بأنّ المجموعة كانت معسرة.[139]

ملكية "دوفرينسي هولدينغ" (Dufresne Holding) وهيكل مجموعة "إن إس أو" المحدّث

في ظل الاضطرابات المستمرة والجهود المبذولة لإعادة هيكلة مجموعة "إن إس أو"، بدأت وسائل الإعلام في آذار/مارس 2023 بالإعلان عن عودة أومري لافي، أحد المؤسّسين الثلاثة للمجموعة، ليصبح المساهم الأكبر الجديد فيها، حيث أصبحت شركته القابضة في لوكسمبورغ Dufresne Holding S.à r.l. (رقم التسجيل: B275054) مالكةً لشركة قابضة

---

[132] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو" (Operating from the Shadows: inside NSO Group's Corporate Structure)* "(NSO)". ص.58.

[133] كلاينمان، م. (2021). *تصفية شركة "نوفالبينا"، مالكة برنامج "بيغاسوس" للتجسّس، بعد الفشل في حلّ الخلافات الداخليّة. (Pegasus spyware owner Novalpina to be liquidated after failure to resolve internal bust-up.)* [متاح على الإنترنت] سكاي نيوز. متوفر على: https://news.sky.com/story/pegasus-spyware-owner-novalpina-to-be-liquidated-after-failure-to-resolve-internal-bust-up-12365638 [تم الاطلاع عليه في: 11 آب/أغسطس 2025]

[134] سريفاستافا، م.، ألياج، أورتنكا، سيفاستوبولو، ديميتري، ويغينز، ك. (2022). *معضلة السيولة النقدية لدى مجموعة "إن إس أو" (NSO): التخلف عن سداد الديون أو البيع لعملاء محفوفين بالمخاطر (NSO's cash dilemma: miss debt repayment or sell to risky customers)* [متاح على الإنترنت] فاينانشال تايمز. متوفر على: https://www.ft.com/content/5ef90e5f-1220-4ed6-a650-985272eb0334 [تم الاطلاع عليه في: 11 آب/أغسطس 2025]

[135] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو" (Operating from the Shadows: inside NSO Group's Corporate Structure)* "(NSO)". ص.49.

[136] ويغينز، ك.، سريفاستافا، م. (2018). *"إرنست ويونغ" (EY) قدّرت قيمة مجموعة "إن إس أو" بـ 2.3 مليار دولار قبل أشهر من الإنقاذ المالي الطارئ (EY valued NSO Group at $2.3bn months before emergency bailout)* [متاح على الإنترنت] فاينانشال تايمز. متوفر على: https://www.ft.com/content/057cece3-eb81-42b8-9a27-e295c61e76b3 [تم الاطلاع عليه في: 11 آب/أغسطس 2025]

[137] ويغينز، ك.، سريفاستافا، م. (2018). *"إرنست ويونغ" (EY) قدّرت قيمة مجموعة "إن إس أو" بـ 2.3 مليار دولار قبل أشهر من الإنقاذ المالي الطارئ (EY valued NSO Group at $2.3bn months before emergency bailout)*

[138] وزارة التجارة الأميركية (2021). وزارة التجارة تضيف مجموعة *"إن إس أو"* وشركات أجنبية أخرى إلى قائمة الكيانات المتورطة في أنشطة سيبرانية خبيثة(*ommerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*)

[139] ويغينز، ك.، سريفاستافا، م. (2018). *"إرنست آند يونغ" (EY) قدّرت قيمة مجموعة "إن إس أو" بـ 2.3 مليار دولار قبل أشهر من الإنقاذ المالي الطارئ (EY valued NSO Group at $2.3bn months before emergency bailout)*

في لوكسمبورغ تمتلك بدورها مجموعة "إن إس أو".[140] والجدير بالذكر أنه في 31 كانون الأول/ديسمبر 2021، أبرمت شركة NorthPole Newco S.à r.l. اتفاقية لتأجيل السداد، وبالتالي بدأت عملية نقل اتفاقيات الائتمان واتفاقيات التأجيل القائمة مسبقاً إلى شركة Dufresne Holding.[141] في 25 كانون الثاني/يناير 2022، خضعت Goatilev Ltd.، وهي الشركة القابضة التابعة لمجموعة "إن إس أو"، والشركتان الفرعيتان "كونفيكسوم" (Convexum) وWayout لإجراءات الإعسار، وبعد ذلك تم بيع شركة "كونفيكسوم" إلى Sagitta HoldCo S.à.r.l. (رقم التسجيل: B268651).[142] وفي 18 تموز/يوليو 2023، غيّرت "كونفيكسوم" اسمها إلى Sentry CS Ltd. ويبدو أنها لم تعد مرتبطة بمجموعة "إن إس أو".[143] [144]

المساهمان المباشران في مجموعة "إن إس أو" هما "كيو سايبر تكنولوجيز المحدودة" (Q Cyber Technologies Ltd.) وشركة NSO Group Technologies Ltd نفسها، إذ يسمح القانون الإسرائيلي للشركات بامتلاك أسهمها الخاصة.[145] [146] وتعود ملكيّة "كيو سايبر تكنولوجيز المحدودة" إلى كلّ من شركة OSY Technologies S.à r.l. وأومري لافي.[147] وتُظهر سجلات لوكسمبورغ لعام 2025 أنّ الكيان القانوني NorthPole Newco S.à r.l. هو المساهم الوحيد في OSY Technologies،[148] وأنّ المساهم الوحيد في NorthPole Newco S.à r.l. هو شركة Dufresne Holding.[149] ويشكّل أومري لافي وأنطوني ليفي مجلس إدارة شركة NorthPole Newco S.à r.l.، وهما مُدرجان كمقيمَين مهنياً في العنوان التالي: 44 شارع دو لا فاليه L-2661، لوكسمبورغ. كما يُعدّ أومري لافي المساهم الوحيد وعضو مجلس الإدارة الوحيد في Dufresne Holding.[150]

تُعزى التقلبات الحادّة في إيرادات مجموعة "إن إس أو" خلال العقد الماضي جزئيّاً إلى سلسلة من الفضائح والتحقيقات والتقارير التي تناولت أنشطة الشركة والاتهامات الموجّهة إلى بعض عملائها بارتكاب انتهاكات لحقوق الإنسان. وبينما

---

[140] كيرشغاسنر، س. (2023). *أحد مؤسّسي مجموعة "إن إس أو" (NSO) يَبرز بوصفه المالك الأكبر الجديد* (*NSO Group Co-founder Emerges as New Majority Owner*). [متاح على الإنترنت] الغارديان. متوفر على:
https://www.theguardian.com/technology/2023/mar/01/one-of-nso-groups-founders-emerges-as-new-majority-owner [تم الاطلاع عليه في: 11 آب/أغسطس 2025]

[141] كيرشغاسنر، س. (2023). *أحد مؤسّسي مجموعة "إن إس أو" (NSO) يَبرز بوصفه المالك الأكبر الجديد* (*NSO Group Co-founder Emerges as New Majority Owner*)

[142] (Triangle Holdings 2023). *الميزانية العمومية: السنة المالية من 01/01/2018 إلى 31/12/2021* (*Balance Sheet: Financial Year from 01/01/2021 to 12/31/2021*) . [متاح على الإنترنت] سجل التجارة والشركات في لوكسمبورغ، ص. 16. متوفر على:
https://gd.lu/rcsl/85HXkB [تم الاطلاع عليه في: 14 آب/أغسطس 2025]

[143] (Sagitta HoldCo S.à r.l. 2023). *الميزانية العمومية الموجزة: السنة المالية من 25/05/2022 إلى 31/12/2022 (Abridged Balance Sheet: Financial Year from 05/25/2022 to 12/31/2022)*. [متاح على الإنترنت] سجل التجارة والشركات في لوكسمبورغ، ص. 11. متوفر على:https://gd.lu/rcsl/1NfWvM [تم الاطلاع عليه في: 14 آب/أغسطس 2025]

[144] "سينتريكس" المتخصصة في الحلول المضادة للطائرات من دون طيار (2025). التحالفات التقنية – *شركة Sentrycs المتخصصة في الحلول المضادة للطائرات من دون طيار* (*Technological Alliances - Sentrycs Counter Drone Solutions*). [متاح على الإنترنت]. متوفر على:
https://sentrycs.com/partners/technological-alliances/. [تم الاطلاع عليه في: 22 آب/أغسطس 2025]

[145] (CheckID 2025). *NSO Group Technologies Ltd. – 514395409*. [متاح على الإنترنت] CheckID. متوفر على:
https://en.checkid.co.il/company/N.S.O.+GROUP+TECHNOLOGIES+LTD-VBo29GD-514395409 [تم الاطلاع عليه في: 28 آب/أغسطس 2025]

[146] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو" (Operating from the Shadows: inside NSO Group's Corporate Structure)* "(*NSO*)". ص.33.

[147] سلطة الشركات الإسرائيلية (2025). *معلومات عن تفاصيل الشركة: السجل الخاص بـ "كيو سايبر تكنولوجيز المحدودة" (Q Cyber Technologies) ltd*

[148] سجل التجارة والشركات في لوكسمبورغ (2025). *الملف التعريفي للشركة: السجل الخاص بـ OSY Technologies S.à r.l.*

[149] سجل التجارة والشركات في لوكسمبورغ (2025). *الملف التعريفي للشركة: السجل الخاص بـ NorthPole Newco S.à r.l.*

[150] سجل التجارة والشركات في لوكسمبورغ (2025). *الملف التعريفي للشركة: السجل الخاص بـ Dufresne Holding.*

كانت الشركة تضم نحو 350 موظفاً في نيسان/أبريل 2025، وحققت إيرادات بلغت 243 مليون دولار في العام 2020، فإنّ وضعها المالي الحالي يبدو مختلفاً تماماً.[151] فقد أظهرت سجلات المحكمة التي نُشرت في أيار/مايو 2025، في سياق الدعوى القضائية التي رفعتها شركة "واتساب"، أنّ مجموعة "إن إس أو" أفادت بتحقيق إيرادات إجمالية قدرها 95.9 مليون دولار وأرباح إجمالية قدرها 84.7 مليون دولار في العام 2023، مع خسارة تشغيلية صافية بلغت 12.7 مليون دولار.[152] وفي أيار/مايو 2025، أمر القاضي الشركة بدفع أكثر من 167 مليون دولار كتعويضات لشركة "واتساب" عن حملاتها التجسّسية التي استغلّت خدمة المراسلة.[153] ولا تزال المجموعة تواجه عدداً من الدعاوى القضائية الجارية حتى الآن.

تُقدّم سجلات الشركات في لوكسمبورغ لمحة عن الوضع المالي الحالي للمجموعة بأكملها. فقد أظهرت الملفات الماليّة لشركة NorthPole Newco S.à r.l. لعام 2024 أنّها سجّلت خسائر بلغت 79,516,731.27 دولاراً أميركياً للسنة الماليّة 2024، ما رفع إجمالي الخسائر المتراكمة المرحّلة للشركة إلى 322,449,975.86 دولاراً أميركياً. ولا تتضمّن هذه الملفات بيانات تفصيلية عن الأرباح والخسائر، ما يجعل من الصعب نسب أرقام الأرباح والخسائر إلى كيانات محدّدة داخل المجموعة. ومع ذلك، تعكس هذه الأرقام إلى حدّ ما الخسائر المجمّعة لجميع الشركات التابعة لـNorthPole Newco S.à r.l. ، بما في ذلك مجموعة "إن إس أو". كما تتوافق هذه الخسائر مع الخسائر الكبيرة التي أبلغت عنها مجموعة "إن إس أو" في قضيتها القضائية لعام 2025 ضد شركة واتساب. ووفقاً لـ"سيتيزن لاب"، هناك حالياً 27 دعوى قضائية جارية مرفوعة ضدّ مجموعة "إن إس أو" أو تؤثّر عليها في جميع أنحاء العالم.[154]

على غرار جميع الشركات الإسرائيلية التي تُصدّر "مواد دفاعية"، تخضع مبيعات مجموعة "إن إس أو" لموافقة وكالة مراقبة الصادرات الدفاعية التابعة لوزارة الدفاع الإسرائيلية، والتي يُقال إنّها تُجري تقييمات في مجال حقوق الإنسان لضمان أن تُباع منتجات مجموعة "إن إس أو" فقط للحكومات التي تستخدمها لأغراض "مشروعة".[155] علاوة على ذلك، تدّعي المجموعة أنّها تخضع لنظام رقابي متعدد الطبقات، يفرض على العملاء توقيع شهادات المستخدم النهائي التي يُفترض أنّها تُلزمهم بالامتثال للقانون الدولي. كما يدّعي فريق الامتثال في المجموعة أنّه يُجري تقييماً لكلّ عميل حكومي محتمل استناداً إلى مصفوفة المخاطر المتعلقة بحقوق الإنسان، وإذا حصل بلد ما على درجة منخفضة جداً، فإنّ الشركة لا تتابع

---

[151] قضية شركة *"واتساب"* ضد مجموعة "إن إس أو" (2025) *(WhatsApp Inc. v. NSO Group Technologies Limited)*. (محكمة المقاطعة، المنطقة الشمالية في كاليفورنيا). متوفر على:
https://www.courtlistener.com/docket/16395340/747/3/whatsapp-inc-v-nso-group-technologies-limited/ [تم الاطلاع عليه في: 10 تموز/يوليو 2025].

[152] قضية شركة *"واتساب"* ضد مجموعة "إن إس أو" (2025) *(WhatsApp Inc. v. NSO Group Technologies Limited)*. (محكمة المقاطعة، المنطقة الشمالية في كاليفورنيا). متوفر على:
https://www.courtlistener.com/docket/16395340/758/2/whatsapp-inc-v-nso-group-technologies-limited/ [تم الاطلاع عليه في: 27 تموز/يوليو 2025].

[153] فرانشيسكي-بيكيراي، ل.، (2025). *مجموعة "إن إس أو" مطالبة بدفع أكثر من 167 مليون دولار كتعويضات لشركة "واتساب" عن حملات التجسّس (NSO Group Must Pay More than $167 Million in Damages to WhatsApp for Spyware Campaign)*. *TechCrunch*. [متاح على الإنترنت]. متوفر على:
https://techcrunch.com/2025/05/06/nso-group-must-pay-more-than-167-million-in-damages-to-whatsapp-for-spyware-campaign/ [تم الاطلاع عليه في: 9 أيار/مايو 2025].

[154] سيبينا أنستيس (2018). *التقاضي والشكاوى الرسمية الأخرى المتعلقة ببرمجيات التجسّس التجارية* (Litigation and other formal complaints related to mercenary spyware) - "سيتيزن لاب" (Citizen Lab). [متاح على الإنترنت]. "سيتيزن لاب" (Citizen Lab). متوفر على:
https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/ [تم الاطلاع عليه في: 14 حزيران/يونيو 2025].

[155] مجموعة "إن إس أو" (2024). *تقرير الشفافية والمسؤولية لعام 2024 (Transparency and Responsibility Report 2024)*. [متاح على الإنترنت]. ص.4. متوفر على:
https://web.archive.org/web/20250518154902/https://www.nsogroup.com/wp-content/uploads/2025/02/2024-Transparency-and-Responsibility-Report.pdf [تم الاطلاع عليه في: 25 حزيران/يونيو 2025]

فرصة التعاون معه. وقد أدّى هذا النهج إلى خفض عدد الدول التي تتعامل معها المجموعة إلى 31 دولة بحلول العام 2024.[156]

في العام 2021، حدّدت مجموعة "إن إس أو" كلّاً من بلغاريا وقبرص وإسرائيل كدول تصدّر منها منتجاتها، على ما يبدو بعد الحصول على التراخيص اللازمة.[157] وقد اعترفت الشركة فقط بتصدير برنامج "بيغاسوس" من إسرائيل. وفي حين حصلت شركات تابعة للمجموعة على تراخيص تصدير من قبرص وبلغاريا، لا يوجد دليل على أنّ برنامج "بيغاسوس" تحديداً (على عكس منتجات أخرى) قد تمّ تصديره من الكيانات الموجودة في هاتين الدولتين.[158] وردّاً على الرسائل التي أرسلها مرصد الأعمال وحقوق الإنسان في العام 2019، نفت السلطات في كلٍّ من قبرص وبلغاريا منح تراخيص تصدير لمجموعة "إن إس أو"، ويبدو أنّ هذا النفي يتعارض مع ما زعمته الشركة نفسها في العام 2021، ومع السجلات الرسمية لتراخيص التصدير المتاحة على الإنترنت في حالة بلغاريا.[159] [160] وفي تقرير الشفافية والمسؤولية الصادر عن مجموعة "إن إس أو" لعام 2024، أشارت الشركة فقط إلى بلغاريا، من دون ذكر قبرص، كدولة تخضع فيها لأنظمة تنظيمية تتعلق بالتصدير.[161]وفي نهاية المطاف، يُنظر إلى حضور مجموعة "إن إس أو" في منطقة غرب آسيا وشمال أفريقيا على أنه مرتبط بإسرائيل وجيشها. وتشير مجموعة البيانات الخاصة بهذا التقرير، والمستندة إلى مصادر علنية، إلى أنّ ما لا يقلّ عن 12 دولة في المنطقة استخدمت برنامج "بيغاسوس"، في حين تعقّب مختبر "سيتيزن لاب" حالات يُشتبه بأنها إصابات ببرنامج "بيغاسوس" في 17 دولة ضمن المنطقة نفسها.[162]

---

[156] مجموعة "إن إس أو" (2024). *تقرير الشفافية والمسؤولية لعام 2024* (*Transparency and Responsibility Report 2024*). ص.12.

[157] مجموعة "إن إس أو" (2024ب). *تقرير الشفافية والمسؤولية لعام 2021* (*Transparency and Responsibility Report 2021*). [متاح على الإنترنت]. ص.4. متوفر على:
https://web.archive.org/web/20250408183946/https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf [تم الاطلاع عليه في: 14 تموز/يوليو 2025]

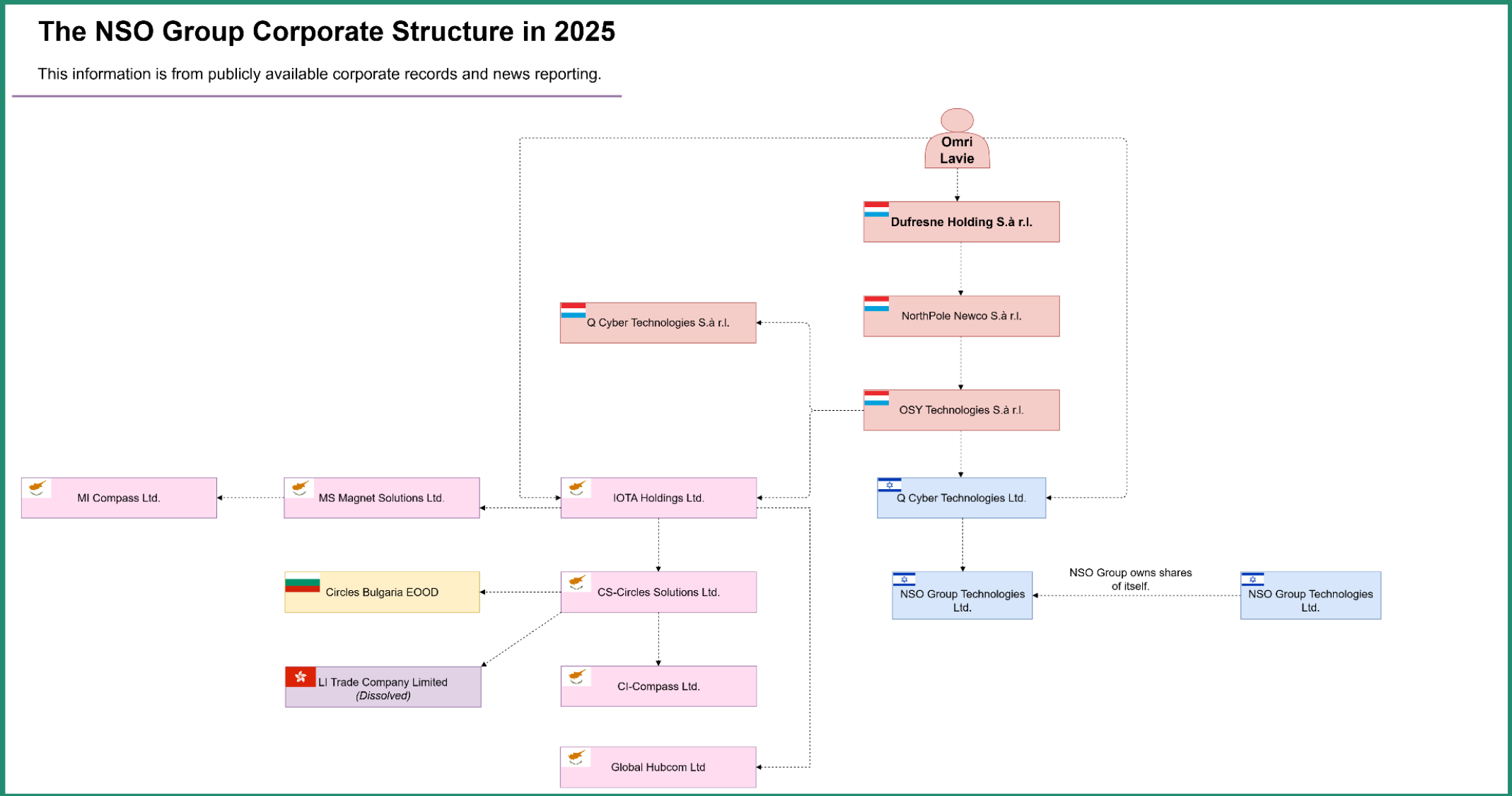
[158] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو"* (*Operating from the Shadows: inside NSO Group's Corporate Structure*) (*NSO*). ص.82-85.

[159] منظمة العفو الدولية، ومنظمة الخصوصية الدولية (Privacy International)، ومركز أبحاث الشركات متعددة الجنسية (2021). *العمل في الخفاء: داخل الهيكل المؤسسي لمجموعة "إن إس أو"* (*Operating from the Shadows: inside NSO Group's Corporate Structure*) (*NSO*). ص.34.

[160] مرصد الأعمال وحقوق الإنسان (2025). *"نوفالبينا كابيتال" (Novalpina Capital) تزعم أنّ مجموعة "إن إس أو" حصلت على تراخيص تصدير من بلغاريا وقبرص، لكنّ الدولتين تنفيان هذه المزاعم - مرصد الأعمال وحقوق الإنسان* (*Novalpina Capital Claims NSO Group Received Export Licences from Bulgaria & Cyprus, but Both States Deny Claims - Business & Human Rights Resource Centre*) [متاح على الإنترنت]. مرصد الأعمال وحقوق الإنسان. متوفر على:
https://www.business-humanrights.org/en/latest-news/novalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/ [تم الاطلاع عليه في: 29 أيلول/سبتمبر 2025]

[161] مجموعة "إن إس أو" (2024). تقرير الشفافية والمسؤولية لعام 2024 (Transparency and Responsibility Report 2024).

[162] ماركزاك، ب.، سكوت-رايلتون، ج.، ماككون، س.، عبد الرزاق، ب.، ديبرت، ر. (2018). *لعبة الغمّيضة* (*HIDE AND SEEK*)



الصورة 3: الهيكل التنظيمي لمجموعة "إن إس أو" لعام 2015.

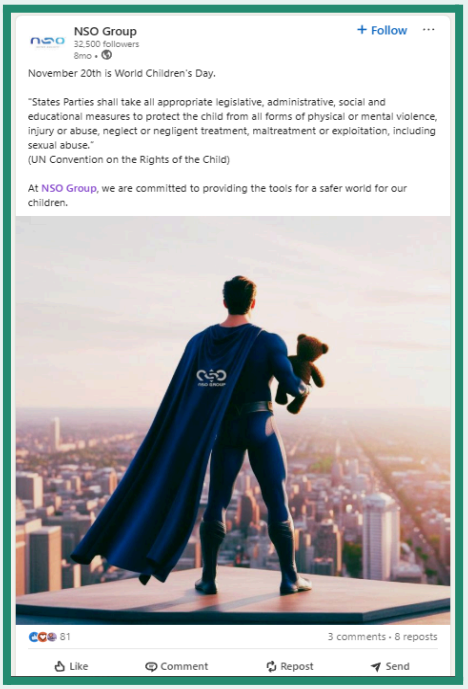
الهيكل التنظيمي لمجموعة "إن إس أو" لعام *2015* هذه المعلومات مستقاة من سجلات الشركة المتاحة للعامة والتقارير الإخبارية.	
أومري لافي	Omri Lavie
Dufresne Holding S.à r.l.	● Dufresne Holding S.à r.l
NorthPole Newco S.à r.l.	o NorthPole Newco S.à r.l.
OSY Technologies S.à r.l.	o OSY Technologies S.à r.l.
"كيو سايبر تكنولوجيز ش.م.م." *(Q Cyber Technologies S.à r.l)*	o Q Cyber Technologies S.à r.l.
"كيو سايبر تكنولوجيز ش.م.م." *(Q Cyber Technologies S.à r.l)*	▪ Q Cyber Technologies Ltd.
NSO Group Technologies Ltd.	▪ NSO Group Technologies Ltd.
تمتلك مجموعة "إن إس أو" جزءاً من أسهمها الخاصة.	▪ *NSO Group owns shares of itself.*
IOTA Holdings Ltd.	● IOTA Holdings Ltd.
MI Compass Ltd.	o MI Compass Ltd.
MS Magnet Solutions Ltd.	o MS Magnet Solutions Ltd.
CS-Circles Solutions Ltd.	o CS-Circles Solutions Ltd.
CI-Compass Ltd.	o CI-Compass Ltd.
Global Hubcom Ltd.	o Global Hubcom Ltd.
Circles Bulgaria EOOD	o Circles Bulgaria EOOD
LI Trade Company Limited *(تمت تصفيتها)*	LI Trade Company Limited ((Dissolved

التسويق: "ضروري ومشروع"

على غرار عدد كبير من بائعي برامج التجسّس التجارية، تقوم استراتيجيات التسويق لدى مجموعة "إن إس أو" على تعزيز عنصري الضرورة والشرعية لمنتجاتها. وتزعم المجموعة على موقعها الإلكتروني أن مهمّتها هي تطوير "تقنيات استخبارات سيبرانية أخلاقية ومبتكرة تمكّن الوكالات الحكومية من منع الجرائم والإرهاب والتحقيق فيهما".[163] كما تؤكد التزامها بأربع قيم أساسية هي: المساءلة، والجرأة، والتميّز، والنزاهة، وتُشير إلى أن منتجاتها تُستخدم حصرياً من قِبل وكالات إنفاذ القانون ووكالات الاستخبارات.

[163] مجموعة "إن إس أو" (2021 أ). من نحن. [متاح على الإنترنت] Nsogroup.com. متوفر على: https://web.archive.org/web/20250701175532/https://www.nsogroup.com/about-us/ [تم الاطلاع عليه في: 3 آب/أغسطس 2025].

كما أوضح الباحثان إلينور كارمي ودان كوتليار في العام 2024، تعتمد مجموعة "إن إس أو" على أربع استراتيجيات لإضفاء الشرعية على منتجاتها، وهي: الأمننة، وادعاء الامتثال للمعايير الأخلاقية، والتطبيع، والوطنية الصهيونية.[164] وتقدّم منشورات المجموعة على وسائل التواصل الاجتماعي لمحة عن هذه الأساليب الأربعة. فعلى سبيل المثال، تنشر المجموعة بشكل متكرّر على منصة "لينكد إن" محتوى يتناول أهمية حقوق الإنسان. وفي 20 تشرين الثاني/نوفمبر 2024، نشرت المجموعة منشوراً بمناسبة اليوم العالمي للطفل، تضمّن اقتباساً من اتفاقية الأمم المتحدة لحقوق الطفل، مرفقاً بصورة بطل خارق يلبس رداءً يحمل شعار المجموعة، يقف على سطح مبنى وهو يحمل دمية دب.[165]



الصورة 4: منشور تسويقي لمجموعة "إن إس أو" على منصة "لينكد إن".

مجموعة "إن إس أو"

32,000 متابع

20 تشرين الثاني/نوفمبر: اليوم العالمي للطفل

"تتخذ الدول الأطراف جميع التدابير التشريعية والإدارية والاجتماعية والتعليمية الملائمة لحماية الطفل من كافة أشكال العنف أو الضرر أو الإساءة البدنية أو العقلية والإهمال أو المعاملة المنطوية على إهمال، وإساءة المعاملة أو الاستغلال، بما في ذلك الإساءة الجنسية". *(اتفاقية الأمم المتحدة لحقوق الطفل)*

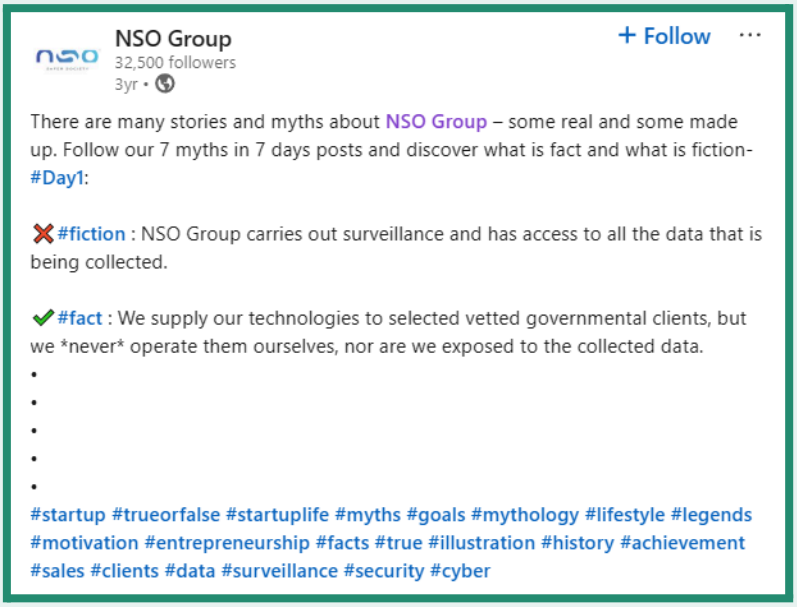
في مجموعة "إن إس أو"، نلتزم بتوفير الأدوات التي تساهم في جعل عالم أطفالنا أكثر أماناً.

---

[164] كوتليار، د. م.، كارمي، إ. (2023). الحفاظ على جهوزية "بيغاسوس": إضفاء الشرعية على التجسّس الإلكتروني. (Keeping Pegasus on the wing: legitimizing cyber espionage). مجلة Information, Communication & Society، ص. 1-31 doi:https://doi.org/10.1080/1369118x.2023.2245873

[165] مجموعة "إن إس أو" (2024). *20 تشرين الثاني/نوفمبر: اليوم العالمي للطفل* (*November 20th is World Children's Day*) [لينكد إن]، تشرين الثاني/نوفمبر 2024. متوفر على: https://www.linkedin.com/posts/nso-group_november-20th-is-world-childrens-day-activity-7264944950981578754-WtHN/ [تم الاطلاع عليه في: 28 آب/أغسطس 2025].

في كانون الثاني/يناير 2022، نشرت مجموعة "إن إس أو" سلسلةً من المنشورات على منصّة "لينكد إن" بعنوان "مفنِّد الخرافات"، حاولت من خلالها تفنيد الشائعات المتعلّقة بمنتجاتها. نشرت المجموعة في أول منشور لها:



الصورة 5: محاولة مجموعة "إن إس أو" نفي الشائعات حول منتجاتها.[166]

مجموعة "إن إس أو" 32,500 متابع 3 سنوات +متابعة	NSO Group 32,500 followers 3yr + Follow
تُحاك قصصٌ وخرافاتٌ حول مجموعة "إن إس أو"، بعضها صحيحٌ وبعضها مُختلق. لذا، تابعوا سلسلة منشوراتنا "7 خرافات في 7 أيام"، واكتشفوا الحقيقة من الخيال. #اليوم1 #خيال: تمارس مجموعة "إن إس أو" عمليات المراقبة وتتمتّع بصلاحية الاطّلاع على كافّة المعلومات التي يجري جمعها. #حقيقة: نحن نزوّد تقنياتنا فقط لجهاتٍ حكوميةٍ مختارة بعد التدقيق، لكننا لا نُشغّلها بأنفسنا*مطلقاً*، ولا نطّلع على أيٍّ من البيانات المُجمّعة.	There are many stories and myths about NSO Group - some real and some made up. Follow our 7 myths in 7 days posts and discover what is fact and what is fiction #Day1: X#fiction: NSO Group carries out surveillance and has access to all the data that is being collected. #fact: We supply our technologies to selected vetted governmental clients, but we never operate them ourselves, nor are we exposed to the collected data.
#شركة_ناشئة #صح_أم_خطأ #حياة_الشركات_الناشئة #خرافة #أهداف #أساطير #أسلوب_حياة #حكايات #تحفيز #ريادة_أعمال #حقائق #صحيح #توضيح #تاريخ #إنجاز #مبيعات #عملاء #بيانات #مراقبة #أمن #سيبراني	#startup #trueorfalse #startuplife #myths #goals #mythology #lifestyle #legends #motivation #entrepreneurship #facts #true #illustration

[166] مجموعة "إن إس أو". (2024). *مفنِّد الخرافات! (Myth Blasters!)* [لينكد إن]، كانون الثاني/يناير 2022. متوفر على: https://www.linkedin.com/posts/nso-group_myth-blasters-day-6-activity-6889607776767635456-Y8v6/ [تم الاطلاع عليه في 25 آب/أغسطس 2025].

#history achievement #sales #clients #data #surveillance #security #cyber	

تصف مجموعة "إن إس أو" منتجاتها باستمرارٍ بأنّها ضرورية ومشروعة نظراً لاستخدامها في القبض على "المتحرّشين بالأطفال" و"المجرمين"، كما صرّح المؤسّس شاليف خوليو في مقابلة مع صحيفة "واشنطن بوست" عام 2021.[167] ويشير كارمي وكوتليار (2023) إلى أنّ مجموعة "إن إس أو" تميل أيضاً إلى وصف منتجاتها بعباراتٍ غامضةٍ ومحايدةٍ مثل "تكنولوجيا".[168] ووفقاً لهذا المنطق التسويقي، لا يمكن تحميل الشركة مسؤولية أفعال عملائها، فهي تزعم التدقيق في خلفيات جميع العملاء للتحقّق من عدم تورّطهم في أيّ انتهاكات محتملة لحقوق الإنسان، وأنّها تبيع تكنولوجيا مشروعة لعملاء شرعيين يحاربون الجريمة والإرهاب حصراً، كما أنّها لا تمتلك صلاحية الوصول إلى ما يقوم به عملاؤها. بعبارة أخرى: الأخيار يزوّدون الأخيار بتكنولوجيا جيدة.

ويشير كارمي وكوتليار (2023) إلى أنّ حضور الشركة الإعلامي على وسائل التواصل الاجتماعي يسعى إلى تطبيع صورتها عبر النشر حصرياً باللغة الإنكليزية، ومشاركة التهنئة في الأعياد وصور الموظفين في الحفلات والمؤتمرات، وحتى الاحتفال بالتنوّع (مثل مشاركة منشور على "لينكد إن" للاحتفاء بشهر الفخر).[169] وتحاول مجموعة "إن إس أو" أيضاً تطبيع صورتها عبر تسويق منتجاتٍ أخرى غير برامج التجسّس. فقد أشار الباحثان إلى أنّ نحو 20% من منشورات الشركة في العام 2020 تركّزت حول تكنولوجيا مضادّة للطائرات المسيّرة طوّرتها بعد شراء شركة "كونفيكسوم" (Convexum). كما اتّجهت الشركة إلى تسويق منتجات تتعلّق بتعقّب مخالطي مرضى كوفيد-19، وتحليل البيانات، ومكافحة غسل الأموال عن طريق العملات المشفّرة.[170] [171] وفي محاولةٍ لإضفاء طابعٍ إنساني على موظفيها، أطلقت مجموعة "إن إس أو" عدّة حملاتٍ على وسائل التواصل الاجتماعي لتسليط الضوء على موظفيها وحياتهم، ومن ضمن هذه الحملات حملة "أنا إن إس أو" (IAMNSO) عام 2021.[172]

لكن هذا لا يعني ابتعادها عن منتجها الأساسي. ففي حزيران/يونيو 2025، نشرت مجموعة "إن إس أو" صوراً من احتفالها بالذكرى الخامسة عشرة لتأسيسها في براغ، بما في ذلك قالب حلوى يعلوه حصان مجنّح، في إشارة إلى مجموعة برامج التجسّس سيّئة السمعة التي تطوّره الشركة.[173]

---

[167] دووسكين، إي. وروبين، س. (2021). "على أحدهم القيام بالعمل القذر": مؤسسو "إن إس أو" يدافعون عن برنامج التجسس الذي طوّروه. ('Somebody has to do the dirty work': NSO Founders Defend the Spyware They Built.) *واشنطن بوست*. [متاح على الإنترنت] 21 تموز/يوليو. متوفر على: https://www.washingtonpost.com/world/2021/07/21/shalev-hulio-nso-surveillance/ [تم الاطلاع عليه في 22 أيار/مايو 2025].

[168] كوتليار، د.م. وكارمي، إي. (2023). استمرار عمل "بيغاسوس": إضفاء الشرعية على التجسس الإلكتروني. (Keeping Pegasus on the wing: legitimizing cyber espionage)

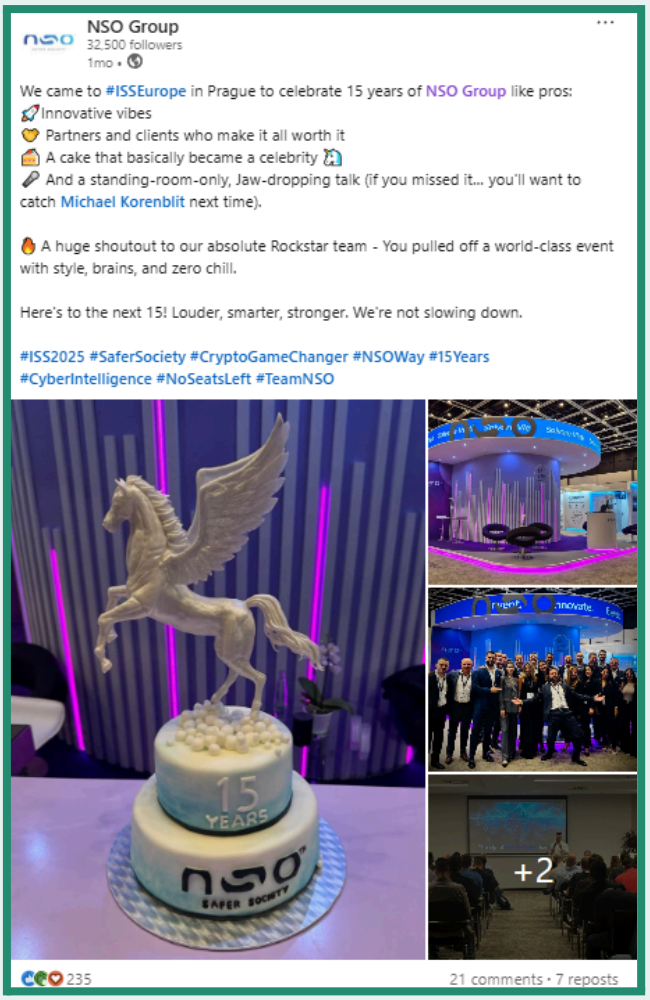
[169] كوتليار، د.م. وكارمي، إي. (2023). استمرار عمل "بيغاسوس": إضفاء الشرعية على التجسس الإلكتروني. (Keeping Pegasus on the wing: legitimizing cyber espionage)

[170] كوتليار، د.م. وكارمي، إي. (2023). استمرار عمل "بيغاسوس": إضفاء الشرعية على التجسس الإلكتروني. (Keeping Pegasus on the wing: legitimizing cyber espionage)

[171] مجموعة "إن إس أو". (2025). *العملات المشفّرة غير المشروعة هي محرّك الجريمة والإرهاب العالميَّيْن*. (*Illicit crypto is the engine of global crime and terrorism*.) [لينكد إن]، أيار/مايو 2025. متوفر على: https://linkedin.com/posts/nso-group_nsogroup-actionableintel-illicitcrypto-activity-7330597266652655616--v_0/?rcm=ACoAABeY6zUBgiQBDJC-OlTmvQ_cJOLPk7ztqDE [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[172] كوتليار، د.م. وكارمي، إي. (2023). استمرار عمل بيغاسوس: إضفاء الشرعية على التجسس الإلكتروني. (Keeping Pegasus on the wing: legitimizing cyber espionage.)

[173] مجموعة "إن إس أو". (2025). *مرور 15 عاماً على تأسيس مجموعة "إن إس أو"*. (*15 years of NSO Group*) [لينكد إن]، حزيران/يونيو 2025. متوفر على: https://www.linkedin.com/posts/nso-group_isseurope-iss2025-safersociety-activity-7336407248438464512-zNNs



الصورة 6: مجموعة "إن إس أو" تشارك قالب حلوى يعلوه بيغاسوس في احتفالها بالذكرى الخامسة عشرة في براغ

NSO Group 32,500 followers 1mo	مجموعة "إن إس أو" 32,500 متابع شهر
We came to #ISSEurope in Prague to celebrate 15 years of NSO Group like pros: Innovative vibes Partners and clients who make it all worth it A cake that basically became a celebrity	حضرنا مؤتمر "آي إس إس" أوروبا (#ISSEurope) في براغ للاحتفال بمرور 15 عاماً على تأسيس مجموعة "إن إس أو" كالمحترفين: أجواء مبتكرة شركاء وعملاء يجعلون كل شيء يستحق العناء قالب حلوى أصبح مشهوراً ومحاضرة مكتظّة أذهلت الحضور (وإن فاتكم حضورها... فلا تفوّتوا مايكل كورنبليت في المرّة القادمة).

?utm_source=share&utm_medium=member_desktop&rcm=ACoAABeY6zUBgiQBDJC-OlTmvQ_cJOLPk7ztqDE

]تم الاطلاع عليه في 25 آب/أغسطس 2025[.

And a standing-room-only, Jaw-dropping talk (if you missed it... you'll want to catch Michael Korenblit next time). A huge shoutout to our absolute Rockstar team - You pulled off a world-class event with style, brains, and zero chill. Here's to the next 15! Louder, smarter, stronger. We're not slowing down.	تحية كبيرة إلى فريقنا المذهل، لقد أنجزتم حدثاً عالمياً بأسلوبٍ وأناقةٍ وذكاء، وبلا أيّ تهاون. لنحتفل بالـ15 عاماً القادمة! بصوتٍ أعلى، وعقلٍ أكثر ذكاءً، وقوةٍ أكبر. لن نتوقّف.
#ISS2025#SaferSociety#CryptoGameChanger#NSOWay#15Years#CyberIntelligence#NoSeatsLeft#TeamNSO	#آي_إس_إس #مجتمع_أكثر_أمناً #تغيير_قواعد_اللعبة_الرقمية #أسلوب "إن إس أو" #15عاماً #الاستخبارات_السيبرانية #لا_مقاعد_شاغرة #فريق "إن إس أو"

تحرص مجموعة "إن إس أو" على تسويق منتجاتها من خلال المشاركة في مؤتمرات أمنية دولية أو تمويلها، مثل معرض الأمن والشرطة عام 2020، والندوة الثالثة للأمن الدولي، أو الدورات المختلفة لمؤتمر "آي إس إس العالمي" (ISS World). كما كانت المجموعة الراعي الرئيسي لمؤتمر "آي إس إس العالمي أوروبا" (ISS World Europe) في العام 2025.[174] [175]

وفي مجال التسويق، تظهر الشركة بوضوحٍ ارتباط هويتها المؤسّسية بعناصر قوية من القومية الصهيونية. فعلى سبيل المثال، ساهمت في نيسان/أبريل 2021 بتنظيم احتفالٍ بمناسبة "عيد استقلال إسرائيل"، وفي اليوم العالمي لإحياء ذكرى الهولوكوست، شاركت على "لينكد إن" منشوراً تصف فيه نفسها بأنّها شركة "إسرائيلية وصهيونية فخورة". وعندما واجهت انتقادات شديدة في العام 2021 على خلفية نشر المنظمة غير الربحية "قصص محظورة" (Forbidden Stories) تحقيقاً صادماً يتعلّق بتسريب 50,000 رقم هاتف استُهدف ببرنامج "بيغاسوس"، زعم خوليو، المدير التنفيذي آنذاك، أنّ الانتقادات مرتبطة بهوية الشركة الإسرائيلية أكثر من ارتباطها ببرنامج التجسّس نفسه.[176]

ولا تتوانى مجموعة "إن إس أو" عن الدخول في سجالات مع مسؤولين دوليّين، وخاصةً بعد اتّهاماتٍ طالتها بانتهاك حقوق الإنسان. فعلى سبيل المثال، بعد أن وجّهت فرانشيسكا ألبانيزي، المقرّرة الخاصة بالأمم المتحدة المعنية بحالة حقوق الإنسان في الأراضي الفلسطينية المحتلة منذ 1967، اتّهاماً للشركة بالتواطؤ في "اقتصاد الإبادة الجماعية" عقب أحداث 7 تشرين الأول/أكتوبر، صرّح المدير التنفيذي يارون شوهات بأنّ تقاريرها لا تُعد سوى "انحرافٍ أخلاقيٍّ" وتنطوي على "معاداة السامية".[177] [178] واستند شوهات إلى ذرائع مضلّلة، حيث زعم أنّ الأمم المتحدة وألبانيزي التزما الصمت حيال "الاغتصاب والتعذيب والخطف والمجازر التي ارتُكبت بحقّ المدنيين الإسرائيليّين في 7 تشرين الأول/أكتوبر". وبهذا، تسعى مجموعة "إن إس أو" إلى ربط صورتها ومنتجاتها بشكلٍ وثيقٍ بمفهوم "الأخلاق" وبنزعةٍ قوميةٍ متعاليةٍ يرفضها منتقدوها.

---

[174] مجموعة "إن إس أو". (2021). *أرشيف المؤتمرات – مجموعة "إن إس أو"*. (*Conferences Archive - NSO Group*) [متاح على الإنترنت] متوفر على: https://web.archive.org/web/20250619091830/https://www.nsogroup.com/conferences/ [تم الاطلاع عليه في 2 تموز/يوليو 2025].

[175] "آي. إس. إس. وورلد ترينينغ" (ISS World Training). (2025). *آي. إس. إس. وورلد أوروبا- الرعاة*. (*ISS World Europe – Sponsors*) [متاح على الإنترنت] متوفر على: https://www.issworldtraining.com/ISS_EUROPE/sponsors.html [تم الاطلاع عليه في 2 تموز/يوليو 2025].

[176] كوتليار، د.م. وكارمي، إي. (2023). استمرار عمل "بيغاسوس": إضفاء الشرعية على التجسس الإلكتروني. (Keeping Pegasus on the wing legitimizing cyber espionage).

[177] مجموعة "إن إس أو". عندما نتعرّض لاتهاماتٍ باطلة، فالسكوت حيالها ليس خياراً! (*When faced with unfounded accusations, silence is not an option!*) [لينكد إن]، حزيران/يونيو 2025. متوفر على: https://www.linkedin.com/posts/yarons_un-nso-letters-ugcPost-7338833305217253376-Z-7i/ [تم الاطلاع عليه في 2 آب/أغسطس 2025].

[178] ألبانيزي، ف. (2025). *من اقتصاد الاحتلال إلى اقتصاد الإبادة الجماعية*. [متاح على الإنترنت] مجلس حقوق الإنسان التابع للأمم المتحدة. متوفر على: https://docs.un.org/ar/A/HRC/59/23 [تم الاطلاع عليه في 2 آب/أغسطس 2025].

المنتج الأبرز: "بيغاسوس" (Pegasus)

يُعتبر برنامج التجسّس "بيغاسوس" المنتج الأبرز لمجموعة "إن إس أو"، وهو برنامج مطوّر بهدف التجسّس. ويُعدّ "بيغاسوس" برمجية خبيثة للمراقبة تعمل بدون أي نقرة، فلا تحتاج الضحية إلى الضغط على رابطٍ أو التفاعل مع المهاجم ليُخترق جهازها.[179] ومع ذلك، يمكن نشر "بيغاسوس" أيضاً من خلال نقرة واحدة أو عبر تثبيته مادياً عبر الجهاز.[180] وتشير إفادة قدّمها يارون شوهات، المدير التنفيذي لمجموعة "إن إس أو"، أمام المحكمة مؤخراً، إلى الطريقة التي تُصوِّر بها الشركة منتجها:

"تشمل منتجات "إن إس أو" مجموعة من التقنيات والوظائف المختلفة التي تُسوَّق وتُعرف مجتمعةً باسم بيغاسوس".[181]

وتصف المجموعة "بيغاسوس" بأنّه "نظام مراقبة موجّه"، مؤكدةً أنّ نطاقه يقتصر على استهداف أجهزة فردية. وكما أوضحت الشركة في تقريرها حول الشفافية والمسؤولية لعام 2024، فإنّ "بيغاسوس":

> "... نظام مراقبة موجّه، مصمَّم للتحميل على جهازٍ محمولٍ واحد فقط، مع تراخيص محدودة للغاية، ويخضع استخدامه لقيودٍ قانونيةٍ شاملةٍ ضمن الإطار القانوني الخاص بكلّ عميل... نحن لا نُشغّل بيغاسوس ولا نشارك في التحقيقات التي تُجريها أجهزة إنفاذ القانون، فنحن لا نصل إلى البيانات المُجمَّعة، ولا نعلم هويّة الأشخاص المستهدفين بالتحقيق."

> *" [إنّه] أشبه بالتنصّت التقليدي على الاتصالات الهاتفية... لكنّه مُكيّف مع حالات الاستخدام في العصر الحديث... [وهو] ليس أداة مراقبة جماعية".*[182]

> *"يتيح [بيغاسوس] لأجهزة إنفاذ القانون أداء مهامها، مع الالتزام بالقوانين المحلية والمعايير الدولية لحقوق الإنسان".*[183]

وبهذا الشكل، تسعى مجموعة "إن إس أو" إلى التنصّل من أيّ مسؤولية تتعلّق بـ"بيغاسوس" وبمستخدميه.

أما تسعير برنامج "بيغاسوس" فيعتمد على نوع المنتج المستخدم، والقدرات المحددة (وعدد القدرات المطلوبة)، إضافةً إلى عدد التراخيص المطلوبة. في العام 2016، أفادت صحيفة "نيويورك تايمز" بأنّ مجموعة "إن إس أو" تحدّد أسعار

---

[179] فاريير، إ. (2022). *ما هو برنامج التجسس "بيغاسوس" وهل اخترق هاتفك؟ (What Is Pegasus Spyware and Is Your Phone Infected with Pegasus?* [online] What Is Pegasus Spyware and Is Your Phone Infected with Pegasus?) [متاح على الإنترنت] ما هو برنامج التجسس "بيغاسوس" وهل اخترق هاتفك؟ متوفر على: https://www.avast.com/c-pegasus-spyware [تم الاطلاع عليه في 11 آب/أغسطس 2025].

[180] زيتر، ك. (2021). *برنامج "بيغاسوس" للتجسس: كيف يعمل وما يجمعه.(Pegasus Spyware: How It Works and What It Collects.*) [متاح على الإنترنت] زيرو داي (ZERO DAY). متوفر على: https://www.zetter-zeroday.com/pegasus-spyware-how-it-works-and/ [تم الاطلاع عليه في 11 آب/أغسطس 2025].

[181] شركة *"واتساب" ضد مجموعة "إن إس أو" المحدودة (WhatsApp Inc. v. NSO Group Technologies Limited)* [2025] ج. (محكمة المقاطعة، المنطقة الشمالية من كاليفورنيا). متوفر على: https://www.courtlistener.com/docket/16395340/760/1/whatsapp-inc-v-nso-group-technologies-limited/ [تم الاطلاع عليه في 27 آب/أغسطس 2025].

[182] مجموعة "إن إس أو" (2024). *تقرير الشفافية والمسؤولية لعام 2024، (Transparency and Responsibility Report 2024*) [متاح على الإنترنت]، ص6 متوفر على: https://web.archive.org/web/20250518154902/https://www.nsogroup.com/wp-content/uploads/2025/02/2024-Transparency-and-Responsibility-Report.pdf [تم الاطلاع عليه في 25 حزيران/يونيو 2025].

[183] مجموعة "إن إس أو" (2024). *تقرير الشفافية والمسؤولية لعام 2024،(Transparency and Responsibility Report 2024)* ص7.

الوصول إلى برنامج التجسّس وفقاً لعدد الأهداف المطلوب اختراقها.[184] فمثلاً، من أجل "الوصول غير المحدود إلى أجهزة الهاتف المحمول الخاصة بالهدف"، تقاضت الشركة في العام 2016 رسوماً بلغت 500,000 $ مقابل تحميل البرنامج، و650,000$ مقابل 10 مستخدمي "آيفون" أو "أندرويد"، و800,000$ مقابل 100 هدف إضافي، و500,000$ مقابل 50 هدفاً إضافياً، و250,000$ مقابل 20 هدفاً إضافياً، بالإضافة إلى 150,000$ مقابل 10 أهداف إضافية. كما تفرض الشركة رسوم صيانة سنوية للمنتج تعادل 17% من القيمة الإجمالية سنوياً بعد السنة الأولى.[185]

أما في الفترة الأخيرة، ووفقاً لشهادة قضائية في قضية "واتساب" ضد مجموعة "إن إس أو"، فقد تراوحت الأسعار في معظم الحالات بين مليون دولار و10 ملايين دولار مقابل ترخيص واحد لاختراق جهاز محمول. كما أنّ استهداف هواتف خارج بلدان العملاء كان يكلّف مبلغاً إضافياً قدره مليون دولار.[186] وتفرض الشركة أيضاً رسوماً إضافية على ما يُعرف بخدمات "Upsell"، أي العناصر المضافة إلى قدرات البرنامج الأساسية. وتشير أمثلة مذكورة في القضية إلى أنّ مجموعة "إن إس أو" تقاضت من ثلاثة عملاء مبالغ قدرها 6,835,000$، و1,412,000$، و5,630,000$ تباعاً، لقاء عناصر إضافية مرتبطة باختراق أجهزة "أندرويد" بين عامي 2018 و2019.[187] وفي إفادة أمام المحكمة، أكّدت ساريت بيزينسكي غيل، نائبة الرئيس للعمليات التجارية العالمية في الشركة، أنّ السعر القياسي لاختراق 15 جهازاً مختلفاً بين عامي 2018 و2020 كان يبلغ 7 ملايين دولار. أما بين الربع الثاني من العام 2018 والربع الثاني من العام 2020، فرضت الشركة مبالغ تراوحت بين 9,899$ و 6 ملايين دولار على 90 حساباً مختلفاً لقاء تكاليف متعلّقة ببرنامج "بيغاسوس".[188]

---

[184] بيرلروث، ن. (2016). كيف تُمكّن شركات تقنيات التجسّس الحكومات من رؤية كل شيء في الهواتف الذكية. (How Spy Tech Firms Let Governments See Everything on a Smartphone.) *نيويورك تايمز*. [متاح على الإنترنت] 2 أيلول/سبتمبر. متوفر على: https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html [تم الاطلاع عليه في 11 آب/أغسطس 2025].

[185] بيرلروث، ن. (2016). كيف تُمكّن شركات تقنيات التجسّس الحكومات من رؤية كل شيء في الهواتف الذكية. (How Spy Tech Firms Let Governments See Everything on a Smartphone.) *نيويورك تايمز*. [متاح على الإنترنت] 2 أيلول/سبتمبر.

[186] *شركة "واتساب" ضد مجموعة "إن إس أو" المحدودة* (2025) [*WhatsApp Inc. v. NSO Group Technologies Limited*د]. (محكمة المقاطعة، المنطقة الشمالية من كاليفورنيا). متوفر على: https://www.courtlistener.com/docket/16395340/679/7/whatsapp-inc-v-nso-group-technologies-limited/ [تم الاطلاع عليه في 27 آب/أغسطس 2025].

[187] *شركة "واتساب" ضد مجموعة "إن إس أو" المحدودة* (2025) [ ] (*WhatsApp Inc. v. NSO Group Technologies Limited*د].

[188] *شركة "واتساب" ضد مجموعة "إن إس أو" المحدودة* (2025) [ ] (*WhatsApp Inc. v. NSO Group Technologies Limited*د].

WhatsApp, et al. v. NSO Group, et al.
Presented Pegasus "Final Relevant Revenue" Excluding Time and Maintenance Adjustments (Q2 2018 - Q2 2020)
Supplemental Exhibit 1.1

	Account No.	Q2 - Q4 2018	2019	Q1 - Q2 2020	Q2 2018 - Q2 2020
1	Acc-01	$ -	$ -	$ -	$ -
2	Acc-02	$ -	$ -	$ -	$ -
3	Acc-03	$ 933,500	$ 1,402,390	$ 660,831	$ 2,996,721
4	Acc-04	$ 6,069,231	$ 2,410,849	$ 763,671	$ 9,243,751
5	Acc-05	$ -	$ 604,000	$ 633,306	$ 1,237,306
6	Acc-06	$ -	$ 1,412,348	$ 180,620	$ 1,592,969
7	Acc-07	$ -	$ -	$ 807,022	$ 807,022
8	Acc-08	$ -	$ -	$ -	$ -
9	Acc-09	$ -	$ -	$ -	$ -
10	Acc-10	$ 455,792	$ 1,055,518	$ 545,751	$ 2,057,060
11	Acc-12	$ -	$ -	$ -	$ -
12	Acc-13	$ 54,963	$ 69,431	$ 35,709	$ 160,102
13	Acc-14	$ -	$ 60,706	$ 37,238	$ 97,944
14	Acc-16	$ -	$ 693,527	$ 87,913	$ 781,440
15	Acc-18	$ -	$ 945,151	$ 54,849	$ 1,000,000
16	Acc-19	$ -	$ -	$ -	$ -
17	Acc-20	$ -	$ -	$ -	$ -
18	Acc-21	$ 990,725	$ 1,256,314	$ 654,452	$ 2,901,491
19	Acc-22	$ -	$ -	$ -	$ -
20	Acc-23	$ -	$ 1,570,849	$ 189,981	$ 1,760,831
21	Acc-24	$ -	$ -	$ -	$ -
22	Acc-25	$ -	$ -	$ -	$ -
23	Acc-26	$ 779,683	$ 188,844	$ 74,452	$ 1,042,979
24	Acc-27	$ -	$ 917,783	$ 105,149	$ 1,022,932
25	Acc-29	$ -	$ 1,593,128	$ 212,159	$ 1,805,287
26	Acc-31	$ 169,166	$ 200,592	$ 100,830	$ 470,588
27	Acc-32	$ -	$ 1,446,189	$ 296,739	$ 1,742,928
28	Acc-33	$ 694,000	$ 567,096	$ 431,750	$ 1,692,846
29	Acc-34	$ 211,916	$ 21,577	$ -	$ 233,493
30	Acc-37	$ -	$ -	$ -	$ -
31	Acc-38	$ -	$ -	$ -	$ -
32	Acc-39	$ -	$ 479,698	$ 38,702	$ 518,400
33	Acc-40	$ 442,500	$ 180,096	$ 176,168	$ 798,764
34	Acc-41	$ -	$ -	$ -	$ -
35	Acc-43	$ -	$ -	$ -	$ -
36	Acc-44	$ 96,250	$ 368,959	$ 185,959	$ 651,167
37	Acc-45	$ 914,805	$ 378,237	$ 160,112	$ 1,453,155
38	Acc-46	$ 791,169	$ 214,157	$ 98,598	$ 1,103,924
39	Acc-47	$ 129,736	$ (15,909)	$ -	$ 113,828
40	Acc-48	$ 574,075	$ 1,182,686	$ 745,545	$ 2,502,306
41	Acc-49	$ 343,289	$ (42,096)	$ -	$ 301,193
42	Acc-50	$ -	$ -	$ -	$ -
43	Acc-51	$ -	$ -	$ -	$ -

الصورة 7: تفصيل جزئي لتدفقات إيرادات "بيغاسوس" بين الربع الثاني من العام 2018 والربع الثاني من العام 2020.[189]

"واتساب" وآخرون ضد مجموعة "إن إس أو" وآخرين

"الإيرادات النهائية ذات الصلة" لبرنامج بيغاسوس باستثناء التعديلات المتعلقة بالوقت والصيانة
(من الربع الثاني لعام 2018 إلى الربع الثاني لعام 2020)

[189] شركة *"واتساب" ضد مجموعة "إن إس أو" المحدودة (WhatsApp Inc. v. NSO Group Technologies Limited)* [2025]د].

الملحق الإضافي 1.1

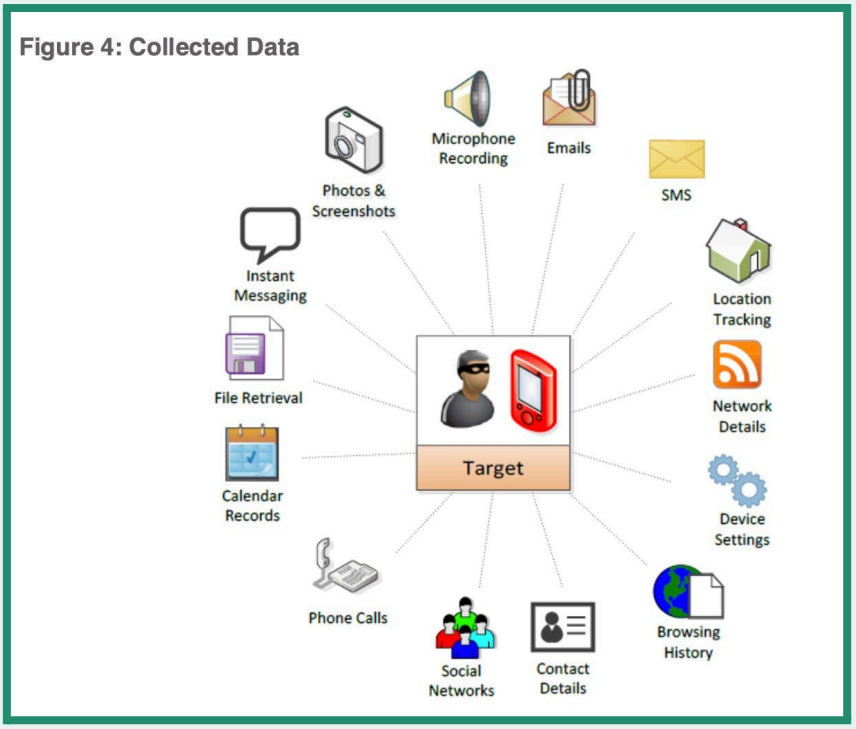
رقم الحساب	الربع الثاني-الربع الرابع 2018		2019		الربع الأول- الربع الثاني 2020		الربع الثاني 2018- الربع الثاني 2020
1 حساب-01	$	-	$	-	$	-	-
2 حساب-02	$	-	$	-	$	-	-
3 حساب-03	$	933,500	$	1,402,390	$	660,831	2,996,721
4 حساب-04	$	6,069,231	$	2,410,849	$	763,671	9,243,751
5 حساب-05	$	-	$	604,000	$	633,306	1,237,306
6 حساب-06	$	-	$	1,412,348	$	180,620	1,592,969
7 حساب-07	$	-	$	-	$	807,022	807,022
8 حساب-08	$	-	$	-	$	-	-
9 حساب-09	$	-	$	-	$	-	-
10 حساب-10	$	455,792	$	1,055,518	$	545,751	2,057,060
11 حساب-12	$	-	$	-	$	-	-
12 حساب-13	$	54,963	$	69,431	$	35,709	160,102
13 حساب-14	$	-	$	60,706	$	37,238	97,944
14 حساب-16	$	-	$	693,527	$	87,913	781,440
15 حساب- 18	$	-	$	945,151	$	54,849	1,000,000
16 حساب-19	$	-	$	-	$	-	-
17 حساب-20	$	-	$	-	$	-	-
18 حساب-21	$	990,725	$	1,256,314	$	654,452	2,901,491
19 حساب-22	$	-	$	-	$	-	-
20 حساب-23	$	-	$	1,570,849	$	189,981	1,760,831
21 حساب-24	$	-	$	-	$	-	-
22 حساب-25	$	-	$	-	$	-	-
23 حساب-26	$	779,683	$	188,844	$	74,452	1,042,979
24 حساب-27	$	-	$	917,783	$	105,149	1,022,932
25 حساب-29	$	-	$	1,593,128	$	212,159	1,805,287
26 حساب-31	$	169,166	$	200,592	$	100,830	470,588
27 حساب-32	$	-	$	1,446,189	$	296,739	1,742,928
28 حساب-33	$	694,000	$	567,096	$	431,750	1,692,846
29 حساب-34	$	211,916	$	21,577	$	-	233,493
30 حساب-37	$	-	$	-	$	-	-
31 حساب-38	$	-	$	-	$	-	-
32 حساب-39	$	-	$	479,698	$	38,702	518,400
33 حساب-40	$	442,500	$	180,096	$	176,168	798,764
34 حساب-41	$	-	$	-	$	-	-
35 حساب-43	$	-	$	-	$	-	-
36 حساب-44	$	96,250	$	368,959	$	185,959	651,167
37 حساب-45	$	914,805	$	378,237	$	160,112	1,453,155
38 حساب-46	$	791,169	$	214,157	$	98,598	1,103,924

39 حساب-47	$	129,736	$	(15,909)	$	-	$	11,828
40 حساب-48	$	574,075	$	1,182,686	$	745,545	$	2,502,306
41 حساب-49	$	343,289	$	(42,096)	$	-	$	301,193
42 حساب-50	$	-	$	-	$	-	$	-
43 حساب-51	$	-	$	-	$	-	$	-

القدرات

تتمثّل الوظيفة الأساسية لبرنامج "بيغاسوس" في مراقبة نشاط المستخدم في الوقت الفعلي والنقل غير المصرّح للبيانات من الهواتف المستهدَفة من دون إشعار المستخدم حول اختراق جهازه.[190] ويمكن للبرنامج استهداف أجهزة "أندرويد" و"آيفون"؛ وتُطلق "غوغل" على النسخة الخاصة بنظام "أندرويد" اسم "كرايساور" (Chrysaor).[191]

تُظهر معلومات تسويقية مسرّبة من العام 2016 لمحة عن قدرات "بيغاسوس". إذ يستطيع البرنامج جمع جميع البيانات المخزّنة على الهواتف، بما في ذلك الرسائل النصية، ورسائل البريد الإلكتروني، والصور، ومقاطع الفيديو، والمذكرات الصوتية، وسجلّ الأحداث، وسجلّ المكالمات، وسجلّ التصفّح، وأسماء المستخدمين وكلمات المرور. كما يمكنه مراقبة مواقع المستخدم، وتشغيل الميكروفون للتنصّت على المحادثات، وتشغيل الكاميرات لالتقاط صورٍ للمستخدم من بُعد.



[190] زيتر، ك. (2021). *برنامج "بيغاسوس" للتجسس: كيف يعمل وما يجمعه.* (*Pegasus Spyware: How It Works and What It Collects*.) [متاح على الإنترنت] زيرو داي (ZERO DAY). متوفر على: https://www.zetter-zeroday.com/pegasus-spyware-how-it-works-and/ [تم الاطلاع عليه في 11 آب/أغسطس 2025].

[191] كوب، م. (2017). *كيف تختلف برمجية "بيغاسوس" الخبيثة على نظام أندرويد عنه على نظام آي أو إس؟* (*How is Pegasus malware different on Android than on iOS?*) [متاح على الإنترنت] سيرش سكيورتي (Search Security). متوفر على: https://www.techtarget.com/searchsecurity/answer/How-is-Pegasus-malware-different-on-Android-than-on-iOS [تم الاطلاع عليه في 11 آب/أغسطس 2025].

الصورة 8: كتيّب تسويقي مُسرّب لبرنامج "بيغاسوس" من العام 2016 يوضّح أنواع البيانات التي يمكنه جمعها.[192]

Figure 4: collected data	الصورة 4: البيانات المُجمّعة
Target	الهدف
Emails	البريد الالكتروني
SMS	الرسائل النصية
Location Tracking	تعقّب الموقع
Network Details	تفاصيل الشبكة
Device Settings	إعدادات الجهاز
Browsing History	سجلّ التصفّح
Contact Details	تفاصيل جهة الاتصال
Social Networks	شبكات التواصل
Phone calls	المكالمات الهاتفية
Calendar Records	سجلّ التقويم
File Retrieval	استرجاع الملفات
Instant Messaging	الرسائل الفورية
Photos and screenshots	صور ولقطات الشاشة
Microphone Recording	تسجيل الميكروفون

يمكن تثبيت "بيغاسوس" على الهواتف مادياً، أو عبر هجمات النقرة الواحدة أو هجمات بدون أي نقرة.[193] ففي حالة "النقرة الواحدة"، يرسل مشغّلو البرنامج رسائل التصيد الاحتيالي عبر النصوص أو البريد الإلكتروني تتضمّن رابطاً ضاراً. وبمجرد النقر، يُوجَّه المستخدم إلى صفحة تُحمّل "بيغاسوس" خلسةً. أما في حالة " بدون أي نقرة"، فيُرسَل البرنامج بطريقة لا تتطلّب من الهدف الضغط على أيّ رابط. ففي السابق، شملت الهجمات تلقّي المستخدم رسالة "iMessage" صامتة تُفعّل سلسلة تدمير تؤدي إلى تثبيت "بيغاسوس" على الهاتف. كما يمكن لمشغّلي البرنامج استغلال أبراج الاتصالات الخلوية المزيفة القريبة من الهاتف المستهدَف، ما يتيح شنّ هجوم الوسيط في المنتصف، حيث تتّصل الضحية ببرج اتصالات وهمي يصيب الجهاز بـ"بيغاسوس". وتنجز مجموعة "إن إس أو" هذه الهجمات عبر تطوير و/أو شراء ثغرات "يوم الصفر" (zero-day) التي تصيب أنظمة "آيفون" و"أندرويد"، وتستهدف ثغرات برمجية لا يعرفها مصنّعو الهواتف.

وبمجرد أن يُصيب "بيغاسوس" الهاتف، ينسخ البيانات المستهدفة ويضغطها ثم يُشفّرها باستخدام معيار التشفير AES 128-bit.[194] وبعدها، يرسل البيانات إلى خادم القيادة والسيطرة ضمن شبكة العميل. ووفقاً للباحثة الأمنية كيم زيتر، يُخفي "بيغاسوس" البيانات في مخازن مؤقتة "مخفية ومشفّرة" ثم ينقلها عبر شبكات "الواي فاي" أو الشبكات الخلوية، وبفضل ضغط البيانات، يبقى تأثيره على أداء الجهاز ضئيلاً جداً ويستهلك كمية قليلة من البيانات. وأخيراً، تدّعي مجموعة "إن إس أو" أنّها تنقل البيانات عبر أدوات إخفاء الهوية لإخفاء معلومات حول البيانات وهوية الجهة المستقبلة. وبحسب منظمة العفو الدولية، تتركّز البنية التحتية لهجمات "بيغاسوس" بشكلٍ أساسي في أميركا الشمالية وأوروبا (مع خادم واحد في البحرين)،

---

[192] مجموعة "إن إس أو" (2016). *"بيغاسوس" – وصف المنتج*. (Pegasus – Product Description) [متاح على الإنترنت] كيم زيتر. متوفر على: https://www.zetter-zeroday.com/content/files/documents/4599753/nso-pegasus.pdf [تم الاطلاع عليه في 7 تموز/يوليو 2025].

[193] زيتر، ك. (2021). *برنامج "بيغاسوس" للتجسس: كيف يعمل وما يجمعه*. (*Pegasus Spyware: How It Works and What It Collects*).

[194] زيتر، ك. (2021). *برنامج "بيغاسوس" للتجسس: كيف يعمل وما يجمعه*. (*Pegasus Spyware: How It Works and What It Collects*).

ومعظمها ملك لشركات أميركية مثل "خدمات أمازون ويب" (Amazon Web Services) و"ديجيتال أوشن" (Digital Ocean) و"لينود" (Linode).[195]

وتزعم المجموعة أنّ "بيغاسوس" يعمل على مستوى النواة وأنه قادر على تدمير نفسه، ما يجعل اكتشافه شبه مستحيل.[196] غير أنّ منظمة العفو الدولية أصدرت أداةً لمساعدة الضحايا على التحقّق مما إذا كانت أجهزتهم قد تعرضت للاختراق أم لا.[197]

هجوم بارز

في كانون الأول/ديسمبر 2021، نشرت صحيفة "واشنطن بوست" تقريراً حقّق في واحدة من أكثر الاستخدامات المشينة لبرنامج التجسّس "بيغاسوس".[198] ففي العام 2018، كانت حنان العتر، زوجة الصحافي السعودي جمال خاشقجي، تعمل مضيفة في شركة طيران الإمارات. وأثناء مرورها في مطار دبي بتاريخ 21 نيسان/أبريل 2018، حاصرها عناصر الأمن، واختطفوها، وعصّبوا عينيها، وصادروا هاتفيها من نوع "أندرويد"، وحاسوبها المحمول، وكلمات السر الخاصة بها. ثمّ خضعت لاستجواب حول خاشقجي وأنشطة اعتُبرت محرّضة على أنظمة الحكم الملكية في الخليج.

وفي اليوم التالي، ثبّت مسؤول أمني برنامج "بيغاسوس" على أحد هواتفها عبر الدخول إلى موقع إلكتروني صمّمته مجموعة "إن إس أو" لعميل إماراتي، حيث جرى تحميل البرنامج خلال بضع دقائق، وبعد أيام قليلة، استلمت العتر هاتفيها. وبينما لم يستطع الباحثون في مجال التكنولوجيا الذين فحصوا أجهزتها من التحقق مما إذا كان برنامج التجسس قد أصاب الهاتف بنجاح، فإنّ مسؤولي الأمن الإماراتيّين لم يُعيدوا إدخال رابط تنزيل البرنامج، ما يشير إلى نجاح التثبيت.[199] وعلى الرغم من أنّ مجموعة "إن إس أو" نفت بشدّة تورّطها في الحادثة، التي وقعت قبل أشهر من اغتيال خاشقجي، كشف تسريب بيانات يضم 50,000 رقم هاتف يُرجّح استهدافه عبر "بيغاسوس" أنّ العتر وخديجة جنكيز، خطيبة خاشقجي التركية، كانتا من بين الأهداف.[200] وأفادت منظمة العفو الدولية بأنّ عملاء مجموعة "إن إس أو" في الإمارات العربية المتحدة حاولوا استخدام بيغاسوس للتجسّس على العتر منذ تشرين الثاني/نوفمبر 2017.[201]

---

[195] مختبر الأمن التابع لمنظمة العفو الدولية (2021). تقرير منهجية التحقيق التقني الجنائي: كيف تكتشف الاختراق ببرنامج "بيغاسوس" التابع لمجموعة "إن إس أو".

[196] زيتر، ك. (2021). *برنامج "بيغاسوس" للتجسس: كيف يعمل وما يجمعه*. (*Pegasus Spyware: How It Works and What It Collects*).

[197] مختبر الأمن التابع لمنظمة العفو الدولية (2021). تقرير منهجية التحقيق التقني الجنائي: كيف تكتشف الاختراق ببرنامج "بيغاسوس" التابع لمجموعة "إن إس أو".

[198] بريست، د. (2021). *وكالة إماراتية زرعت برنامج التجسس "بيغاسوس" في هاتف زوجة جمال خاشقجي قبل أشهر من مقتله، وفقاً لأدلة جنائية جديدة*. (*Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months before His Murder, New Forensics Show*) [متاح على الإنترنت] واشنطن بوست. متوفر على: https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/ [تم الاطلاع عليه في 11 تموز/يوليو 2025].

[199] بريست، د. (2021). *وكالة إماراتية زرعت برنامج التجسس "بيغاسوس" في هاتف زوجة جمال خاشقجي قبل أشهر من مقتله، وفقاً لأدلة جنائية جديدة*. (*Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months before His Murder, New Forensics Show*)

[200] بريست، د.، وميخنيت، س.، وبوفارت، أ. (2021). *استهداف زوجة جمال خاشقجي ببرنامج تجسس قبل مقتله*. (*Jamal Khashoggi's wife targeted with spyware before his death*.) [متاح على الإنترنت] واشنطن بوست. متوفر على: https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/ [تم الاطلاع عليه في 11 تموز/يوليو 2025].

[201] بريست، د. (2021). *وكالة إماراتية زرعت برنامج التجسس "بيغاسوس" في هاتف زوجة جمال خاشقجي قبل أشهر من مقتله، وفقاً لأدلة جنائية جديدة*. (*A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months before His Murder, New Forensics Show*)

أثّرت هذه الحادثة على العتر بشدّة. ففي مقابلة مع "واشنطن بوست"، قالت: كل يوم عندما أرى ضوء النهار، لا أعرف لماذا ما زلت على قيد الحياة... لقد فقدت حياتي ... كنت أعول عائلتي والآن لا يمكنني حتى توفير قوت لنفسي".[202] كما تغيّرت حياة جنكيز تغيّراً جذريّاً خوفاً على حياتها بعد اغتيال خاشقجي وكشف تفاصيل "بيغاسوس"، فاضطرّت إلى توظيف حراس شخصيّين ولم تعد تشعر بالأمان. وهذا بالضبط ما يفعله "بيغاسوس": يجرّد ضحاياه من حقّهم الأساسي في الخصوصية، وقد يساهم في ارتكاب أشكالٍ أخرى من القمع، تشمل الاختطاف وحتى القتل.

3.2 تحالف "سايتروكس" و"إنتلكسا"

"الكون يحتاج إلى منتجنا، بطريقة أو بأخرى".

-تال ديليان، مؤسّس تحالف "إنتلكسا"

نبذة عن شركة "سايتروكس"

بدأت قصة "سايتروكس" في العام 2017، عندما تأسّست كشركة ناشئة في مجال "الحلول السيبرانية".[203] وقد سُجّلت الشركة تحت اسم "Cytrox AD" (رقم التسجيل: 7191391، وتُعرف أيضاً باسم CAJTPOKC АД) في سكوبيا بتاريخ 27 آذار/مارس 2017. أسّسها خمسة رجال أعمال إسرائيليّين هم: ألون أرابوف، وأبراهام روبنشتاين، وإيال أبراهام أورين، ودرور هارباز، وشارون أدلر، بالإضافة إلى رجل الأعمال المجري روتم فاركاش.[204] [205] وكما أشار مختبر "سيتيزن لاب" في تقريره الأول حول "سايتروكس" وبرنامجها للتجسّس "بريداتور"، فقد وصفت الشركة نفسها على موقع "بيتش بوك" (Pitchbook) بأنّها شركة تساعد عملاء حكوميين على "جمع المعلومات من... الأجهزة الطرفية... [و] خدمات السحابة".[206]

وبحسب صحافيَّيْن استقصائيّين من مقدونيا الشمالية يعملان لدى مختبر التحقيقات الاستقصائية في مقدونيا الشمالية (IRL Macedonia)، كان إيفو مالينكوفسكي المدير التنفيذي الأول للشركة، وهو رائد أعمال مقدوني يبلغ من العمر 26 عاماً،

---

[202] بريست، د. (2021). *وكالة إماراتية زرعت برنامج التجسس "بيغاسوس" في هاتف زوجة جمال خاشقجي قبل أشهر من مقتله، وفقاً لأدلة جنائية جديدة.* (*A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months before His Murder, New (Forensics Show*

[203] "كرانشبيس" (Crunchbase) (2024). *"سايتروكس" – الملف التعريفي والتمويل على كرنشبيس.* (*Cytrox - Crunchbase Company Profile & Funding*) [متاح على الإنترنت] "كرانشبيس". متوفر على: https://www.crunchbase.com/organization/cytrox [تم الاطلاع عليه في 27 آب/أغسطس 2025].

[204] السجل المركزي لجمهورية مقدونيا الشمالية. (2025). ملف التعريف الأساسي لكيان قانوني مسجَّل: "سايتروكس". (Basic Profile of a Registered Legal Entity: Entry for CAJTPOKC АД.) [متاح على الإنترنت] متوفر على: https://crm.com.mk/en/open-data/basic-profile-of-a-registered-entity?embs=7191391 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[205] سفيتكوسكا، س.، ناستيسكا، آي.، ستويانوفسكي، ب.، تيلوغلو، ت.، تريانتافيلو، إي.، وسيمونوفسكا، م. (2023). *شركة إسرائيلية طوّرت برنامج تجسس في سكوبيا بينما تجاهل المسؤولون المحليون الأمر.* (*Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way*) *مختبر الصحافة الاستقصائية في مقدونيا الشمالية (IRL).* [متاح على الإنترنت] متوفر على: https://irl.mk/israeli-company-developed-spyware-in-skopje-local-officials-looked-the-other-way/ [تم الاطلاع عليه في 26 تموز/يوليو 2025].

[206] "كرانشبيس" (Crunchbase) (2024). *"سايتروكس" – الملف التعريفي والتمويل على كرنشبيس.* (*Cytrox - Crunchbase Company (Profile & Funding*

ينتمي إلى عائلة تعمل في تجارة السلاح وصناعة النبيذ. وتُظهر نسخة مؤرشفة من الموقع الإلكتروني المبكر للشركة بتاريخ 17 كانون الأول/ديسمبر 2017، أنّ البريد الإلكتروني لمالينكوفسكي (ivo@cytrox[.]com) كان مدرجاً كجهة للتواصل.[207] كما أُدرج اسم مايير شامير، وهو ضابط سابق في سلاح الجو الإسرائيلي تربطه علاقاتٌ برائد الأعمال في مجال برامج التجسّس تال ديليان، كمالك مستفيد من "سايتروكس". وفي 6 تشرين الأول/أكتوبر 2017، قدّم مالينكوفسكي، عبر شركتين كان يديرهما، طلباً رسمياً إلى وزارة الداخلية في مقدونيا الشمالية للحصول على إذن ببيع منتجات برمجية لاعتراض البيانات الشخصية لصالح عملاء حكوميين. ثمّ أعاد تقديم الطلب في 7 تشرين الثاني/نوفمبر 2017 مرفقاً بمزيدٍ من التفاصيل التي قدّمت شرحاً حول المنتج الأساسي لـ"سايتروكس"، وهو برنامج "بريداتور".[208] [انظر أدناه لمزيد من التفاصيل حول بريداتور]

الصورة 9: شعار شركة سايتروكس التجاري، كما ورد في موقع IT[.]mk.[209]

سايتروكس	Cytrox
حلول الاستخبارات السيبرانية	Cyber-Intelligence-Solutions

ويبدو أنّ ثلاث شركات لها صلة بـ"سايتروكس" قد تأسّست أيضاً في العام 2017 في كلٍّ من إسرائيل والمجر. فالشركتان الإسرائيليتان "سايتروكس في أوروبا والشرق الأوسط وأفريقيا المحدودة" (Cytrox EMEA Ltd.) (رقم التسجيل: 515692135) و"سايتروكس سوفتوير المحدودة" (Cytrox Software Ltd.) (رقم التسجيل: 515693893) أُعيد تسميتهما في العام 2019 إلى " بالينيز المحدودة" (Balinese Ltd.) وبيتربالد المحدودة" (Petrbald Ltd.). أما الشركة المجرية "سايتروكس هولدينغز المحدودة" (Cytrox Holdings Zrt) (رقم التسجيل: 01-10-049372)، فيبدو أنها دخلت مرحلة التصفية اعتباراً من العام 2025، وفقاً للسجلات التجارية المجرية.[210] وبحسب تقرير صادر عن شبكة البلقان للتحقيقات الاستقصائية (BIRN) في مقدونيا بتاريخ 30 كانون الأول/ديسمبر 2021، فإنّ ملفات "سايتروكس" لعام 2020 تُظهر أنّ إيراداتها بلغت 1.5 مليون يورو، وعدد موظفيها 16 موظفاً، بينما بلغت نفقاتها 100,000 يورو.[211]

---

[207] سايتروكس (2017). *الصفحة الرئيسية لـ"سايتروكس" – الاستخبارات السيبرانية*. (*Cytrox – Cyber Intelligence Home Page*.) [متاح على الإنترنت] متوفر على: https://web.archive.org/web/20171217071850/http://cytrox.com/ [تم الاطلاع عليه في 1 آب/أغسطس 2025].

[208] سفيتكوسكا، س.، ناستيسكا، آي.، ستويانوفسكي، ب.، تيلوغلو، ت.، تريانتافيلو، إي.، وسيمونوفسكا، م. (2023). *شركة إسرائيلية طوّرت برنامج تجسس في سكوبيا بينما تجاهل المسؤولون المحليون الأمر*. (*Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way*) مختبر الصحافة الاستقصائية في مقدونيا الشمالية (IRL).

[209] فريق تحرير موقع (2021) IT.mk. *لماذا حظرت "ميتا" شركة برامج التجسس المقدونية "سايتروكس"*. (*Зошто Мета ја баниираше македонската компанија за шпионски софтвер, Cytrox*)موقع IT.mk

[210] وزارة العدل – خدمة معلومات الشركات والإجراءات الإلكترونية في المجر (2025). السجل الوطني للشركات ونظام معلومات الشركات: شركة "سايتروكس هولدينغز Zrt" (National Company Register and Company Information System: Entry for Cytrox Holdings Zrt.) [متاح عبر الإنترنت] متوفر على: https://www.e-cegjegyzek.hu/?cegkereses [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[211] أبوستولوف، ف. (2021). *التجسس الإلكتروني على الأراضي المقدونية*. (*Елитна сајбер-шпионажа На Македонски Погон) [متاح على الإنترنت] شبكة البلقان للتحقيقات الاستقصائية، مقدونيا. متوفر على:* https://prizma.mk/elitna-sajber-shpionazha-na-makedonski-pogon/ [تم الاطلاع عليه في 12 تموز/يوليو 2025].

كما تأسّست أربع شركات أخرى متخصّصة بالأمن السيبراني بين عامي 2017 و2020 تحت العنوان نفسه لصالح شركة "سايتروكس" في سكوبيا، وهي: " سينتيليكسا" (Cintellexa) (رقم التسجيل: 7398085، "СИНТЕЛЕКСА ДООЕЛ Скопје")،[212] و"سايبرلاب" (Cyberlab) (رقم التسجيل: 7319339، " САЈБЕР ЛАБ ДООЕЛ Скопје")،[213] و"سايغنت" (Cygent) (رقم التسجيل: 7473222، "САЈГНЕТ ДООЕЛ Скопје")،[214] و"سايشارك" (Cyshark) (رقم التسجيل: 7187254، "САЈШАРК ДООЕЛ Скопје").[215] [216] ويرتبط أبراهام روبنشتاين وروتم فاركاش بصفة مالكين مستفيدين بشركتي "سايتروكس" و"سايبرلاب"، بينما يُعدّ موشيه فاركاش (والد روتم) شريكاً في ملكية "سايشارك" مع مالينكوفسكي.[217] وتُشير التقارير إلى أنّ جميع هذه الكيانات على صلة بـتال ديليان.[218] كما بدأت العلاقات بين شبكة الشركات هذه والجيش الإسرائيلي بالتطوّر خلال هذه الفترة.

وبحسب مهندس برمجيات سابق عمل في الشركات الخمس مجتمعةً، أدار شاحاك شاليف شركة "سايبرلاب"، وهو إسرائيلي شغل منصب رئيس قسم البحث والتطوير في "إنتلكسا" وعمل سابقاً كـ"خبير في الأمن السيبراني" ضمن قوات

---

[212] شركة CompanyWall Business (2019). "*سينتليكسا ذ.م.م.*"، سكوبيا. *СИНТЕЛЕКСА ДООЕЛ Скопје [متاح عبر الإنترنت]* شركة CompanyWall Business. متوفر على: https://www.companywall.com.mk/kompanija/%D1%81%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%81%D0%B0-%D0%B4%D0%BE%D0%BE%D0%B5%D0%BB-%D1%81%D0%BA%D0%BE%D0%BF%D1%98%D0%B5/MMvwvEq [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[213] شركة CompanyWall Business (2018). "*سايبرلاب ذ.م.م.*"، سكوبيا. *САЈБЕР ЛАБ ДООЕЛ Скопје*. [متاح عبر الإنترنت] شركة CompanyWall Business. متوفر على: https://www.companywall.com.mk/kompanija/%D1%81%D0%B0%D1%98%D0%B1%D0%B5%D1%80-%D0%B%D0%B0%D0%B1-%D0%B4%D0%BE%D0%BE%D0%B5%D0%BB-%D1%81%D0%BA%D0%BE%D0%BF%D1%98%D0%B5/MMx2VZyY [تم الاطلاع عليه في 28 25 آب/أغسطس 2025].

[214] شركة CompanyWall Business (2020). "*سايغنت ذ.م.م.*"، سكوبيا. *САЈГНЕТ ДООЕЛ Скопје*. [متاح عبر الإنترنت] شركة CompanyWall Business. متوفر على: https://www.companywall.com.mk/kompanija/%D1%81%D0%B0%D1%98%D0%B3%D0%BD%D0%B5%D1%82-%D0%B4%D0%BE%D0%BE%D0%B5%D0%BB-%D1%81%D0%BA%D0%BE%D0%BF%D1%98%D0%B5/MMf8srq [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[215] شركة CompanyWall Business (2017). "*سايشارك ذ.م.م.*"، سكوبيا. *САЈШАРК ДООЕЛ Скопје* [متاح عبر الإنترنت] شركة CompanyWall Business. متوفر على: https://www.companywall.com.mk/kompanija/%D1%81%D0%B0%D1%98%D1%88%D0%B0%D1%80%D0%BA-%D0%B4%D0%BE%D0%BE%D0%B5%D0%BB-%D1%81%D0%BA%D0%BE%D0%BF%D1%98%D0%B5/MMxrrUsD [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[216] سفيتكوسكا، س.، ناستيسكا، آي.، ستويانوفسكي، ب.، تيلوغلو، ت.، تريانتافيلو، إي.، وسيمونوفسكا، م. (2023). *شركة إسرائيلية طوّرت برنامج تجسس في سكوبيا بينما تجاهل المسؤولون المحليون الأمر*. (*Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way*) *مختبر الصحافة الاستقصائية في مقدونيا الشمالية (IRL)*.

[217] أدرجت عدّة شركات مرتبطة بـ"سايتروكس" أسماء أشخاصٍ لا تربطهم بها أيّ صلةٍ فعليةٍ في سجلاتها الرسمية ومعلومات الاتصال الخاصة بها، بهدف إخفاء شبكتها المؤسسية المعقّدة. فعلى سبيل المثال، ووفقاً لمختبر التحقيقات الاستقصائية في مقدونيا الشمالية، أُدرج اسم جدّة مالينكوفسكي من جهة الأم بصفتها مالكة لشركة "سايشارك"، من دون أن يتّضح ما إذا كانت قد وافقت على ذلك أم لا. وفي مثال آخر، أفاد موقع "إنفستيغايت" (Investigate[.]cz) في العام 2024 بأنّ شركة "سايتروكس" أدرجت اسم امرأة تشيكية مسنّة تقيم في قرية صغيرة بصفتها مديرةً للشركة، من دون علمها بذلك. وبعد أيامٍ قليلة من زيارة أحد الصحافيين لها في العام 2023، غيّرت سايتروكس اسم المديرة المسجّلة إلى سيلفيا ج.، وهي امرأة بولندية تبلغ من العمر 25 عاماً. وعندما زار الصحافيون عنوانها، لم يجدوا أيّ دليل على إقامتها هناك. وقد تمكّنوا من التواصل معها عبر تطبيق "إنستغرام"، وتحقّقوا من أنّها الشخص نفسه المذكور في السجلات التجارية للشركة، لكنها نفت أي علاقة لها بالشركة، ثمّ حذفت حسابها على الفور وأنشأت حساباً جديداً باسمٍ مختلف.

[218] سفيتكوسكا، س.، ناستيسكا، آي.، ستويانوفسكي، ب.، تيلوغلو، ت.، تريانتافيلو، إي.، وسيمونوفسكا، م. (2023). *شركة إسرائيلية طوّرت برنامج تجسس في سكوبيا بينما تجاهل المسؤولون المحليون الأمر*. (*Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way*) *مختبر الصحافة الاستقصائية في مقدونيا الشمالية (IRL)*.

الجيش الإسرائيلي.[219] وأفاد موقع "إنتلجنس أونلاين" (Intelligence Online) في العام 2017 بأنّ شاليف كان مدير البحث والتطوير في سايتروكس".[220] وعلى الرغم من أنّ مالينكوفسكي كان المدير الرسمي لـ"سايبرلاب"، إلّا أنّ شركة "إنبيديو" (Inpedio) الهولندية، التي يملكها روبنشتاين وفاركاش، كانت المالك الفعلي للمشروع. وشغل شاليف منصب نائب الرئيس للتكنولوجيا في "إنبيديو" حتى العام 2020.[221] وقد حصلت كلٌّ من "إنبيديو" و"سايتروكس" على استثمارات من الصناعات الجوية الإسرائيلية (IAI) في العام 2017، كما يبدو أنّ "سايتروكس" كانت مرتبطة أيضاً بصندوق "أتورو" (Atooro Fund).[222] والمفارقة أنّ شاليف يعمل اليوم في شركة "مالويربايتس" (Malwarebytes)، وهي شركة متخصّصة في مكافحة الفيروسات والبرمجيات الخبيثة وتقديم خدمة الحماية من الاحتيال، حيث يشغل منصب المدير الأول للتكنولوجيا والهندسة في قسم حماية خصوصية المستهلك.

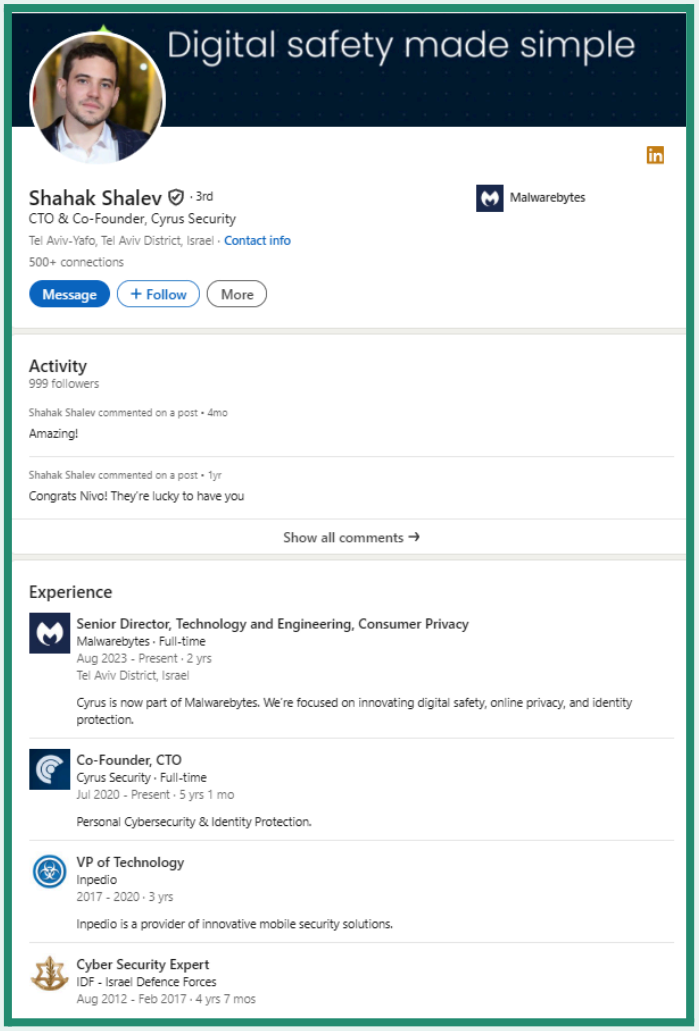
---

[219] سفيتكوسكا، س.، ناستيسكا، آي.، ستويانوفسكي، ب.، تيلوغلو، ت.، تريانتافيلو، إي.، وسيمونوفسكا، م. (2023). *شركة إسرائيلية طوّرت برنامج تجسس في سكوبيا بينما تجاهل المسؤولون المحليون الأمر.* (*Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way*) *مختبر الصحافة الاستقصائية في مقدونيا الشمالية (IRL).*

[220] إنتلجنس أونلاين (Intelligence Online) (2017). *النجوم السيبرانية الجديدة للصناعات الجوية الإسرائيلية (IAI).* إنتلجنس أونلاين [متاح عبرالإنترنت] 7 أيار/مايو. متوفر على: https://www.intelligenceonline.com/corporate-intelligence/2017/07/05/cytrox-and-inpedio-iai-s-new-cyber-stars,108252955-bre [تم الاطلاع عليه في 28 حزيران/يونيو 2025].

[221] سفيتكوسكا، س.، ناستيسكا، آي.، ستويانوفسكي، ب.، تيلوغلو، ت.، تريانتافيلو، إي.، وسيمونوفسكا، م. (2023). *شركة إسرائيلية طوّرت برنامج تجسس في سكوبيا بينما تجاهل المسؤولون المحليون الأمر.* (*Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way*) *مختبر الصحافة الاستقصائية في مقدونيا الشمالية (IRL).*

[222] صندوق "أتورو" (Atooro Fund) (2024). *الصفحة الرئيسة لصندوق "أتورو".* (*Atooro Fund Home Page*) *[متاح* عبرالإنترنت] متوفر على: https://www.atooro.com/ [تم الاطلاع عليه في 28 آب/أغسطس 2025].



الصورة 10: صفحة "لينكد إن" العامة لشاحاك شالف تُظهر تاريخ عمله في شركة "إنبيديو".[223]

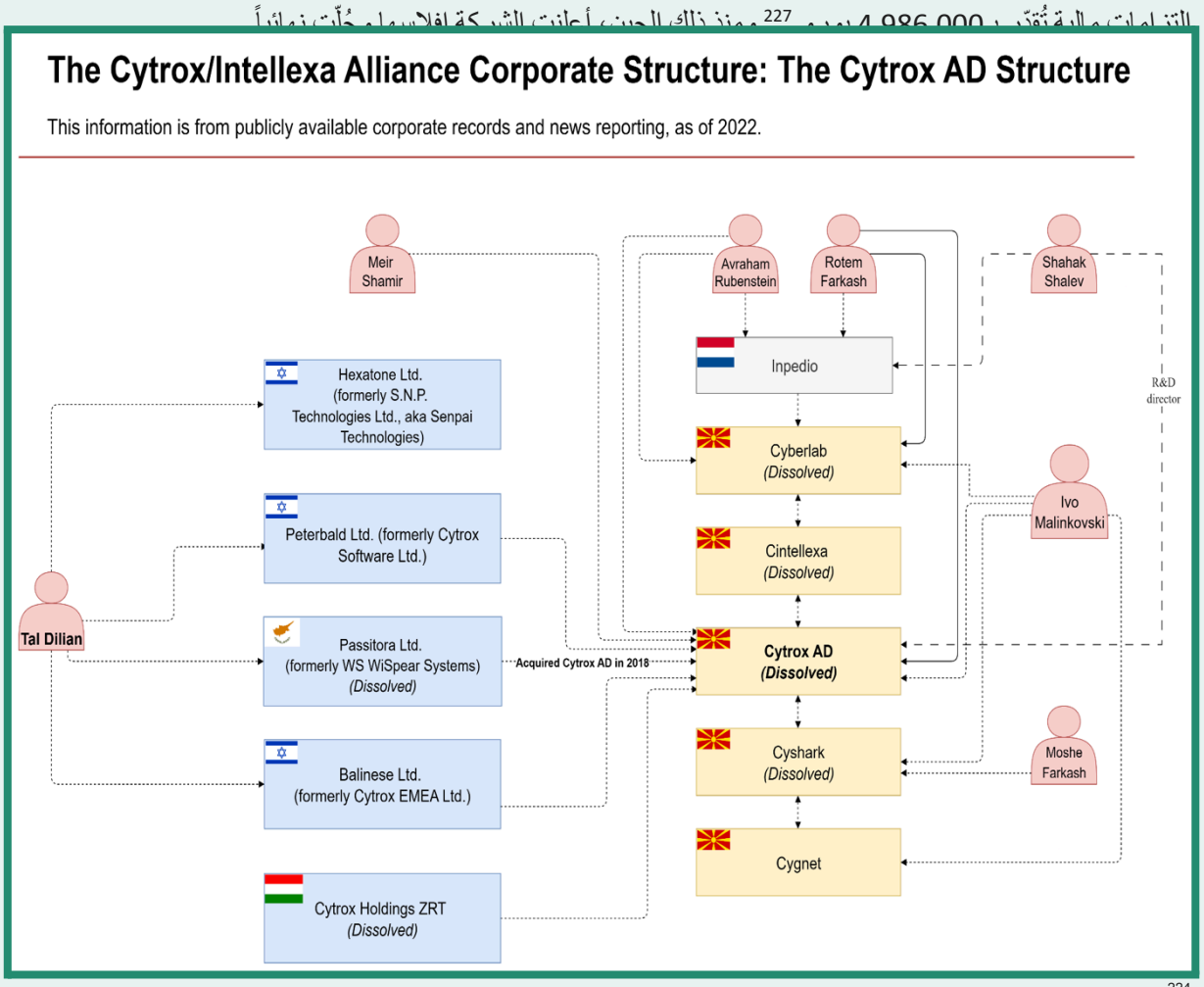
Digital safety made simple	الأمان الرقمي بطريقة بسيطة
Shahak Shalev	شاحاك شالف
3rd	الدرجة الثالثة من الاتصال
CTO & Co-Founder, Cyrus Security	المدير التقني والمؤسِّس الشريك لشركة "سايرس سيكيوريتي" (Cyrus Security)
Tel Aviv-Yafo, Tel Aviv District, Israel. Contact info	تل أبيب – يافا، منطقة تل أبيب، إسرائيل معلومات الاتصال
500+ connections	أكثر من 500 اتصال
Message	رسالة
+ Follow	+متابعة
More	المزيد
Malwarebytes	"مالويربايتس" (Malwarebytes)
Activity	النشاط
999 followers	999 متابعاً

[223] شالف، ش. (2025). صفحة *شاحاك شالف على "لينكد إن"*. [لينكد إن]. [تم الاطلاع عليه في 14 آب/أغسطس 2025]. متوفر على: https://www.linkedin.com/in/shahak-shalev-ba2a49135/.

Shahak Shalev commented on a post- 4mo Amazing! Shahak Shalev commented on a post 1yr Congrats Nivo! They're lucky to have you	شاحاك شالف علّق على منشور- 4 أشهر رائع! شاحاك شالف علّق على منشور- سنة تهانينا يا نيفو! إنهم محظوظون بانضمامك إليهم
Show all comments → Experience Senior Director, Technology and Engineering, Consumer Privacy Malwarebytes. Full-time Aug 2023-Present. 2 yrs Tel Aviv District Israel Cyrus is now part of Malwarebytes. We're focused on innovating digital safety, online privacy, and identity protection.	عرض جميع التعليقات ← الخبرة المدير الأول للتكنولوجيا والهندسة، خصوصية المستهلك شركة "مالويربايتس" - دوام كامل منذ آب/أغسطس 2023 حتى الآن. سنتان منطقة تل أبيب، إسرائيل أصبحت شركة "سايروس" (Cyrus) الآن جزءاً من "مالويربايتس". نركّز على تطوير الابتكار في مجال الأمان الرقمي، والخصوصية على الإنترنت، وحماية الهوية.
Co-Founder, CTO Cyrus Security. Full-time Jul 2020-Present - 5 yrs 1 mo Personal Cybersecurity & Identity Protection.	الشريك المؤسِّس والرئيس التنفيذي للتكنولوجيا شركة "سايروس سيكيوريتي" (Cyrus Security) - دوام كامل منذ تموز/يوليو 2020 حتى الآن. 5 سنوات وشهر واحد الأمن السيبراني الشخصي وحماية الهوية.
VP of Technology Inpedio 2017-2020 3 yrs Inpedio is a provider of innovative mobile security solutions.	نائب رئيس قسم التكنولوجيا شركة "إنبيديو" (Inpedio) 2017-2020. 3 سنوات تقدّم "إنبيديو" حلولاً مبتكرة لأمن الأجهزة المحمولة.
Cyber Security Expert IDF-Israel Defence Forces	خبير أمن سيبراني قوات الدفاع الإسرائيلية آب/أغسطس 2012-شباط/فبراير 2017. 4 سنوات و7 أشهر

Aug 2012 Feb 2017-4 yrs 7 mos	

واليوم، إمّا جرى حلّ كلّ من شركة "سايتروكس" و"سايشارك و"سايبرلاب" و"سينتيليكسا"، أو أُعلن أنها غير نشطة، أو أُعلن عن إفلاسها. فبحسب السجلات المتاحة، لم تُسجّل "سينتيليكسا" أي إيرادات منذ العام 2021، وتم حلّها في 15 تشرين الثاني/نوفمبر 2023.[224] أما "سايتروكس"، فقد حقّقت في العام 2024 إيرادات إجمالية بلغت 5,026,000 يورو، بينما سجّلت التزامات مالية قدرها 150,486,000 يورو.[225] ولا تتوفّر معلومات واضحة عن إيرادات "سايبرلاب"، إلا أنّها لا تبدو نشطة حالياً.[226] أما "سايشارك"، فقد أعلنت في العام 2023 عن خسارة صافية بلغت 3,519,000 يورو، مع التزامات مالية تُقدّر بـ 4,986,000 يورو.[227] ومنذ ذلك الحين، أعلنت الشركة إفلاسها وحُلّت نهائياً.



[224] شركة CompanyWall Business (2019). "*سينتليكسا ذ.م.م.*"، سكوبيا. *СИНТЕЛЕКСА ДООЕЛ Скопје*.

[225] شركة CompanyWall Business (2017 ب). "*سايتروكس ذ.م.م.*"، سكوبيا. *САЈТРОКС ДООЕЛ Скопје* [متاح عبر الإنترنت] شركة CompanyWall Business متوفر على:
https://www.companywall.com.mk/kompanija/%D1%81%D0%B0%D1%98%D1%82%D1%80%D0%BE%D0%BA%D1%81-%D0%B4%D0%BE%D0%BE%D0%B5%D0%BB-%D1%81%D0%BA%D0%BE%D0%BF%D1%98%D0%B5/MMxs7WNq [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[226] شركة CompanyWall Business (2018). "*سايبر لاب ذ.م.م.*"، سكوبيا. *САЈБЕР ЛАБ ДООЕЛ Скопје*.

[227] إنّ الاعتماد على المعلومات الواردة في منصّات تجميع البيانات المالية التابعة لجهاتٍ خارجية مثل "Company Wall" يُعدّ مفيداً لفهم الصورة التقريبية للوضع المالي المرتبط بالشركات، إلّا أنّه ليس مصدراً مثالياً وقد يتضمّن بعض الأخطاء أو البيانات غير الدقيقة.

[228] شركة CompanyWall Business (2020). "*سايغنت ذ.م.م.*"، سكوبيا.

[229] سفيتكوسكا، س.، ناستيسكا، آي.، ستويانوفسكي، ب.، تيلوغلو، ت.، تريانتافيلو، إي.، وسيمونوفسكا، م. (2023). *شركة إسرائيلية طوّرت برنامج تجسس في سكوبيا بينما تجاهل المسؤولون المحليون الأمر.* (*Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way*) *مختبر الصحافة الاستقصائية في مقدونيا الشمالية (IRL).*

The Cytrox/Intellexa Alliance Corporate Structure: The Cytrox AD Structure	الهيكل المؤسسي لتحالف "سايتروكس" / "إنتلكسا": هيكل "سايتروكس ش.م.ع." (Cytrox AD)
This information is from publicly available corporate records and news reporting, as of 2022.	تستند هذه المعلومات إلى السجلات التجارية العامة والمتاحة والتقارير الإخبارية حتى عام 2022.
Tal Dilian	تال ديليان
Meir Shamir	مايير شامير
Hexatone Ltd. (formerly S.N.P. Technologies Ltd., aka Senpai Technologies)	شركة هيكساتون م.م. (Hexatone Ltd.) (اسمها السابق: شركة "إس. إن. بي تكنولوجيز م.م." S.N.P. Technologies Ltd.، المعروفة أيضاً باسم "سينباي تكنولوجيز" (Senpai Technologies)
Peterbald Ltd. (formerly Cytrox Software Ltd.)	شركة بيتربالد م.م. (Peterbald Ltd.) (اسمها السابق: شركة "سايتروكس سوفتوير م.م." Cytrox Software Ltd.)
Passitora Ltd. (formerly WS WiSpear Systems) (Dissolved)	شركة باسيتورا م.م. (Passitora Ltd.) (اسمها السابق: "دبليو إس وايسبير سيستمز" (WS WiSpear Systems (تم حلّها)
Balinese Ltd. (formerly Cytrox EMEA Ltd.)	شركة بالينيز م.م. (Balinese Ltd.) (اسمها السابق: "شركة سايتروكس م.م. في أوروبا والشرق الأوسط وأفريقيا" Cytrox EMEA Ltd.)
Cytrox Holdings ZRT (Dissolved)	سايتروكس هولدينغز ش.م.خ. (Cytrox Holdings ZRT) (تم حلّها)
Avraham Rubenstein	أبراهام روبنشتاين
Rotem Farkash	روتم فاركاش
Inpedio	إنبيديو
Cintellexa (Dissolved)	سينتيليكسا (تم حلّها)
Cyberlab (Dissolved)	سايبرلاب (تم حلّها)
Cytrox AD (Dissolved)	**سايتروكس ش.م.ع. (تم حلّها)**
Cyshark (Dissolved)	سايشارك (تم حلّها)
Cygnet	(تم حلّها)
Shahak Shalev	شاحاك شاليف
R and D director	مدير البحث والتطوير
Ivo Malinkovski	إيفو مالينكوفسكي
Moshe Farkash	موشيه فاركاش

تحالف "إنتلكسا"

في العام 2018، استحوذت شركة "دبليو إس وايسبير سيستمز المحدودة" (WS WiSpear Systems Limited) (رقم التسجيل: 318328) المملوكة لرجل الأعمال تال ديليان على شركة "سايتروكس" بمبلغٍ يقلّ عن خمسة ملايين دولار،

وضمتها في العام 2019 إلى ما يُعرف باسم تحالف "إنتلكسا".[230] [231] ويُعدّ هذا التحالف اتّحاداً يضم عدّة شركات متخصّصة في تطوير برامج التجسّس، من بينها شركتا "نيكسا تكنولوجيز" (Nexa Technologies) و"دبليو إس وايسبير سيستمز المحدودة".[232] وبحسب أبحاث أجرتها منظمة العفو الدولية، يتألّف تحالف "إنتلكسا" من مجموعتين من شركات برامج التجسّس: إحداها مجموعة "إنتلكسا" والأخرى مجموعة "نيكسا".[233] وعلى الرغم من أنّ التحالف بحدّ ذاته ليس شركةً مسجّلةً رسمياً، إلّا أنّ عدّة كيانات تحمل اسم "إنتلكسا" مسجّلة في جزر العذراء البريطانية،[234] واليونان،[235] وإيرلندا (مع تعليق تسجيل المؤسّسة اليونانية بسبب التأخّر في تقديم الملفات المالية).[236] وتشترك معظم الشركات المنضوية ضمن مجموعة "إنتلكسا" في علاقاتٍ تجاريةٍ متبادلةٍ وأسماء متشابهة. كما يستخدم بعض الباحثين والمسؤولين الحكوميين مصطلح اتحاد "إنتلكسا"، للإشارة إلى مجموعة الشركات التي تجمعها علاقات تجارية و/أو بحثية مشتركة.[237]

---

[230] بروستر، ت. (2019). *تاجر مراقبة صاحب الملايين يخرج من الظلال... وشاحنته المخصّصة لاختراق "واتساب" بقيمة 9 ملايين دولار*. (*A Multimillionaire Surveillance Dealer Steps out of the Shadows . . . and His $9 Million WhatsApp Hacking Van*). [متاح على الإنترنت] "فوربس" الشرق الأوسط. متوفر على: https://www.forbesmiddleeast.com/innovation/technology/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van [تم الاطلاع عليه في 2 آب/أغسطس 2025].

[231] وفقاً لسجلات الشركات القبرصية، جرى حلّ شركة باسيتورا م.

[232] مارزاك، ب.، سكوت-رايلتون، ج.، بردان، ك.، عبد الرزاق، ب.، ديبرت، ر.، الجيزاوي، ن.، وأنستيس، س. (2021). *"بيغاسوس" ضد "بريداتور" الاستهداف المضاعف لجهاز "الآيفون" الخاص بمعارض يكشف عن برنامج التجسس المأجور من "سايتروكس"*. [متاح على الإنترنت] "سيتيزن لاب". جامعة تورونتو. متوفر على: https://citizenlab.ca/2021/12/%D8%A8%D9%8A%D8%BA%D8%A7%D8%B3%D9%88%D8%B3-pegasus-%D8%B6%D8%AF-%D8%A8%D8%B1%D9%8A%D8%AF%D8%A7%D8%AA%D9%88%D8%B1-predator-%D8%A7%D9%84%D8%A7%D8%B3%D8%AA%D9%87%D8%AF%D8%A7%D9%81-%D8%A7%D9%84%D9%85/ [تم الاطلاع عليه في 5 آب/أغسطس 2025].

[233] منظمة العفو الدولية (2023). *ملفات "بريداتور": في أحابيل الشبكة*. [متاح على الإنترنت] *منظمة العفو الدولية*، لندن: المملكة المتحدة: منظمة العفو الدولية المحدودة. متوفر على: https://www.amnesty.org/ar/documents/act10/7246/2023/ar/

[234] دان وبراد ستريت (بدون تاريخ). *"إنتلكسا" المحدودة*. (*Intellexa Limited*.) [متاح على الإنترنت] دان وبراد ستريت. متوفر على: https://www.dnb.com/business-directory/company-profiles.intellexa_limited.2610c71eee08982e83b1dc8bb7899ea6.html [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[235] وزارة التنمية في جمهورية اليونان (2025). السجلات العامة للسجل التجاري العام في اليونان: شركة "إنتلكسا ش.م.ع." (GEMI Public Records: Entry for INTELLEXA ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ). [متاح على الإنترنت] متوفر على: https://publicity.businessportal.gr/company/154460701000 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[236] مكتب تسجيل الشركات (2025). CORE: شركة "إنتلكسا" المحدودة. (CORE: Entry for Intellexa Limited.) [متاح على الإنترنت] متوفر على: https://core.cro.ie/e-commerce/company/search/697890 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[237] روبرتس، ج.، هير، ت.، تايلور، إي.، وبانسال، ن. (2024). *أهمية الأسواق: نظرة على صناعة برامج التجسس*. (*Markets Matter: a Glance into the Spyware Industry*.).

مجموعة "إنتلكسا"

صمّم تال ديليان مجموعة "إنتلكسا" بصفتها مجموعةً من الشركات التي تُكمّل بعضها البعض من خلال منتجاتها التكنولوجية. وبدأ بناء المجموعة في العام 2018 عندما استحوذ على شركة "دبليو إس وايسبير سيستمز المحدودة" ومقرّها قبرص، والمتخصّصة في النقل غير المصرّح للبيانات الحساسة من بُعد عبر اعتراض إشارات "الواي فاي".[238] ولاحقاً، تغيّر اسم الشركة إلى "باسيتورا م.م."، ومن خلال شركة "وايسبير"، اشترى ديليان أيضاً "سايتروكس ش.م.ع." في العام نفسه. ثمّ استحوذ لاحقاً في 2018 على شركة "سينباي تكنولوجيز م.م." (رقم التسجيل: 515385748)، وهي شركة، مقرّها إسرائيل، متخصّصة في الاستخبارات مفتوحة المصدر وتحليل البيانات المسروقة عبر برامج التجسّس.[239]

تأسّست شركة "سينباي تكنولوجيز" على يد إريك بانون، وغاي ديفيد، وجوناثان لامبرت، وعمري رايتر، وروي شلومان.[240] وعلى الرغم من أنّها تُعرف وتُسوَّق باسم "سينباي تكنولوجيز"، فإنّ اسمها الرسمي وفق الترجمة الحرفية هو "إس. إن. بي. تكنولوجيز م.م." (S.N.P. Technologies Ltd.) (بالعبريّة: ס.נ.פ טכנולוגיות בע"מ). وقد تغيّر اسم الشركة مرّتين على الأقل، إذ تُعرف منذ العام 2025 باسم "هيكساتون م.م." (Hexatone Ltd.) (بالعبريّة الأصلية: האקסטון גרופ בע"מ).[241] وفي العام 2020، أضاف تال ديليان شركة "إنتلكسا إس. إيه" (Intellexa S.A.) ومقرّها اليونان، إلى شبكة الشركات التي يديرها، والتي كشفت عنها وزارة الخزانة الأميركية في العام 2024 باعتبارها الكيان الرئيسي الذي تبيع من خلاله "إنتلكسا" برنامج "بريداتور".[242]

---

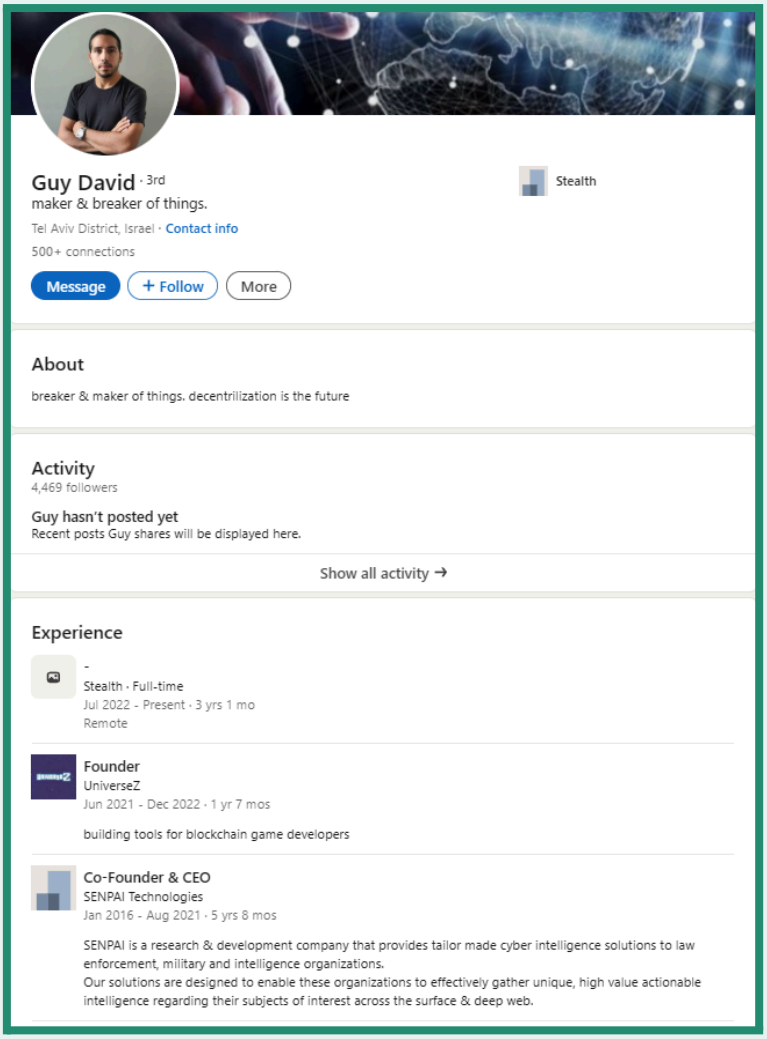
[238] روبرتس، ج.، هير، ت.، تايلور، إي.، وبانسال، ن. (2024ب). *أهمية الأسواق: نظرة على صناعة برامج التجسس* (*Markets Matter: a Glance into the Spyware Industry*).

[239] روبرتس، ج.، هير، ت.، تايلور، إي.، وبانسال، ن. (2024ب). *أهمية الأسواق: نظرة على صناعة برامج التجسس* (*Markets Matter: a Glance into the Spyware Industry*).

[240] أورباخ، م. (2019). الشركة السيبرانية، الضابط السابق، والمال المفقود (The Cyber Company, the Former Officer, and the Lost Money). *"سي تك" (CTech)*. [متاح على الإنترنت] 17 تشرين الأول/أكتوبر. متوفر على: https://www.calcalistech.com/ctech/articles/0,7340,L-3772040,00.html [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[241] "تشيك آي دي" (CheckID) (2025). *مجموعة "هاكستون م.م." / مجموعة "هيكساتون م.م." – 515385748. (HEXATONE GROUP LTD - 515385748 / Haxton Group Ltd.)*. [متاح على الإنترنت] تشيك آي دي. [متاح على الإنترنت] متوفر على: https://en.checkid.co.il/company/HEXATONE+GROUP+++LTD-g3LW9ky-515385748 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[242] وزارة الخزانة الأميركية (٢٠٢٤). *عقوبات وزارة الخزانة على أعضاء اتحاد "إنتلكسا" لبرامج التجسس التجارية* (*Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium*). [متاح على الإنترنت] متوفر على: https://home.treasury.gov/news/press-releases/jy2155 [تم الاطلاع عليه في 10 آب/أغسطس 2025].



الصورة 12: غاي ديفيد، أحد مؤسّسي شركة "سينباي تكنولوجيز"، يصف تجربته في الشركة على موقع "لينكد إن". ويبدو أنّه المؤسّس الوحيد الذي يذكر علانيةً عمله مع "سينباي تكنولوجيز".[243]

Guy David	غاي ديفيد
3rd	زملاء من الدرجة الثالثة
maker & breaker of things.	
Tel Aviv District, Israel Contact Info	صانع الأشياء ومحطّمها
Stealth	منطقة تل أبيب، إسرائيل
500+ connections	"ستيلث" (Stealth)
Message	أكثر من 500 صلة
+Follow	إرسال رسالة

[243] ديفيد، غ. (2025). صفحة *غاي ديفيد الشخصية*. (*Guy David's profile page*.) [لينكد إن]. [تم الاطلاع عليه في 10 آب/أغسطس 2025]. متوفر على: https://www.linkedin.com/in/guy-david-5a99a731/

More	+متابعة المزيد
About breaker & maker of things, decentrilization is the future	نبذة: صانع الأشياء ومحطّمها، اللامركزيّة هي مستقبل العالم.
Activity 4,489 followers Guy hasn't posted yet Recent posts Guy shares will be displayed here Show all activity	النشاط 4,469 متابعاً لم ينشر غاي ديفيد أي منشورات بعد. سيُعرض هنا أحدث ما يشاركه من منشورات. عرض كل النشاط
Stealth Full-time Jul 2022 - Present. 3 yrs 1 mo Remote	**الخبرة** شركة "ستيلث" - دوام كامل تموز/يوليو 2022 – حتى الآن. 3 سنوات وشهر العمل من بُعد
Founder UniverseZ Jun 2021 - Dec 2022. 1 yr 7 mos building tools for blockchain game developers	المؤسّس شركة "يونيفيرس ز" (UniverseZ) تموز/يونيو 2021 – كانون الأول/ديسمبر 2022. عام وسبعة أشهر العمل على تطوير أدوات لمطوّري ألعاب سلسلة الكتل.
Co-Founder & CEO SENPAI Technologies Jan 2016 - Aug 2021-5 yrs 8 mos SENPAI is a research & development company that provides tailor made cyber intelligence solutions to law enforcement, military and intelligence organizations. solutions to Our solution's are designed to enable these organizations to effectively gather unique, high value actionable intelligence regarding their subjects of interest across the surface & deep web.	الشريك المؤسس والرئيس التنفيذي "سينباي تكنولوجيز" كانون الثاني/يناير 2016 – آب/أغسطس 2021 (5 سنوات و8 أشهر) "سينباي تكنولوجيز" شركة بحث وتطوير متخصّصة في تقديم حلول في مجال الاستخبارات السيبرانية ومصمّمة خصيصاً لأجهزة إنفاذ القانون، والجيش، وأجهزة الاستخبارات. تهدف حلولنا إلى تمكين هذه الجهات من جمع معلومات استخباراتية فريدة وذات قيمة عالية وقابلة للتنفيذ حول الأهداف المعنية، عبر الويب السطحي والويب العميق.

تغيّر هيكل ملكية "إنتلكسا": من "أليادا" إلى "ثالستريس"

في العام 2020، نُقلت جميع أسهم شركة "بالينيز م.م." (المعروفة سابقاً بـ"سايتروكس أوروبا والشرق الأوسط وأفريقيا")، والمملوكة من "سايتروكس هولدينغز ش.م.خ." إلى مجموعة "أليادا" (Aliada Group)، وهي كيانٌ تجاريٌّ مسجَّل في جزر العذراء البريطانية (رقم التسجيل: 1926732).[244] وتُعتبر "أليادا" على ما يبدو المالك الرئيسي لشركة "بالينيز".[245] ومع حلّ "سايتروكس هولدينغز ش.م.خ."، أصبح تال ديليان المالك الوحيد لشركة "بيتربالد" (المعروفة سابقاً بـ"سايتروكس سوفتوير").[246] وحصلت مجموعة "أليادا" على تمويلٍ من شركة الاستثمار الخاص "ميفتاش-شامير هولدينغز م.م." (Mivtach-Shamir Holdings Ltd.، بالعبرية: מבטח שמיר אחזקות בע"מ)، التي أسّسها مايير شامير، أحد المؤسّسين الأساسيين لـ"سايتروكس ش.م.ع." في مقدونيا الشمالية.[247] [248] وتُدرج شركة "ميفتاش-شامير" (رقم التسجيل: 520034125) في بورصة تل أبيب (رمز التداول: "ميش" Mish).[249] وفي العام 2020، رفع أفي روبنشتاين، أحد مؤسّسي شركة "سايتروكس"، دعوى قضائية ضدّ تال ديليان أمام محكمة المقاطعة في تل أبيب، اتّهمه فيها هو ومايير شامير بتخفيف حصّته من الأسهم عبر شبكة معقّدة من الشركات الخارجية.[250] وقبل حلّ "سايتروكس ش.م.ع."، كانت ملكيّتها مشتركةً بين "سايتروكس هولدينغز ش.م.خ." و"بالينيز م.م." و"بيتربالد م.م.".[251]

وفي العام 2017، أفاد موقع "إنتلجنس أونلاين" بأنّ "أليادا" كانت المالك الفعلي لشركة "دبليو إس وايسبير سيستمز المحدودة"، وهي التي اشترت "سايتروكس ش.م.ع.".[252] وفي العام 2020، اشترت "مجموعة مايروس للتطوير" (Miros

---

[244] مارزاك، ب.، سكوت-رايلتون، ج.، بردان، ك.، عبد الرزاق، ب.، ديبرت، ر.، الجيزاوي، ن.، وأنستيس، س. (2021). *"ليغاسوس" ضد "بريداتور" الاستهداف المضاعف لجهاز "الآيفون" الخاص بمعارض يكشف عن برنامج التجسس المأجور من "سايتروكس"*.

[245] "تشيك آي دي" (CheckID) (2025). *"بالينيز م.م." – 515692135. (BALINESE LTD – 515692135)* [متاح على الإنترنت] تشيك آي دي. متوفر على: https://en.checkid.co.il/company/BALINESE++LTD-P02VO4w-515692135 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[246] "تشيك آي دي" (CheckIDج) (2025). *"بيتربالد م.م." – 515693893. (PETERBALD LTD - 515693893.)* [متاح على الإنترنت] تشيك آي دي. متوفر على: https://en.checkid.co.il/company/PETERBALD++LTD-rMeDN2x-515693893 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[247] "كرانشبيس" (Crunchbase) (2024). *"ميفتاش شامير هولدينغز م.م." - كرانش بيس نبذة عن الشركة والتمويل. (Mivtach Shamir Holdings LTD - Crunchbase Company Profile & Funding.)* [متاح على الإنترنت] كرانشبيس. متوفر على: https://www.crunchbase.com/organization/mivtach-shamir-holdings-ltd [تم الاطلاع عليه في 27 آب/أغسطس 2025].

[248] "إنتلجنس أونلاين" (Intelligence Onlineب) (2017). مع وايسبير، بطل اعتراض شبكات GSM تال ديليان يدخل مجال الواي فاي. (With WiSpear, GSM Interception Champion Tal Dilian Gets into WiFi.). *إنتلجنس أونلاين*. [متاح على الإنترنت] 20 أيلول/سبتمبر. متوفر على:
https://www.intelligenceonline.com/surveillance--interception/2017/09/20/with-wispear-gsm-interception-champion-tal-dilian-gets-into-wifi,108262318-art [تم الاطلاع عليه في 28 حزيران/يونيو 2025].

[249] "ستوك أناليسيس" (StockAnalysis). (2025). *"ميفتاش-شامير هولدينغز". (Mivtach Shamir Holdings)* [متاح على الإنترنت] متوفر على: https://stockanalysis.com/quote/tlv/MISH/ [تم الاطلاع عليه في 27 تموز/يوليو 2025].

[250] ساديه، س. (2020). عبقري استخبارات إسرائيلي غامض، وشاحنة تجسس إلكتروني، وصفقات بملايين الدولارات. (A Shady Israeli Intel Genius, His Cyber-spy Van and Million-dollar Deals.) *هآرتس*. [متاح على الإنترنت] 31 كانون الأول/ديسمبر. متوفر على:
https://www.haaretz.com/israel-news/tech-news/2020-12-31/ty-article-magazine/.highlight/a-shady-israeli-intel-genius-his-cyber-spy-van-and-million-dollar-deals/0000017f-f21e-d497-a1ff-f29ed7c30000 [تم الاطلاع عليه في 27 آب/أغسطس 2025].

[251] روبرتس، ج.، هير، ت.، تايلور، إي.، وبانسال، ن. (2024). *أهمية الأسواق: نظرة على صناعة برامج التجسس. (Markets Matter: a Glance into the Spyware Industry.)*.

[252] "إنتلجنس أونلاين" (Intelligence Onlineب) (2017). مع وايسبير، بطل اعتراض شبكات GSM تال ديليان يدخل مجال الواي فاي. (With WiSpear, GSM Interception Champion Tal Dilian Gets into WiFi.).

(Development Group Inc شرة "دبليو إس وايسبير سيستمز المحدودة"،[253] ثمّ اشترت شركة "ثالستريس" المحدودة (Thalestris Limited) المسجّلة في إيرلندا، والتي ترأسها سارة حمو زوجة تال ديليان السابقة، مجموعة "مايروس" للتطوير.[254] [255]

أما اليوم، فتُعدّ "مايروس" شركةً فرعيةً، تمتلك "ميفتاش-شامير هولدينغز م.م." 45% من أسهمها.[256] ووفقاً للتقرير السنوي للشركة الصادر في آذار/مارس 2025، فإنّ "مايروس" تمتلك أسهماً في شركة "ثالستريس" المحدودة. وفي العام 2020، حصلت "مايروس" على 10% من أسهم "ثالستريس" مقابل نقل جميع أصول مجموعة "أليادا" والتزاماتها التي كانت قد استحوذت عليها في وقتٍ سابق من ذلك العام.[257] وبحسب وزارة الخزانة الأميركية، تمتلك شركة "ثالستريس" حقوق توزيع برنامج "بريداتور".[258]

الشركات التابعة لـ"ثالستريس"

وفقاً للبيانات المالية الصادرة عن شركة "ثالستريس" لعام 2021، استحوذت الشركة على عددٍ من الشركات التابعة من خلال استحواذها على أصول مجموعة "أليادا".[259] ففي 3 شباط/فبراير 2021، تأسّست شركة "إلبيدينا م.م." (Elpidina Ltd.) في إيرلندا (رقم التسجيل: 687102)، ثم أُلحقت لاحقاً بـ"ثالستريس". وأدرجت "ثالستريس" شركة "إلبيدينا" في وثائقها المالية كشركة "خاملة".[260] كما تأسّست شركة "إنتلكسا م.م." (رقم التسجيل: 665443)، بصفتها "شركة موزّعة للتقنيّات" في إيرلندا عام 2019.[261] وفي الفترة نفسها، استحوذت "ثالستريس" أيضاً على شركتي "هيرميس تكنولوجيز

---

[253] شارياتيس، م. (2022). استنتاجات حزبَيْ سيريزا وباسوك بشأن التنصّت: فضيحة وتستّر في آنٍ واحد. (*Τα Πορίσματα ΣΥΡΙΖΑ - ΠΑΣΟΚ Για Τις υποκλοπές: Και Σκάνδαλο Και Συγκάλυψη*). [متاح على الإنترنت] آي إيديسيس (iEidiseis). متوفر على: https://web.archive.org/web/20221010203948/https://www.ieidiseis.gr/politiki/167144/ta-porismata-syriza-pas-ok-gia-tis-ypoklopes-kai-skandalo-kai-sygkalypsi [تم الاطلاع عليه في 24 آب/أغسطس 2025].

[254] شارياتيس، م. (2022). استنتاجات حزبَيْ سيريزا وباسوك بشأن التنصّت: فضيحة وتستّر في آنٍ واحد. (*Τα Πορίσματα ΣΥΡΙΖΑ - ΠΑΣΟΚ Για Τις υποκλοπές: Και Σκάνδαλο Και Συγκάλυψη*).

[255] روبرتس، ج.، هير، ت.، تايلور، إي.، وبانسال، ن. (2024). *أهمية الأسواق: نظرة على صناعة برامج التجسس*. (*Markets Matter: a Glance into the Spyware Industry*).

[256] "ميفتاش-شامير هولدينغز م.م." (2024). "*ميفتاش-شامير هولدينغز م.م.": التقرير السنوي لعام 2024*. (*Mivtach-Shamir Hodings Ltd.: Annual Report for 2024*) [متاح على الإنترنت] ص 81. متوفر على: https://msgroup.co.il/wp-content/uploads/2025/03/%D7%93%D7%95%D7%97-%D7%AA%D7%A7%D7%95%D7%A4%D7%AA%D7%99-%D7%95%D7%A9%D7%A0%D7%AA%D7%99-%D7%9C%D7%A9%D7%A0%D7%AA-2024-merged-6.pdf .

[257] "ميفتاش-شامير هولدينغز م.م." (2024). "*ميفتاش-شامير هولدينغز م.م.": التقرير السنوي لعام 2024*. (*Mivtach-Shamir Hodings Ltd.: Annual Report for 2024*) [متاح على الإنترنت] ص 179.

[258] وزارة الخزانة الأميركية (2024). *عقوبات وزارة الخزانة على أعضاء اتحاد "إنتلكسا" لبرامج التجسس التجارية*. (*Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium*).

[259] "ثالستريس م.م." (2022). *التقرير السنوي والبيانات المالية المجمعة للسنة المنتهية في 31 كانون الأول/ديسمبر 2021*. (*Annual Report and Consolidated Financial Statements for the Year Ended 31 December 2021*).

[260] باور، ج. (2023). *ما هي "إنتلكسا"، شركة برامج التجسس الأيرلندية المُدرجة على "القائمة السوداء" الأميركية؟* (*Who Are Intellexa, the Irish Spyware Company Placed on a US 'blacklist'?*) [متاح على الإنترنت] صحيفة "آيريش تايمز". متوفر على: https://www.irishtimes.com/technology/2023/07/19/who-are-intellexa-the-irish-spyware-company-placed-on-a-us-blacklist/ [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[261] باور، ج. (2023). *من هي "إنتلكسا"، شركة برامج التجسس الأيرلندية المُدرجة على "القائمة السوداء" الأميركية؟* (*Who Are Intellexa, the Irish Spyware Company Placed on a US 'blacklist'?*)

ش.م." (Hermes Technologies S.A) (رقم التسجيل: 154461601000)[262] و"أبولو تكنولوجيز ش.م" (Apollo Technologies S.A) (رقم التسجيل: 154460301000) المسجلتين في اليونان.[263] وقد تأسّست الشركتان في 11 آذار/مارس 2020، إلّا أنّ تسجيلهما بقي معلّقاً حتى العام 2025. وتصف "ثالستريس" كلّاً من "أبولو" و"هيرميس" بأنّهما تعملان في "تصميم تكنولوجيا المعلومات وتطويرها لتطبيقاتٍ مختلفة".[264]

كما استحوذت "ثالستريس" من مجموعة "أليادا" على شركتَيْ "نورول م.م."[265] (Nurul Ltd.) (رقم التسجيل: 405667) و"ميسترونا م.م."[266] (Mistrona Ltd.) (رقم التسجيل: 405562) في قبرص.[267] وأفادت شركة "نورول" في بيانها المالي الصادر في العام 2024 أنّ رصيدها الدائن بلغ 9,863 يورو لدى شركة "ثالستريس سويسرا ش.م." (Thalestris Switzerland SA) (رقم التسجيل: 1437847)،[268] التي حُلّت في 28 آذار/مارس 2024.[269] وتُظهر آخر الملفات المالية المتاحة لشركة "ميسترونا" لعام 2021 وجود علاقة "مالية" مبهمة مع "ثالستريس" (في إيرلندا)، وعلاقة تجارية مع شركة "إنتلكسا" المحدودة (في جزر العذراء البريطانية). ويبدو اليوم أنّ المساهم الوحيد في "ميسترونا" هو شركة "إنتلكسا" المحدودة (في إيرلندا).[270] كما تُظهر سجلات كلٍّ من شركتي "نورول" و"ميسترونا" أنّ باناغيوتا كارولي تشغل منصب المدير، فيما تُشير سجلات "نورول" إلى أنّها المساهم الوحيد فيها.[271] [272] وفي 16 أيلول/سبتمبر 2024، فرضت وزارة

---

[262] وزارة التنمية في جمهورية اليونان (2025). السجلات العامة للسجل التجاري العام في اليونان: شركة "هيرميس تكنولوجيز ش.م." (GEMI Public Records: Entry for INTELLEXA ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ). [متاح على الإنترنت] متوفر على: https://publicity.businessportal.gr/company/154461601000 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[263] وزارة التنمية في جمهورية اليونان (2025). السجلات العامة للسجل التجاري العام في اليونان: شركة "أبولو تكنولوجيز" (GEMI Public Records: Entry for APOLLO TECHNOLOGIES ΜΟΝΟΠΡΟΣΩΠΗ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ.). [متاح على الإنترنت] متوفر على: https://publicity.businessportal.gr/company/154460301000 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[264] "ثالستريس م.م." (2022). *التقرير السنوي والبيانات المالية المجمعة للسنة المنتهية في 31 كانون الأول/ديسمبر 2021*. (*Annual Report and Consolidated Financial Statements for the Year Ended 31 December 2021*) دبلن، إيرلندا: مكتب تسجيل الشركات (CORE)، ص 29.

[265] "نورول م.م." (2024). تفاصيل تسجيل شركة "نورول م.م.". (Registration Details for Nurul Ltd.) [متاح على الإنترنت] متوفر على: https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=dernova+limited&number=%25&searchtype=optStartMatch&index=1&tname=%25&sc=0 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[266] "ميسترونا م.م." (2023). تفاصيل تسجيل شركة "ميسترونا م.م.". (Registration Details for Mistrona Ltd.) [متاح على الإنترنت] متوفر على: https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=mistrona&number=%25&searchtype=optStartMatch&index=1&tname=%25&sc=0 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[267] ذكرت شركة "ثالستريس" في بيانها المالي لعام 2021 أنّ شركة "نورول" (التي كانت تُعرف سابقاً بـ"ديرنوفا") هي شركة "خاملة"، كما أشارت إلى أنّ شركة "ميسترونا" تعمل في "تطوير برامج الحوسبة السحابية وترخيصها".

[268] إلياديس، ك. (2024). *البيانات المالية للفترة من 1 كانون الثاني/يناير 2024 إلى 31 آب/أغسطس 2024*. (*Financial Statements Period (from 1 January 2024 to 31 August 2024*) نيقوسيا، قبرص: شركة نورول م.م. ، ص 11.

[269] "ثالستريس" (سويسرا) ش.م. (2024). تفاصيل تسجيل شركة "ثالستريس" (سويسرا) ش.م. ع. [متاح على الإنترنت] متوفر على: https://traderegistry.ch/company-search/ [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[270] "بليفور م.م." (2021). *البيانات المالية للسنة المنتهية في 31 كانون الأول/ديسمبر 2021*. (*Financial Statements Year ended 31 December 2021*.) نيقوسيا، قبرص: شركة "نورول م.م."، ص 24.

[271] "نورول م.م." (2025). *التفاصيل التنظيمية*. (*Organizational Details*) [متاح على الإنترنت] إدارة تسجيل الشركات والمستلم الرسمي، قبرص، ص 2.

[272] "ميسترونا م.م." (2025). *التفاصيل التنظيمية*. (*Organizational Details*) [متاح على الإنترنت] إدارة تسجيل الشركات والمستلم الرسمي، قبرص، ص 2.

الخزانة الأميركية عقوباتٍ على باناغيوتا كارولي لدورها في إدارة "عدّة كيانات ضمن اتحاد إنتلكسا، التي تخضع لسيطرة شركة ثالستريس م.م. أو تُعدّ تابعةً لها".[273]

إذاً، حافظت شركة "ثالستريس" على ملكيّتها الكاملة لمعظم الشركات التابعة لـ"إنتلكسا" في قبرص واليونان، باستثناء شركة "إنتلكسا ش.م." في اليونان، التي امتلكت 65% منها، وفقاً لأحدث البيانات المالية الصادرة عن "ثالستريس". وتشير التقارير إلى أنّ تال ديليان باع النسبة المتبقية البالغة 35% من الشركة إلى فيليكس بيتزيوس، الذي يُعتقد أنّه أحد الوسطاء العاملين لصالح ديليان عبر شركة "سانتينومو م.م." (Santinomo Limited) في قبرص (رقم التسجيل: 402203).[274] [275] وفي وقتٍ لاحق، فرضت وزارة الخزانة الأميركية على بيتزيوس عقوبات في 16 أيلول/سبتمبر 2024.[276]

وتختلف التقارير العامة بشأن تحديد ملكيّة شركة "إنتلكسا ش.م."، إذ أفاد المجلس الأطلسي في العام 2024 بأنّ ملكيّة الشركة تعود إلى "إنتلكسا المحدودة" في جزر العذراء البريطانية و"إنتلكسا م.م." في إيرلندا.[277] في المقابل، أشارت وسائل إعلام استقصائية، مثل "لايتهاوس ريبورتس" (Lighthouse Reports) و"هآرتس" (Haaretz) و"إنسايد ستوري" (Inside Story) و"سولومون" (Solomon) منذ العام 2022 وحتى آذار/مارس 2025 إلى أنّ ملكيّة الشركة موزّعة بين بيتزيوس و"ثالستريس".[278] [279] ولم يتمكّن معدّو هذا التقرير من التحقّق من الهيكل الكامل لملكيّة شركة "إنتلكسا ش.م." عبر السجلات الرسمية.

وأشارت "ثالستريس" أيضاً إلى أنّها كانت تمتلك شركة "إنتلكسا سولوشنز م.م." (Intellexa Solutions Ltd.) في جزر العذراء البريطانية منذ العام 2021، لكنها وصفت دورها بـ"الخامل" ضمن هيكل الكيان.[280] وأفادت بأنّ عدد موظّفيها بلغ 26 موظّفاً حتّى نهاية العام 2021.[281]

وتُظهر بيانات "ثالستريس" المالية لعام 2021 لمحةً عن الإيرادات التي حقّقتها المجموعة، إذ سجّلت إيراداتٍ بلغت 34,362,408 يورو في العام 2021، وأرباحاً إجمالية قدرها 29,260,165 يورو. **وتجدر الإشارة إلى أنّه عند تحليل**

---

[273] وزارة الخزانة الأميركية. (2024أ). *وزارة الخزانة تفرض عقوبات على ميسّري اتحاد "إنتلكسا" لبرامج التجسس التجارية*. (*Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium*.) [متاح على الإنترنت] متوفر على:
https://home.treasury.gov/news/press-releases/jy2581 [تم الاطلاع عليه في 20 آب/أغسطس 2025].

[274] تيلوغلو، ت.، تريانتافيلو، إ.، بلاك، ك.، بنجاكوب، ع.، شارف، أ.، ستاتيوس، ت.، جايغر، غ.، فاس ديكن، ك.، ديب، ب.، سابوش، ج.، هاودن، د.، غيبس، م. وفاول، ل. (2022). *رحلة المفترس (Flight of the Predator)*. [متاح على الإنترنت] تقارير "لايتهاوس". متوفر على:
https://www.lighthousereports.com/investigation/flight-of-the-predator/

[275] " سانتينومو م.م." (2024). تفاصيل تسجيل شركة "سانتينومو" المحدودة. (Registration Details for Santinomo Limited) [متاح على الإنترنت] متوفر على:
https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=Santinomo&number=%25&searchtype=optStartMatch&index=1&tname=%25&sc=0 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[276] وزارة الخزانة الأميركية. (2024أ). *وزارة الخزانة تفرض عقوبات على ميسّري اتحاد "إنتلكسا" لبرامج التجسس التجارية*. (*Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium*.)

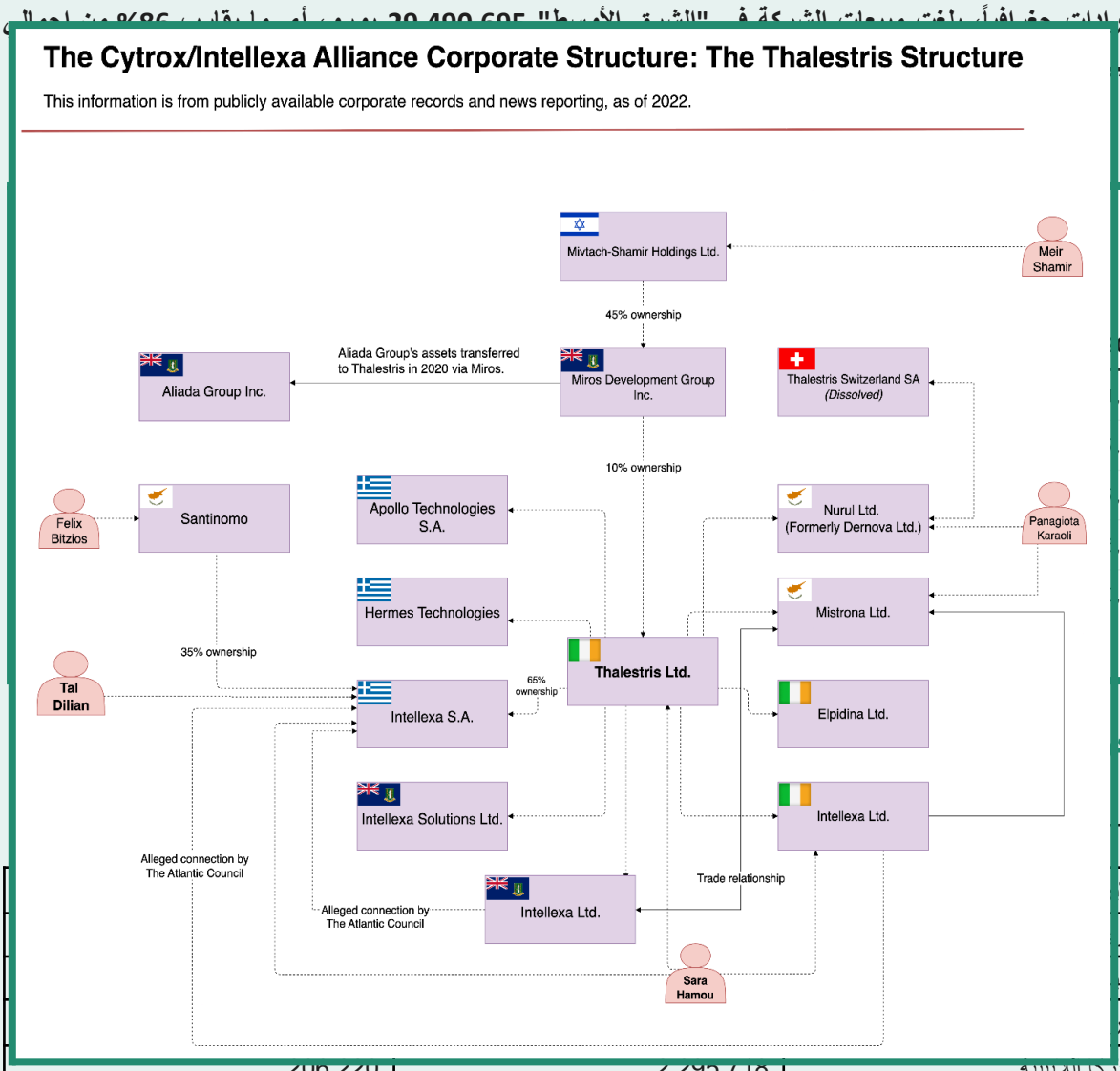
[277] روبرتس، ج.، هير، ت.، تايلور، إي.، وبانسال، ن. (2024). *أهمية الأسواق: نظرة على صناعة برامج التجسس*. (*Markets Matter: a Glance into the Spyware Industry*.)

[278] تيلوغلو، ت.، تريانتافيلو، إ.، بلاك، ك.، بنجاكوب، ع.، شارف، أ.، ستاتيوس، ت.، جايغر، غ.، فاس ديكن، ك.، ديب، ب.، سابوش، ج.، هاودن، د.، غيبس، م. وفاول، ل. (2022). *رحلة المفترس (Flight of the Predator)*.

[279] مارانغوداكي، د. وتريانتافيلو، إ. (2025). *التنصّت: الفصل الأخير من عملية التغطية*. (*Interceptions: the Last Act of a Cover*) [متاح على الإنترنت] متوفر على: https://wearesolomon.com/el/mag/format-el/reportaz/ypoklopes-i-teleftaia-praxi-mias-sygkalipsis/ [تم الاطلاع عليه في 21 أيلول/سبتمبر 2025].

[280] " ثالستريس م.م." (2022). *التقرير السنوي والبيانات المالية المجمعة للسنة المنتهية في 31 كانون الأول/ديسمبر 2021*. (*Annual Report and Consolidated Financial Statements for the Year Ended 31 December 2021*.) [متاح على الإنترنت] مكتب تسجيل الشركات، جمهورية إيرلندا، ص 29.

[281] "ثالستريس م.م." (2022). *التقرير السنوي والبيانات المالية المجمعة للسنة المنتهية في 31 كانون الأول/ديسمبر 2021*. (*Annual Report and Consolidated Financial Statements for the Year Ended 31 December 2021*.)، ص 23.



أميركا الشمالية	2,295,718	206,220
الشرق الأوسط	11,229,050	29,490,695

الجدول: "سمكس" – المصدر: "سمكس" - أُعدّ الجدول باستخدام Datawrapper

[282] "ثالستريس م.م." (2022). *التقرير السنوي والبيانات المالية المجمعة للسنة المنتهية في 31 كانون الأول/ديسمبر 2021*. (*Annual Report and Consolidated Financial Statements for the Year Ended 31 December 2021*)، ص 22.

الصورة 13: الهيكل المؤسسي لشركة "ثالستريس".

The Cytrox/Intellexa Alliance Corporate Structure: The Thalestris Structure	الهيكل المؤسسي لتحالف سايتروكس / إنتلكسا: هيكل شركة ثالستريس
This information is from publicly available corporate records and news reporting, as of 2022.	تستند هذه المعلومات إلى سجلات الشركات المتاحة والتقارير الإخبارية، اعتباراً من العام 2022
Felix Bitzios	فيلكس بيتزيوس
Tal Dilian	تال ديليان
AliadaGroup inc.	مجموعة أليادا
Santinomo	سانتينومو
35% ownership	35% من الملكية
Alleged connection by The Atlantic council	ارتباطٌ مزعوم من المجلس الأطلسي
Aliada Group's assets transferred to Thalestris in 2020 via Miros	نُقلت أصول مجموعة أليادا إلى شركة ثالستريس في العام 2020 عبر مايروس
Apollo Technologies S.A.	أبولو تكنولوجيز ش.م.
Hermes technologies	هيرميس تكنولوجيز
Intellexa S.A.	إنتلكسا ش.م.
Intellexa Solutions Ltd.	إنتلكسا سولوشنز م.م.
Alleged connection by The Atlantic Council	ارتباطٌ مزعوم من المجلس الأطلسي
Mivtach-Shamir Holdings Ltd.	ميفتاش-شامير هولدينغز م.م.
45% ownership	45% من الملكية
Miros Development Group Inc.	مجموعة مايروس للتطوير
10% ownership	10% من الملكية
Thalestris Ltd.	ثالستريس ش.م
65% ownership	65% من الملكية

Intellexa Ltd.	إنتلكسا م.م.
Sara Hamou	سارة حمو
Thalestris Switzerland SA (dissolved)	ثالستريس سويسرا ش.م (تمّ حلّها)
Nurul Ltd. (formerly Dernova Ltd.)	نورول المحدودة (المعروفة سابقاً بشركة "ديرنوفا م.م." Dernova Ltd.)
Mistrona Ltd.	ميسترونا م.م.
Elpidina Ltd.	إلبيدينا م.م.
Intellexa Ltd.	إنتلكسا م.م.
Trade relationship	علاقة تجارية
Meir Shamir	مايير شامير
Panagiota Karaoli	باناغيوتا كارولي

هيكل تحالف "إنتلكسا"

أُعلن عن تحالف "إنتلكسا" في العام 2019 كشراكة بين الشركات المنضوية ضمن مجموعتي "إنتلكسا" و"نيكسا".[283] وتُظهر نسخةٌ أرشيفيةٌ من موقع Intellexa[.]com بتاريخ 14 تشرين الأول/أكتوبر 2019، أنّ "إنتلكسا" عرّفت "نيكسا تكنولوجيز"، و"ويسبيير"، و"سايتروكس"، و"سينباي تكنولوجيز" بصفتهم أعضاءها المؤسّسين.[284] ولا تُعدّ مجموعة "نيكسا" كياناً قانونياً رسمياً، لكنها تتكوّن، وفقاً للتقارير، من عدّة شركات، من بينها: شركة "آر بي 42" (RB 42، المعروفة سابقاً بـ"نيكسا تكنولوجيز")، ومقرّها فرنسا؛ شركة "سيتكو تكنولوجي سولوشنز م.م." (Secto Technology Solutions Ltd.)، المعروفة سابقاً بـ"نيكسا تكنولوجيز" التشيكية ذ.م.م.، ومقرّها جمهورية التشيك (وتخضع حالياً للتصفية[285])؛

شركة الأنظمة المتقدمة للشرق الأوسط (المنطقة الحرة) ذ.م.م. (Advanced Middle East Systems FZ llc)، المعروفة اختصاراً بـ"AMES"، ومقرّها الإمارات العربية المتحدة؛ شركة "سيربيكوم" (Serpikom) في فرنسا؛ شركة "دي إف سيستمز" (المنطقة الحرة) ذ.م.م. (DF Systems FZ-LLC، المعروفة سابقاً بـ"تروفيكور" (المنطقة الحرة) ذ.م.م. Trovicot FZ-LLC، التي أصبحت جزءاً من مجموعة شركات أعيدت تسميتها إلى "داتا فيوجن سيستمز" Datafusion Systems)، ومقرّها الإمارات؛ "بوس إندستريز" ش.م.ب. (Boss Industries SAS) في فرنسا، وهي الشركة الأمّ والمستثمر الرئيسي للمجموعة (رقم التسجيل: 853 120 541).[286]

تأسست شركة "نيكسا تكنولوجيز" (رقم التسجيل: 751 230 681) في فرنسا في العام 2013 بهدف الاستحواذ على منتج المراقبة الشهير "إيغل" (Eagle) الذي كانت تطوّره شركة "أميسيس" (Amesys) الفرنسية لتقنيات المراقبة، بعد أن اشترتها "مجموعة بول ش.م.ع." (Bull Group SA) في العام 2010 (ثمّ أصبح المنتج يُعرف لاحقاً بـ"سيريبرو" (Cerebro) تحت إدارة "نيكسا"). كما أُنشئت "شركة نيكسا تكنولوجيز" التشيكية عام 2015 (رقم التسجيل: 04654951)

---

[283] "نيكسا تكنولوجيز" (2019). تحالف "إنتلكسا". (*Intellexa Alliance*.) [متاح على الإنترنت] "نيكسا تكنولوجيز". متوفر على: https://web.archive.org/web/20200109072024/https:/www.nexatech.fr/intellexa-alliance-press-news [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[284] "إنتلكسا" *(2019). "إنتلكسا" | تحالف الاستخبارات. (Intellexa | the Intelligence Alliance)* [متاح على الإنترنت] متوفر على: https://web.archive.org/web/20191014000753/https://intellexa.com/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[285] كورزي (2015) (Kurzy.cz). *شركة "سيتكو" لحلول التكنولوجيا ذ.م.م. في حالة التصفية - السجل التجاري، نسخة كاملة | كورزي.س.ز. (Setco Technology Solutions s.r.o. V Likvidaci - Obchodní rejstřík, Úplný Výpis | Kurzy.cz*.) [متاح على الإنترنت] كورزي. متوفر على: https://rejstrik-firem.kurzy.cz/rejstrik-firem/DO-04654951-setco-technology-solutions-sro-v-likvidaci/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[286] منظمة العفو الدولية (2023). *ملفات "بريداتور": في أحابيل الشبكة*. [متاح على الإنترنت] *منظمة العفو الدولية*، لندن: المملكة المتحدة: منظمة العفو الدولية م. متوفر على: https://www.amnesty.org/ar/wp-content/uploads/sites/9/2023/10/ACT1072462023ARABIC.pdf

لمتابعة أنشطة البحث والتطوير.[287] أما شركة الأنظمة المتقدمة للشرق الأوسط (المنطقة الحرة) ذ.م.م. (رقم التسجيل: 21063)، فقد تأسست في الإمارات لبيع منتجات "نيكسا تكنولوجيز"، ويُعتقد أنّها استُخدمت أيضاً للتحايل على قيود التصدير في الاتحاد الأوروبي.[288] وفي العام 2019، استحوذت "بوس إندستريز ش.م.ب." على شركة "تروفيكور سولوشنز (المنطقة الحرة) ذ.م.م." (Trovicor Solutions FZ-LLC) (رقم التسجيل: 91646)، المتخصّصة في تطوير تقنيات الاعتراض.[289] وتشير ملاحظات المجلس الأطلسي إلى أنّ شركة "سيربيكوم" انضمّت إلى هذا الهيكل بعد العام 2019 (رقم التسجيل: 492 531 371).[290] وتجدر الإشارة إلى امتلاك شركات مجموعة "نيكسا" تاريخاً مؤسسياً معقّداً وسلسلة من تغييرات الأسماء، ما يجعل تتبّع تاريخها الكامل خارج نطاق هذا التقرير.[291]

ويرى المجلس الأطلسي أنّ حلول مراقبة الأجهزة والبرمجيات التي طوّرتها وسوّقتها وباعتها شركات مجموعة "نيكسا" قد تُكمّل منتجات برامج التجسّس التابعة لمجموعة "إنتلكسا"، وخصوصاً برنامج "سيريبرو" (Cerebro) المخصّص للمراقبة الشاملة.[292] ووفقاً لتقرير صادر عن منظمة العفو الدولية في 5 تشرين الأول/أكتوبر 2023، فإنّ

"المساهمين الرئيسيين والمديرين التنفيذيين السابقين لمجموعة نيكسا" يدّعون أنّ تحالف "إنتلكسا" لم يعد موجوداً.[293]

---

[287] روبرتس، ج.، هير، ت.، تايلور، إي.، وبانسال، ن. (2024). *أهمية الأسواق: نظرة على صناعة برامج التجسس*. (*Markets Matter: a Glance into the Spyware Industry*).

[288] بيكر، س.، بوشمان، ر.، هوبنشتيدت، م.، نابر، ن.، وروزنباخ، م. (2023). *ملفات بريداتور: اتحاد برامج التجسس الأوروبي يزوّد الطغاة والدكتاتوريين*. (*The Predator Files: European Spyware Consortium Supplied Despots and Dictators*) [متاح على الإنترنت] دير شبيغل. متوفر على:
https://www.spiegel.de/international/business/the-predator-files-european-spyware-consortium-supplied-despots-and-dictators-a-2fd8043f-c5c1-4b05-b5a6-e8f8b9949978 [تم الاطلاع عليه في 29 آب/أغسطس 2025].

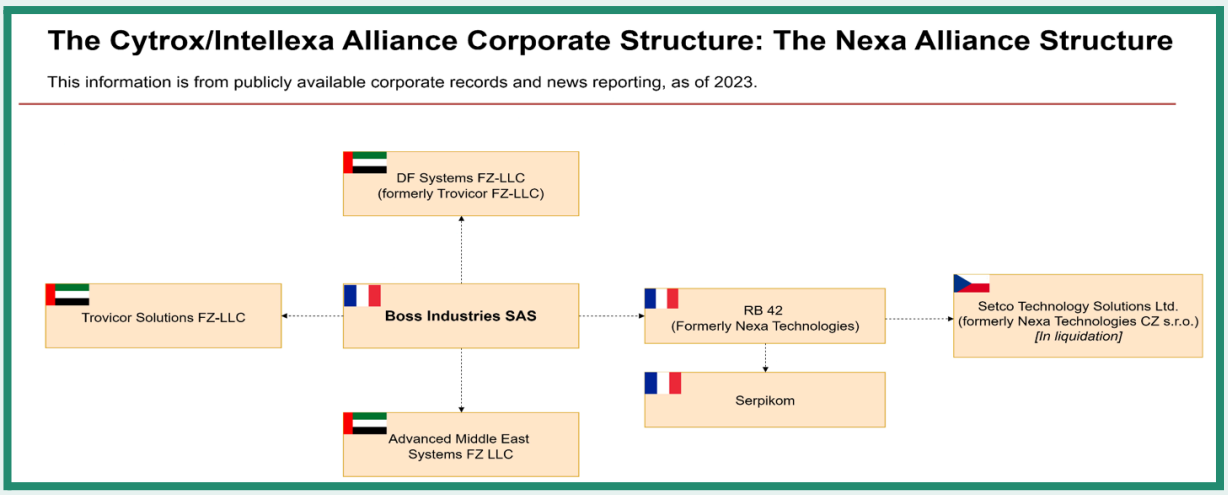
[289] كليرفيلد. (2019). *كليرفيلد تقدّم استشارة لشركة "بوس إندستريز" بشأن الاستحواذ على شركة "تروفيكور – كليرفيلد" في دبي*. (*Clairfield Advises Boss Industries on the Acquisition of the Dubai-based Company Trovicor -Clairfield*.) [متاح على الإنترنت] متوفر على:
https://www.clairfield.com/transaction/clairfield-advises-boss-industries-on-the-acquisition-of-the-dubai-based-company-trovicor/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[290] روبرتس، ج.، هير، ت.، تايلور، إي.، وبانسال، ن. (2024). *أهمية الأسواق: نظرة على صناعة برامج التجسس*. (*Markets Matter: a Glance into the Spyware Industry*).

[291] روبرتس، ج.، هير، ت.، تايلور، إي.، وبانسال، ن. (2024). *أهمية الأسواق: نظرة على صناعة برامج التجسس*. (*Markets Matter: a Glance into the Spyware Industry*).

[292] روبرتس، ج.، هير، ت.، تايلور، إي.، وبانسال، ن. (2024). *أهمية الأسواق: نظرة على صناعة برامج التجسس*. (*Markets Matter: a Glance into the Spyware Industry*).

[293] التعاون التحقيقي الأوروبي (EIC) ومختبر الأمن التابع لمنظمة العفو الدولية (2023). *عالمياً: فضيحة تجسس 'ملفات بريداتور' تكشف عن استهداف صارخ للمجتمع المدني والسياسيين والمسؤولين*. [متاح على الإنترنت] *منظمة العفو الدولية*. متوفر على:
https://www.amnesty.org/ar/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].



الصورة 13: الهيكل المؤسسي لتحالف "نيكسا".

The Cytrox/Intellexa Alliance Corporate Structure: The Nexa Alliance Structure	الهيكل المؤسسي لتحالف سايتروكس/إنتلكسا: هيكل تحالف نيكسا
This information is from publicly available corporate records and news reporting, as of 2023.	تستند هذه المعلومات إلى سجلات الشركات المتاحة والتقارير الإخبارية، اعتباراً من العام 2023.
Trovicor Solutions FZ-LLC	تروفيكور سولوشنز (المنطقة الحرة) ذ.م.م.
DF Systems FZ-LLC (formerly Trovicor FZ-LLC)	"دي إف سيستمز" (المنطقة الحرة) ذ.م.م (المعروفة سابقاً بتروفيكور (المنطقة الحرة)) ذ.م.م.)
Boss Industries SAS	بوس إندستريز ش.م.ب.
Advanced Middle East Systems FZ LLC	شركة الأنظمة المتقدمة للشرق الأوسط (المنطقة الحرة) ذ.م.م.
RB 42 (Formerly Nexa Technologies)	آر بي 42 (المعروفة بنيكسا تكنولوجيز)
Serpikom	سيربيكوم
Setco Technology Solutions Ltd. (formerly Nexa Technologies CZ sro.) [In liquidation]	سيتكو تكنولوجي سولوشنز م.م. (المعروفة سابقاً بنيكسا تكنولوجيز التشيكية ذ.م.م) (تخضع للتصفية)

الشبكة التشيكية

في العام 2024، كشف صحافيون استقصائيون تشيكيّون من موقع Investigate[.]cz عن شبكة جديدة من الكيانات التشيكية يُعتقد أنّها قدّمت دعماً لتحالف "إنتلكسا" في مجالات التسويق والاستشارات والخدمات التقنية. وكان دفير حوريف حزان، وهو صاحب مطعم تشيكي يتمتّع بخلفية في البرمجة، يملك ما لا يقلّ عن أربع شركات في التشيك يُرجّح أنّها تعاونت مع "إنتلكسا".[294]

[294] شوتوفا، ز. و ماي، ب. (2024). صانع السحر: لماذا يعمل صاحب مطعم تشيكي لصالح شركة "إنتلكسا"؟ (*The Magic Maker: Why Is a Czech Bistro Owner Working for Intellexa?*) - موقع *VSquare.org*. [متاح على الإنترنت] موقع VSquare.org. متوفر على: https://vsquare.org/greece-czech-republic-intellexa-cytrox-spyware/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

وقد تلقّت ثلاثٌ من شركاته - "هاداستك ذ.م.م." (Hadastech s.r.o)[295] و"زامبرانو تريد ذ.م.م." (Zambrano Trade s.r.o)[296] و"شيلو ذ.م.م." (Shilo s.r.o.)[297] - مدفوعاتٍ إجمالية بلغت 2.9 مليون يورو بين عامَيْ 2020 و2023 من شركات تابعة لـ"إنتلكسا". ويبدو أنّ "هاداستك" طلبت 40 شحنة من "معدات الشبكات" وهواتف من شركة أوكرانية لم يُفصح عن اسمها لصالح "إنتلكسا"، كما استضافت شركة "شيلو" عنوان بروتوكول الإنترنت الخاص بموقع "إنتلكسا".[298] وجرت تصفية الشركات الثلاث — "هاداستك" (رقم التسجيل: 08980683) و"زامبرانو تريد" (رقم التسجيل: 08629773) و"شيلو" (رقم التسجيل: 10764186) — أو تخضع حالياً لذلك. أما شركة حزان الرابعة المرتبطة بـ"إنتلكسا"، وهي "بيندر وان ذ.م.م." (BenderOne s.r.o.)، فما زالت نشطة حتى اليوم (رقم التسجيل: 06627951)،[299] وتقع في المبنى نفسه الذي تشغله شركة تشيكية أخرى مملوكة لصديقٍ مقرّب من حزان تُدعى "فوكس آي تك ذ.م.م." (FoxITech s.r.o.) ويملكها ميخائيل إيكونوميديس (رقم التسجيل: 14243873).[300] ووفقاً لتقرير صادر عن مجموعة "إنسيكت غروب"، تستضيف شركة "فوكس آي تك" بنيةً تحتية للشبكة المرتبطة ببرنامج التجسّس "بريداتور".[301] ومن غير المعلوم أيٌّ من كيانات "إنتلكسا" قد سدّد المبالغ لحزان مقابل خدماته.

---

[295] كورزي (2024) (Kurzy.cz). *شركة "هاداستك ذ.م.م." في حالة التصفية، كرنوف، رقم الشركة 08980683 – السجل التجاري للشركات. (Setco Technology Solutions s.r.o. V Likvidaci - Hadastech s.r.o. v likvidaci, Krnov IČO 08980683 - Obchodní rejstřík firem*.) [متاح على الإنترنت] كورزي. متوفر على: https://rejstrik-firem.kurzy.cz/08980683/hadastech-s-r-o-v-likvidaci/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[296] كورزي (2024) (Kurzy.cz). *شركة "زامبرانو ذ.م.م." في حالة التصفية، كرنوف، رقم الشركة 08629773– السجل التجاري للشركات. (ZAMBRANO trade s.r.o. v likvidaci , Krnov IČO 08629773 - Obchodní rejstřík firem)* [متاح على الإنترنت] كورزي. متوفر على: https://rejstrik-firem.kurzy.cz/08629773/zambrano-trade-s-r-o-v-likvidaci/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

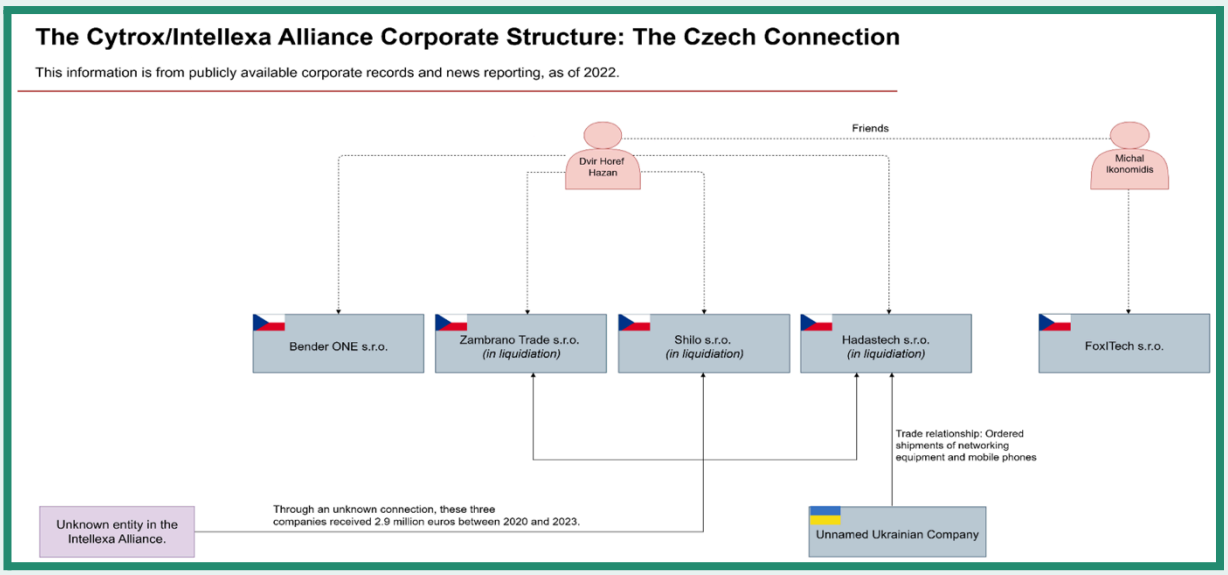
[297] كورزي (2024) (Kurzy.cz). *شركة "شيلو ذ.م.م." في حالة التصفية، كرنوف، رقم الشركة 10764186– السجل التجاري للشركات. (Shilo s.r.o. v likvidaci, Krnov IČO 10764186 - Obchodní rejstřík firem)* [متاح على الإنترنت] كورزي. متوفر على: http://rejstrik-firem.kurzy.cz/10764186/shilo-s-r-o-v-likvidaci/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[298] شوتوفا، ز. و ماي، ب. (2024). صانع السحر: لماذا يعمل صاحب مطعم تشيكي لصالح شركة "إنتلكسا"؟ (*The Magic Maker: Why Is a Czech Bistro Owner Working for Intellexa?*)

[299] كورزي (2024) (Kurzy.cz). *شركة "بيندر وان ذ.م.م."، كرنوف، رقم الشركة 06627951 – السجل التجاري للشركات. (BENDER ONE s.r.o. , Krnov IČO 06627951)* [متاح على الإنترنت] كورزي. متوفر على: https://rejstrik-firem.kurzy.cz/06627951/bender-one-sro/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[300] كورزي (2024) (Kurzy.cz). *شركة" فوكس آي تك ذ.م.م."، كرنوف، رقم الشركة 14243873 – السجل التجاري للشركات. (FoxITech s.r.o. Krnov IČO 14243873 - Obchodní rejstřík firem* .,) [متاح على الإنترنت] كورزي. متوفر على: https://rejstrik-firem.kurzy.cz/14243873/foxitech-sro/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[301] إنسيكت غروب" (2025أ)، *لا يزال "بريداتور" نشطاً، مع تحديد عميل جديد وروابط شركات جديدة. (Predator Still Active, with New Client and Corporate Links Identified*.) [متاح على الإنترنت] "ريكوردد فيوتشير". (Recorded Future.). "ريكوردد فيوتشير". متوفر على: https://www.recordedfuture.com/research/predator-still-active-new-links-identified [تم الاطلاع عليه في 29 آب/أغسطس 2025].



الصورة 14: الهيكل المؤسسي لتحالف "نيكسا"

The Cytrox/Intellexa Alliance Corporate Structure: The Czech Connection	الهيكل المؤسسي لتحالف سايتروكس/إنتلكسا: الشبكة التشيكية
This information is from publicly available corporate records and news reporting, as of 2022.	تستند هذه المعلومات إلى سجلات الشركات المتاحة والتقارير الإخبارية، اعتباراً من العام 2022.
Dvir Horef Hazan	دفير حوريف حزان
Friends	أصدقاء
Michal Ikonomidis	ميخائيل إيكونوميديس
BenderOne s.r.o.	بيندر وان ذ.م.م.
Zambrano Trade s.r.o	زامبرانو تريد ذ.م.م.
Shilo s.r.o. (in liquidation)	شيلو ذ.م.م.
Hadastech s.r.o (in liquidation)	هاداستك ذ.م.م.
FoxITech s.r.o.	فوكس آي تك ذ.م.م
Unknown entity in the Intellexa Alliance	كيان مجهول في اتّحاد إنتلكسا
Through an unknown connection, these three companies received 2.9 million euros between 2020 and 2023.	من خلال صلة غير معروفة، تلقّت هذه الشركات الثلاث 2.9 مليون يورو بين عامي 2020 و2023.
Trade relationship: Ordered shipments of networking equipment and mobile phones	العلاقة التجارية: طلب شحنات من معدات الشبكات والهواتف المحمولة
Unnamed Ukranian Company	شركة أوكرانية لم يُكشف عن اسمها

في نهاية المطاف، يبقى حجم نشاط مجموعة "إنتلكسا" أو تحالفها في العام 2025 غير مؤكّد. وتشير سجلات التسجيل التجاري إلى أنّ عدداً من الكيانات المُدرجة ضمن مجموعة "إنتلكسا" ومجموعة "نيكسا" (اللتين شكّلتا معاً تحالف "إنتلكسا") ما زال نشطاً حتى منتصف العام 2025.[302]

إسرائيل

- باليونيز م.م.[303]
- بيتربالد م.م.[304]
- سينباي تكنولوجيز م.م.[305]

فرنسا

- آر بي 42 [306]
- بوس إندستريز ش.م.ب[307]
- سيربيكوم[308]

إيرلندا

- ثالستريس المحدودة[309]
- إنتلكسا المحدودة[310]
- إلبيدينا المحدودة[311]
-

---

[302] لا تُعدّ هذه القائمة شاملة، بل تُجسّد ما تمكّنت "سمكس" من الحصول عليه حتى تاريخ إعداد هذا التقرير. ولم تتمكّن "سمكس" من التحقّق من الوضع القانوني لتسجيل بعض الكيانات التجارية الواقعة ضمن ولايات قضائية يصعب الحصول على وثائق منها، مثل مجموعة "مايروس" للتطوير و"إنتلكسا؛ المحدودة و"إنتلكسا سولوشنز" المحدودة في جزر العذراء البريطانية.

[303] "تشيك آي دي" (CheckID) (2025). *"باليونيز م.م." – 515692135*. (*BALINESE LTD - 515692135*.)

[304] "تشيك آي دي" (CheckIDج) (2025). *"بيتربالد م.م." – 515693893*. (*PETERBALD LTD – 515693893*)

[305] "تشيك آي دي" (CheckID) (2025). مجموعة *"هيكساتون م.م." / مجموعة "هيكساتون م.م." – 515385748*. (*Haxton Group Ltd. /HEXATONE GROUP LTD - 515385748*.)

[306] المعهد الوطني للملكية الصناعية (2024). سجل الشركات الفرنسي: "آر بي 42" – نظام SIREN 751 230 681. (French Companies Register: RB 42 - SIREN 751 230 681.) [متاح على الإنترنت] متوفر على:
https://data.inpi.fr/entreprises/751230681?q=RB%2042#751230681 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[307] المعهد الوطني للملكية الصناعية (2024). سجل الشركات الفرنسي: "بوس إندستريز" – نظام SIREN 853 120 541. (French Companies Register: BOSS INDUSTRIES - SIREN 853 120 541.) [متاح على الإنترنت] متوفر على:
https://data.inpi.fr/entreprises/853120541?q=Boss%20industries#853120541 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[308] المعهد الوطني للملكية الصناعية (2024). سجل الشركات الفرنسي: "سيربيكوم" – نظام SIREN 492 531 371. (French Companies Register: SERPIKOM - SIREN 492 531 371.) [متاح على الإنترنت] متوفر على:
https://data.inpi.fr/entreprises/492531371?q=Serpikom#492531371 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[309] سجل التجارة الأيرلندي (2023). بحث عن شركة: "ثاليستريس" المحدودة – 661545 [متاح على الإنترنت] متوفر على:
https://traderegistry.ie/company-search/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[310] سجل التجارة الأيرلندي (2023). بحث عن شركة: "إنتلكسا" المحدودة – 665443 [متاح على الإنترنت] متوفر على:
https://traderegistry.ie/company-search/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[311] سجل التجارة الأيرلندي (2023). بحث عن شركة: "إلبيدينا" المحدودة – 687102 [متاح على الإنترنت] متوفر على:
https://traderegistry.ie/company-search/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

اليونان

- أبولو[312]
- هيرميس[313]
- إنتلكسا ش.م.ع.[314] (تسجيلها معلّق)

قبرص

- نورول م.م.[315]
- ميسترونا م.م.[316]

جزر العذراء البريطانية

- مجموعة أليادا[317]

الإمارات العربية المتحدة

- شركة الأنظمة المتقدمة للشرق الأوسط[318]
- تروفيكور سولوشنز (المنطقة الحرة) ذ.م.م.[319]
- دي إف سيستمز (المنطقة الحرة) ذ.م.م.[320]

في نهاية المطاف، تستند معرفتنا بالتحالف إلى التسريبات والتصريحات العلنية والمواد الترويجية، غير أنّه لا تتوافر أدلّة عامة حديثة تشير إلى أنّ الشركات المرتبطة بتحالف "إنتلكسا" ما زالت تتعاون في مشاريع بيع مشتركة. وعلى الرغم من أنّ كثيراً من هذه الكيانات الخاضعة لـ"ثالستريس" لا تزال نشطة من الناحية القانونية، إلا أنّ حجم ممارستها لأنشطة تجارية فعلية في العام 2025 ما زال غير واضح.

---

[312] وزارة التنمية في جمهورية اليونان (2025). السجلات العامة للسجل التجاري العام في اليونان: شركة "أبولو تكنولوجيز" (GEMI Public Records: Entry for GEMI Public Records: Entry for APOLLO TECHNOLOGIES ΜΟΝΟΠΡΟΣΩΠΗ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ).

[313] وزارة التنمية في جمهورية اليونان (2025). السجلات العامة للسجل التجاري العام في اليونان: شركة "هيرميس تكنولوجيز ش.م." (GEMI Public Records: Entry for INTELLEXA ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ).

[314] وزارة التنمية في جمهورية اليونان (2025). السجلات العامة للسجل التجاري العام في اليونان: "شركة إنتلكسا ش.م.ع." (GEMI Public Records: Entry for INTELLEXA ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ).

[315] "نورول م.م." (2024). تفاصيل تسجيل شركة "نورول م.م.". (Registration Details for Nurul Ltd.)

[316] "ميسترونا م.م." (2023). تفاصيل تسجيل شركة "ميسترونا م.م.". (Registration Details for Mistrona Ltd.)

[317] "أوبن سانكشينز" (OpenSanctions). (2025). مجموعة *"أليادا"* (*Aliada Group Inc*). [متاح على الإنترنت] متوفر على: https://www.opensanctions.org/entities/NK-fMNGjhDzoCeprF53r9hapr/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[318] السجل الاقتصادي الوطني للإمارات العربية المتحدة (2025). تفاصيل رخصة العمل: الأنظمة المتقدمة للشرق الأوسط. [متاح على الإنترنت] متوفر على: https://ner.economy.ae/Search_By_BN.aspx [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[319] السجل الاقتصادي الوطني للإمارات العربية المتحدة (2025). تفاصيل رخصة العمل: "تروفيكور سولوشنز" (المنطقة الحرة) [متاح على الإنترنت] متوفر على: https://ner.economy.ae/Search_By_BN.aspx [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[320] السجل الاقتصادي الوطني للإمارات العربية المتحدة (2025). تفاصيل رخصة العمل: "دي إف سيستمز" (المنطقة الحرة) ذ.م.م.

تغيير ملكيّة برنامج "بريداتور"

في العام 2023، وفي إطار التحقيق في "ملفّات بريداتور" الذي أجرته منظمة العفو الدولية، أفاد موقع "دير شبيغل" بأنّ شركة AMES كانت الكيان الرسمي الذي باعت من خلاله شركة "إنتلكسا" برنامج "بريداتور" لمصر وفيتنام في نهاية العام 2020.[321]

وفي 5 آذار/مارس 2024، فرض مكتب مراقبة الأصول الأجنبية التابع لوزارة الخزانة الأميركية عقوبات رسمية على عددٍ من الأفراد والكيانات المرتبطة بتحالف "إنتلكسا"، من بينهم تال ديليان، وسارة حمو، و"إنتلكسا ش.م.ع."، و"إنتلكسا المحدودة"، و"سايتروكس ش.م.ع."، و"سايتروكس هولدينغز ش.م.خ."، و"ثالستريس المحدودة".[322] [323] ومع ذلك، وعلى الرغم من تزايد المعارضة ضدّ برنامج "بريداتور" ومطوّريه، إلّا أنه في الواقع ما زال قيد الاستخدام.

ففي 1 آذار/مارس 2024، نشرت مجموعة "إنسيكت غروب" (Insikt Group) التابعة لشركة "ريكوردد فيوتشر" (Recorded Future) تقريراً رصدت فيه أدلّة تؤكّد تشغيل برنامج "بريداتور" في عدّة دول خلال الأشهر الاثني عشر السابقة، من بينها مصر وعُمان والسعودية.[324] وفي 12 حزيران/يونيو 2025، نشرت المجموعة تقريراً آخر أشارت فيه إلى أنّها حدّدت بنية تحتية جديدة مرتبطة بمشغّلي "بريداتور".[325] وعلى الرغم من أنّ الكيانات التابعة لشركة "سايتروكس" التي أُنشئت في المجر ومقدونيا الشمالية تبدو غير نشطة اليوم، إلا أنّ مجموعة "إنتلكسا" نفسها هي التي تتولّى إنتاج برنامج "بريداتور" حالياً.[326]

وترتبط أنشطة "إنتلكسا" في منطقة غرب آسيا وشمال أفريقيا، شأنها شأن مجموعة "إن إس أو"، ارتباطاً كبيراً بوجودها وعلاقاتها التجارية في إسرائيل. كما كان لتحالف "إنتلكسا" حضورٌ مؤسّسيٌّ في الإمارات العربية المتحدة من خلال "شركة الأنظمة المتقدمة للشرق الأوسط" وكيانات "تروفيكور"/"داتا فيوجن سيستمز"، وجميعها ما زالت نشطة حتى وقت إعداد هذا التقرير. وتشير البيانات المستقاة من التقارير العامّة إلى أنّ ما لا يقلّ عن أربع دولٍ في المنطقة قد استخدمت برنامج "بريداتور".

---

[321] بيكر، س.، بوشمان، ر.، هوبنشتيدت، م.، نابر، ن.، وروزنباخ، م. (2023). *ملفات "بريداتور": اتحاد برامج التجسس الأوروبي يزوّد الطغاة والدكتاتوريين*. (*The Predator Files: European Spyware Consortium Supplied Despots and Dictators*)

[322] وزارة الخزانة الأميركية (2024). *عقوبات وزارة الخزانة على أعضاء اتحاد "إنتلكسا" لبرامج التجسس التجارية*. (*Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium*).

[323] وفقاً لوزارة الخزانة الأميركية، تصدّر "إنتلكسا ش.م.ع." أدوات المراقبة التابعة لتحالف "إنتلكسا" إلى "الأنظمة الاستبدادية"، وتعيد الشركة اليونانية "إنتلكسا" المحدودة بيع التكنولوجيا للتحالف وتحافظ على أصوله. كما تطوّر "سايتروكس ش.م.ع."، برنامج "بريداتور"، وقد ساهمت "سايتروكس ش.م.خ." في تطوير البرنامج، بينما تعمل "ثالستريس" كشركة قابضة لـ"إنتلكسا". وفي 18 تموز/يوليو، فرضت وزارة الخزانة عقوبات على "سايتروكس ش.م.ع."، و"سايتروكس هولدينغز ش.م.خ."، و"إنتلكسا" المحدودة، و"إنتلكسا ش.م.ع."، لكنها أزالت لاحقاً صفحتها الخاصة بالعقوبات.

[324] "إنسيكت غروب" (2024)، *مشغلو برامج التجسس "بريداتور" يعيدون بناء البنية التحتية متعددة المستويات لاستهداف الأجهزة المحمولة*. (*Predator Spyware Operators Rebuild Multi-Tier Infrastructure to Target Mobile Devices*.) [متاح على الإنترنت] "ريكوردد فيوتشير". (Recorded Future). متوفر على:
https://www.recordedfuture.com/research/predator-spyware-operators-rebuild-multi-tier-infrastructure-target-mobile-devices ied [تم الاطلاع عليه في 13 آب/أغسطس 2025].

[325] "إنسيكت غروب" (2025)، *لا يزال "بريداتور" نشطاً، مع تحديد عميل جديد وروابط شركات جديدة*. (*Predator Still Active, with New Client and Corporate Links Identified*.)

[326] التعاون الإستقصائي الأوروبي (EIC) ومختبر الأمن التابع لمنظمة العفو الدولية (2023). *عالمياً: تحقيق 'ملفات بريداتور' يكشف عن تقاعس كارثي عن تنظيم تجارة تكنولوجيات المراقبة*.

التسويق: "الطرف الصالح"

على عكس مجموعة "إن إس أو"، لا تسعى مجموعة "إنتلكسا" إلى تسويق أعمالها بنشاطٍ على وسائل التواصل الاجتماعي – وكذلك الأمر بالنسبة لشركة "سايتروكس" عندما كانت نشطة. غير أنّ التصريحات العلنية التي أدلى بها تحالف "إنتلكسا" وقادته تقدّم نظرةً مهمّةً حول أسلوب تصوير منتجاتهم.[327]

ففي نسخةٍ من موقع "إنتلكسا" تعود إلى العام 2019، جرى تقديم التحالف باعتباره يزوّد "أجهزة إنفاذ القانون والاستخبارات بمحفظةٍ شاملةٍ من حلول الاستخبارات الممتازة والرائدة".[328] أما نسخة الموقع في العام 2021، فقد ركّزت على تسويق "الاعتراض التكتيكي".[329] وعلى مرّ السنوات، يقدّم الموقع وموادّه التسويقية الشركة بأنّ "مقرّها الاتحاد الأوروبي وتخضع للتنظيم القانوني فيه".[330] [331]

ووفقاً لتقريرٍ صادرٍ عن منظمة العفو الدولية في العام 2023 حول تحالف "إنتلكسا"، أفاد مديرون تنفيذيون سابقون في شركة "نيكسا" للباحثين بأنّ جميع "العلاقات التجارية" كانت تقوم على "الامتثال الكامل للوائح المعمول بها"، مؤكدين أنّ جميع تعاملات مجموعة "نيكسا" تخضع وفقاً لقوانين الاتحاد الأوروبي.[332] غير أنّ الكيانات التابعة لمجموعة "إنتلكسا" صدّرت برنامج "بريداتور" إلى عددٍ من الدول التي استخدمته في ارتكاب انتهاكات لحقوق الإنسان، من بينها السودان.[333]

كما يعرض الحساب الرسمي لـ"إنتلكسا" على منصة "لينكد إن"، الذي لا يرتبط صراحةً بأيّ كيانٍ محدّدٍ تابعٍ للتحالف أو المجموعة، أنشطته في سياق ما يسمّيه "سباقاً رقمياً" بين أجهزة إنفاذ القانون والمجرمين الذين يستغلّون "الانتشار الواسع لعمليات التشفير".

---

[327] سفيتكوسكا، س.، ناستيسكا، آي.، ستويانوفسكي، ب.، تيلوغلو، ت.، تريانتافيلو، إي.، وسيمونوفسكا، م. (2023). *شركة إسرائيلية طوّرت برنامج تجسس في سكوبيا بينما تجاهل المسؤولون المحليون الأمر.* (*Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way*) مختبر الصحافة الاستقصائية في مقدونيا الشمالية *(IRL)*.

[328] "إنتلكسا" *(2019). "إنتلكسا"| تحالف الاستخبارات. (Intellexa | the Intelligence Alliance).*

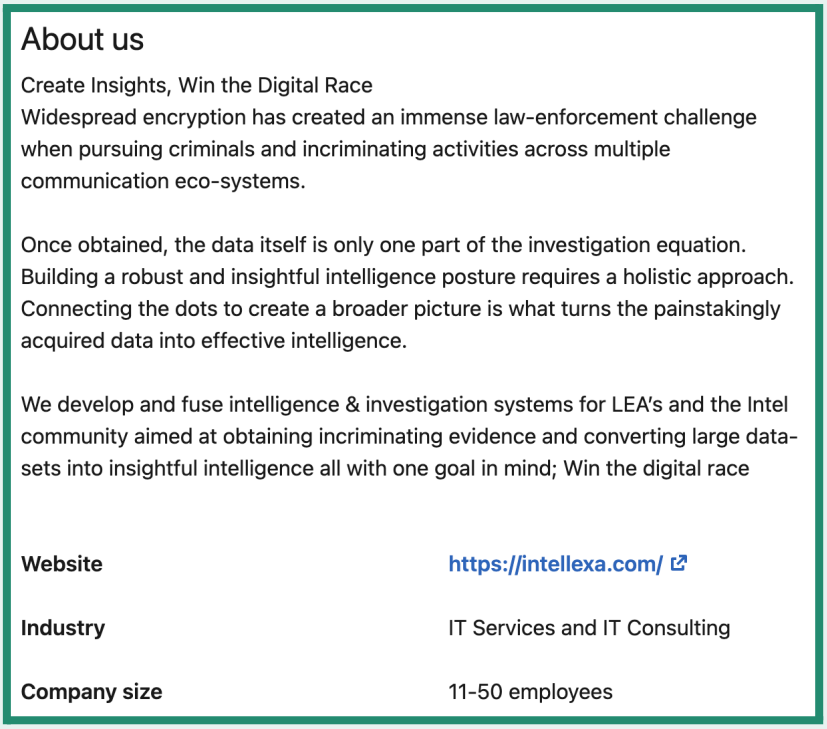
[329] مارزاك، ب.، سكوت-رايلتون، ج.، بردان، ك.، عبد الرزاق، ب.، ديبرت، ر.، الجيزاوي، ن.، وأنستيس، س. (2021). *"بيغاسوس" ضد "بريداتور" الاستهداف المضاعف لجهاز "الآيفون" الخاص بمعارض يكشف عن برنامج التجسس المأجور من "سايتروكس".*

[330] مارزاك، ب.، سكوت-رايلتون، ج.، بردان، ك.، عبد الرزاق، ب.، ديبرت، ر.، الجيزاوي، ن.، وأنستيس، س. (2021). *"بيغاسوس" ضد "بريداتور" الاستهداف المضاعف لجهاز "الآيفون" الخاص بمعارض يكشف عن برنامج التجسس المأجور من "سايتروكس".*

[331] فوكس، م. (2023). "إنتلكسا": استخدام برنامج تجسس مرتبط بإيرلندا في "اعتداء سافر" - تقرير. *بي بي سي.* (Intellexa: Irish-linked Spyware Used in 'brazen attacks' - Report. *BBC*) [متاح على الإنترنت] 21 تشرين الأول/أكتوبر. متوفر على: https://www.bbc.com/news/articles/c0wxr9rnnxeo [تم الاطلاع عليه في 3 آب/أغسطس 2025].

[332] التعاون الإستقصائي الأوروبي (EIC) ومختبر الأمن التابع لمنظمة العفو الدولية (2023). *عالمياً: تحقيق 'ملفات بريداتور' يكشف عن تقاعس كارثي عن تنظيم تجارة تكنولوجيات المراقبة.*

[333] " د. لاب" (Dr Lab) (2022). السودان: برنامج تجسّس مصدره الاتحاد الأوروبي بين أيدي "رجال بلا رحمة". "سمكس". متوفر على: https://smex.org/ar/%d8%a7%d9%84%d8%b3%d9%88%d8%af%d8%a7%d9%86-%d8%a8%d8%b1%d9%86%d8%a7%d9%85%d8%ac-%d8%aa%d8%ac%d8%b3%d9%91%d8%b3-%d8%a7%d9%84%d8%a7%d8%aa%d8%ad%d8%a7%d8%af-%d8%a7%d9%84%d8%a3%d9%88%d8%b1%d9%88%d8%a8/ [تم الاطلاع عليه في 17 تموز/يوليو 2025].



About us

Create Insights, Win the Digital Race
Widespread encryption has created an immense law-enforcement challenge when pursuing criminals and incriminating activities across multiple communication eco-systems.

Once obtained, the data itself is only one part of the investigation equation. Building a robust and insightful intelligence posture requires a holistic approach. Connecting the dots to create a broader picture is what turns the painstakingly acquired data into effective intelligence.

We develop and fuse intelligence & investigation systems for LEA's and the Intel community aimed at obtaining incriminating evidence and converting large data-sets into insightful intelligence all with one goal in mind; Win the digital race

Website	https://intellexa.com/
Industry	IT Services and IT Consulting
Company size	11-50 employees

الصورة 16: يصف حساب "إنتلكسا" على "لينكد إن" عمله بأنه يقدّم معلومات استخباراتية معمّقة لأجهزة إنفاذ القانون ومجتمع الاستخبارات.[334]

من نحن ابتكر الرؤى، واربح السباق الرقمي أدّى الانتشار الواسع لعمليات التشفير إلى إيجاد تحدٍّ كبيرٍ أمام أجهزة إنفاذ القانون في ملاحقة المجرمين والسلوكيات الإجرامية عبر أنظمة اتصالات متعدّدة. وبعد الحصول على البيانات، فإنّها لا تمثّل سوى جزءٍ واحدٍ من معادلة التحقيق. إذ يتطلّب بناء منظومة استخباراتية قوية وقادرة على تقديم رؤى تحليلية نهجاً شمولياً. فربط النقاط وتجميع الصورة الأوسع هو ما يحوّل البيانات التي جُمعت بصعوبة إلى معلومات استخباراتية فعّالة. وبالتالي، نسعى إلى تطوير أنظمة الاستخبارات والتحقيق ودمجها لصالح أجهزة إنفاذ القانون ومجتمع الاستخبارات، بهدف الحصول على دليل إدانة وتحويل مجموعات البيانات الضخمة إلى معلومات استخباراتية ذات قيمة، وكل ذلك لهدفٍ واحد، وهو الفوز بالسباق الرقمي.	About us Create Insights, Win the Digital Race Widespread encryption has created an immense law-enforcement challenge when pursuing criminals and incriminating activities across multiple communication eco-systems. Once obtained, the data itself is only one part of the investigation equation. Building a robust and insightful intelligence posture requires a holistic approach. Connecting the dots to create a broader picture is what turns the painstakingly acquired data into effective intelligence. We develop and fuse intelligence & investigation systems for LEA's and the intel community aimed at obtaining incriminating evidence and converting large data-sets into insightful intelligence all with one goal in mind; Win the digital race
الموقع الإلكتروني https://intellexa.com/	Website https://intellexa.com/

[334] "إنتلكسا" (2025). صفحة *"نبذة عن إنتلكسا"*. (*Intellexa's About page*.) [لينكد إن]. [تم الاطلاع عليه في 11 آب/أغسطس 2025]. متوفر على: https://www.linkedin.com/company/intellexa/about/

القطاع خدمات تكنولوجيا المعلومات والاستشارات	Industry IT Services and IT Consulting
حجم الشركة من 11 إلى 50 موظفاً	Company size 11-50 employees

في 6 آب/أغسطس 2019، نشرت مجلة "فوربس" مقابلةً إيجابيةً مع تال ديليان، قدّمت فيها وصفاً تفصيلياً لقدرات "الشاحنة المخصّصة لاختراق واتساب التي صمّمها بقيمة 9 ملايين دولار".[335] ووفقاً للمجلة، تُظهر "هذه الشاحنة" القدرات التي كان يمتلكها تحالف "إنتلكسا" الناشئ آنذاك. وقد صوّرت "فوربس" ديليان على أنّه "نسخة أكثر إهمالاً وأكثر شعراً من جورج كلوني"، لكنها أشارت إلى أنّ "إنتلكسا" كانت "تروّج لحقبة جديدة من الانفتاح" في سوق المراقبة السيبرانية التجارية وأنّها أنشأت "ترسانة سيبرانية شاملة لتكون بمثابة مركز خدمات موحّد لعناصر الشرطة في الميدان".

وكما هي الحال مع مجموعة "إن إس أو"، تُظهر تصريحات ديليان أنّه يسوّق "إنتلكسا" على أنّها شركة لا تتعامل إلّا مع "الطرف الصالح". فقد صرّح في مقابلته مع "فوربس" بأنّه صمّم منتجاته لمراقبة أسوأ المجرمين. وعندما سألته المجلة عن انتهاكات حقوق الإنسان المرتبطة بتطوير برامج التجسّس، تجاهل ديليان هذه المخاوف، قائلاً: **"لسنا شرطة العالم... نحن نعمل مع الطرف الصالح. وأحياناً لا يتصرّف الطرف الصالح كما يجب".**[336] وأكّد أنّ حماية الفئات الضعيفة من الانتهاكات هي مسؤولية الحكومات التي تنظّم بيع برامج التجسّس واستخدامها، وليست مسؤولية الشركات التي تطوّرها. وبعبارةٍ أخرى، عندما يسيء الطرف الصالح التصرّف (من خلال استغلال برامج التجسّس وانتهاك حقوق الإنسان)، فهذه ليست مشكلة الشركات المنتجة. وختم ديليان قائلاً: "الكون يحتاج إلى منتجنا، بطريقةٍ أو بأخرى".[337]

تتمحور أغلب استراتيجية تسويق مجموعة "إنتلكسا" لمنتجاتها من برامج التجسّس حول جهلها بكيفية استخدام عملائها لهذه المنتجات وأين.[338] وكما هي الحال مع مجموعة "إن إس أو"، أشارت الشركة في عرضٍ مسرّبٍ يعود إلى العام 2022 إلى أنّ "خدمات السحابة، وأسماء النطاقات، وسلسلة إخفاء الهوية" تقع تحت مسؤولية العميل. وبهذه الطريقة، تُحمّل الشركة الجزء الأكبر من المسؤولية المتعلّقة بالكشف عن النشاطات لعملائها. وتُعزّز "إنتلكسا" هذا النهج في طريقة تسليم منتجاتها، إذ تستخدم مبدأ "التكلفة والتأمين والشحن" و/أو "التسليم في محطة الوصول"، أي أنّها تسلّم منتجاتها للعملاء في المطارات،[339] ما يُبعدها أكثر عن عمليات التشغيل والمواقع التي تعمل فيها أنظمة برامج التجسّس. وكما تشير شركة "تالوس إنتليجنس" (Talos Intelligence)، فإنّ ذلك يولّد إحساساً مفيداً بـ"الإنكار المقبول".[340]

وفي مؤتمرٍ صحافي عُقد في آب/أغسطس 2022، اعتبرت صوفي إينت فيلد، العضو السابق في البرلمان الأوروبي والمقرّرة المسؤولة عن تقرير لجنة "بيغا" (PEGA) الخاص بالتحقيق في استخدام برامج التجسّس، أنّ "إنتلكسا" تدّعي

---

[335] بروستر، ت. (2019). *تاجر مراقبة صاحب الملايين يخرج من الظلال... وشاحنته المخصّصة لاختراق واتساب بقيمة 9 ملايين دولار*. (*A Multimillionaire Surveillance Dealer Steps out of the Shadows . . . and His $9 Million WhatsApp Hacking Van*).

[336] بروستر، ت. (2019). *تاجر مراقبة صاحب الملايين يخرج من الظلال... وشاحنته المخصّصة لاختراق واتساب بقيمة 9 ملايين دولار*. (*A Multimillionaire Surveillance Dealer Steps out of the Shadows . . . and His $9 Million WhatsApp Hacking Van*).

[337] بروستر، ت. (2019). *تاجر مراقبة صاحب الملايين يخرج من الظلال... وشاحنته المخصّصة لاختراق "واتساب" بقيمة 9 ملايين دولار*. (*A Multimillionaire Surveillance Dealer Steps out of the Shadows . . . and His $9 Million WhatsApp Hacking Van*).

[338] فينتورا، ف (2023). "إنتلكسا" و"سايتروكس": من شركة متعثّرة إلى برامج تجسّس بمستوى وكالات الاستخبارات. (Intellexa and Cytrox: from fixer-upper to Intel Agency-grade Spyware). *مدونة تالوس إنتليجنس*. متوفر على: https://blog.talosintelligence.com/intellexa-and-cytrox-intel-agency-grade-spyware/ [تم الاطلاع عليه في 2 آب/أغسطس 2025].

[339] فينتورا، ف. (2023). "إنتلكسا" و"سايتروكس": من شركة متعثّرة إلى برامج تجسّس بمستوى وكالات الاستخبارات. (Intellexa and Cytrox: from fixer-upper to Intel Agency-grade Spyware).

[340] فينتورا، ف. (2023). "إنتلكسا" و"سايتروكس": من شركة متعثّرة إلى برامج تجسّس بمستوى وكالات الاستخبارات. (Intellexa and Cytrox: from fixer-upper to Intel Agency-grade Spyware).

خضوعها للوائح الاتحاد الأوروبي كأداةٍ تسويقية.[341] كما اتّهمت فيلد الشركة بانتهاك لوائح التصدير في الاتحاد الأوروبي ورفض التعاون مع السلطات الأوروبية.[342] ومع ازدياد تورّط علامة "إنتلكسا" التجارية في الفضيحة التي كشفت عن تجسّس الحكومة اليونانية على أعضاءٍ في أحزاب المعارضة وصحافيين باستخدام برنامج "بريداتور" خلال ذلك العام، ردّ محامو الشركة على تصريحات فيلد بالقول:[343]

"للأسف، تؤدي الانتخابات اليونانية المقبلة إلى قيام وسائل الإعلام بإعادة تدوير الخرافات بشأن أنشطتنا. لا ننوي المشاركة في "حملة التشهير" هذه، فنحن لسنا جزءاً من الحملة الانتخابية. نحن نخضع بالكامل للوائح الاتحاد الأوروبي، ونعمل وفقاً للقانون، ونواصل التعاون مع السلطات المختصّة ذات الصلة".[344]

وبالعودة إلى منشورات مجموعة "إن إس أو" على "لينكد إن" التي هدفت إلى تفنيد الخرافات، أصرّ محامو ديليان على أنّ أنشطة تحالف "إنتلكسا" متوافقة تماماً مع قوانين الاتحاد الأوروبي. كما وصف ديليان الاتهامات الموجّهة إليه في العام 2019 بأنّها "حملة تشهير"، بعد أن فتحت السلطات في لارنكا، قبرص، تحقيقاً ضدّه وصادرت "شاحنته المخصّصة للتجسّس" بعدما تفاخر بقدراتها في مقابلةٍ مع مجلة "فوربس".[345] ومع ذلك، فإنّ لجوء تحالف "إنتلكسا" إلى إنشاء شركاتٍ تابعة في مختلف أنحاء العالم، ولا سيّما في الإمارات العربية المتحدة، يكشف عن روايةٍ مغايرة – وهي محاولة لتفادي لوائح الاتحاد الأوروبي المتعلّقة بتصدير التقنيات ذات الاستخدام المزدوج.

المنتجات والقدرات الرئيسية : "بريداتور"

يُعدّ برنامج "بريداتور" منتج التجسّس الأبرز لـ"سايتروكس"، ويُباع اليوم ويُسوّق تحت العلامة التجارية "إنتلكسا". وكما هي الحال مع "بيغاسوس"، يمنح "بريداتور" مشغّليه القدرة الكاملة على التحكّم في هاتف الهدف.[346] فعلى الرغم من

---

[341] مركز الوسائط المتعددة في البرلمان الأوروبي. (2022). مؤتمر صحافي لسوفي إينت فيلد، مقررة مشروع تقرير بيجا - مركز *الوسائط المتعددة*. (*Press conference by Sophie IN 't VELD, rapporteur on the PEGA Draft Report - Multimedia Centre*) [متاح على الإنترنت] متوفر على:
https://multimedia.europarl.europa.eu/en/webstreaming/press-conference-by-sophie-in-t-veld-rapporteur-on-pega-draft-report_20221108-1100-SPECIAL-PRESSER [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[342] سفيتكوسكا، س.، ناستيسكا، آي.، ستويانوفسكي، ب.، تيلوغلو، ت.، تريانتافيلو، إي.، وسيمونوفسكا، م. (2023). *شركة إسرائيلية طوّرت برنامج تجسس في سكوبيا بينما تجاهل المسؤولون المحليون الأمر- مختبر الصحافة الاستقصائية في مقدونيا الشمالية* (*Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way-IRL*)

[343] تيلوغلو، ت.، وتريانتافيلو، إي. (2022) فضيحة برامج التجسس اليونانية: كيف ترتبط الحكومة اليونانية بشركة "إنتلكسا" الإسرائيلية. (*Spyware scandal: How the Greek Government Is Tied to the Israeli Company Intellexa Greece*) [متوفر على الإنترنت] أخبار يونانية عند الطلب (Greek News on Demand). متوفر على:
https://greeknewsondemand.com/2022/11/30/greece-spyware-scandal-how-the-greek-government-is-tied-to-the-israeli-company-intellexa/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[344] سفيتكوسكا، س.، ناستيسكا، آي.، ستويانوفسكي، ب.، تيلوغلو، ت.، تريانتافيلو، إي.، وسيمونوفسكا، م. (2023). *شركة إسرائيلية طوّرت برنامج تجسس في سكوبيا بينما تجاهل المسؤولون المحليون الأمر- مختبر الصحافة الاستقصائية في مقدونيا الشمالية* (*Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way-IRL*)

[345] "تايمز أوف إسرائيل" و"أ. ف. ب." (2019). *الرئيس التنفيذي لشركة تجسس إلكتروني إسرائيلية مطلوب للتحقيق لدى الشرطة القبرصية*. [متوفر على الإنترنت] تايمز أوف إسرائيل. متوفر على:
https://ar.timesofisrael.com/%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3-%D8%A7%D9%84%D8%AA%D9%86%D9%81%D9%8A%D8%B0%D9%8A-%D9%84%D8%B4%D8%B1%D9%83%D8%A9-%D8%AA%D8%AC%D8%B3%D8%B3-%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D8%A5/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[346] "إنسيكت غروب" (2025)، *لا يزال "بريداتور" نشطاً، مع تحديد عميل جديد وروابط شركات جديدة*. (*Predator Still Active, with New Client and Corporate Links Identified*.)

محاولته إخفاء أنشطته، يمكن للبرنامج الوصول إلى كاميرا الضحية ومكبّر صوتها وقائمة اتصالاتها ورسائلها وصورها ومقاطع الفيديو الخاصّة بها وغيرها من البيانات من دون علمها. ووفقاً لتقرير صادر عن مجموعة "إنسيكت غروب"، كُتب "بريداتور" بلغة "بايثون" (Python) ليكون معياريّاً، ما يتيح للمشغّلين تحديث خصائصه من بُعد.[347] ويمكن إرسال البرنامج عبر هجمات "النقرة الواحدة" أو "من دون أي نقرة". وبذلك، يستطيع المشغّلون الاعتماد على أساليب الهندسة الاجتماعية لدفع الضحية إلى التفاعل معهم، مثل النقر على رابطٍ ضار، أو استخدام تقنيات لا تتطلّب أي تفاعل من المستخدم، مثل "هجمات حقن الشبكة".[348]

وتُشير منظمة العفو الدولية إلى أنّ "بريداتور" يُباع كحزمةٍ متكاملةٍ من البرمجيات والبنية التحتية، إذ يُباع مع واجهة على شبكة الإنترنت لإطلاق الهجمات وإدارة عمليات الاختراق، بحيث تسوّقها "إنتلكسا" تحت عنوان منصّة العمليات السيبرانية.[349] ووفقاً للمنظمة، يسوّق تحالف "إنتلكسا" منتجاتها من برامج التجسّس تحت عدّة أسماء ترتبط جميعها بـ"بريداتور": منها السهم الأخضر للمنتج الخاص بـ"أندرويد"، والسهم الأحمر للمنتج الخاص بنظام "آي أو إس"، و"هيليوس" و"نوفا". وتُقدّر منظمة العفو أنّ جميع هذه الأسماء تشير في الواقع إلى المنتج التجسّسي نفسه الذي طوّرته سايتروكس" في الأصل.[350]:

يعتمد "بريداتور" على شبكة إعداد "تثبيت" مخصّصة، تُرسل منها برمجيات خبيثة إلى الأجهزة المستهدفة.[351] وتتّصل الأجهزة المصابة بشبكة "القيادة والسيطرة" التابعة لـ"إنتلكسا"، ما يتيح للعملاء المشغّلين للبرنامج إرسال استخدام الأوامر للتحكّم بالأجهزة المصابة. ثمّ تُرسل أوامر المشغّل عبر "شبكة إخفاء الهوية"، التي تهدف إلى إخفاء موقع مستخدمي "بريداتور" وهويتهم الحقيقية. كما وثّقت مجموعة "إنسيكت غروب" اعتماد بعض عملاء بريداتور على "شبكات بنى تحتية متعددة الطبقات" في محاولة لإخفاء هويتهم بشكلٍ أكبر.[352]

وتُشير "إنسيكت غروب" إلى أنّ التقارير السابقة عن بريداتور ركّزت على اعتماده على نطاقات مزيّفة تنتحل هويّة مؤسسات معروفة مثل وسائل الإعلام، لكنّ البرنامج بدأ باستخدام أساليب أخرى مع نهاية العام 2023.[353] فقد رُصد استخدام روابط ضارّة ومتنوعة كوسيلة اختراق بنقرة واحدة، بعضها يتضمّن كلمات بغير اللغة الإنكليزية لجذب الضحايا بحسب تفضيلاتهم اللغوية. ثمّ بات مشغّلو "بريداتور" يستخدمون تكتيكات جديدة لتفادي الاكتشاف، مثل تكوينات الخوادم الحديثة والمواقع الإلكترونية الوهمية.[354] وتعكس هذه التغييرات التكتيكية طبيعة "القط والفأر" لعالم الأمن السيبراني: فمع تزايد توثيق الباحثين لنشاط "بريداتور" وفضحهم له، بدأ مشغّلوه بتطوير أساليب جديدة لتجنّب الرصد.

شهد النصف الأخير من العقد عدّة تسريباتٍ كبيرةٍ كشفت عن الأسعار التي تتقاضاها مجموعة "إنتلكسا" لقاء برامجها التجسّسية – وهي أسعار مرتفعة جداً. ففي العام 2022، نشرت صحيفة "نيويورك تايمز" للمرة الأولى عرض أسعارٍ

---

[347] "إنسيكت غروب" (2025)، *لا يزال "بريداتور"نشطاً، مع تحديد عميل جديد وروابط شركات جديدة*. (*Predator Still Active, with New Client and Corporate Links Identified*.)

[348] منظمة العفو الدولية (2023). *ملفات "بريداتور": في أحابيل الشبكة*. ص 16.

[349] منظمة العفو الدولية (2023). *ملفات "بريداتور": في أحابيل الشبكة*. [متاح على الإنترنت] *منظمة العفو الدولية*، لندن: المملكة المتحدة: منظمة العفو الدولية المحدودة. متوفر على: https://www.amnesty.org/ar/documents/act10/7246/2023/ar/

[350] منظمة العفو الدولية (2023). *ملفات "بريداتور": في أحابيل الشبكة*. ص 21.

[351] منظمة العفو الدولية (2023). *ملفات "بريداتور": في أحابيل الشبكة*. ص 22.

[352] منظمة العفو الدولية (2023). *ملفات "بريداتور": في أحابيل الشبكة*. ص 22.

[353] إنسيكت غروب (2025)، *لا يزال بريداتور نشطاً، مع تحديد عميل جديد وروابط شركات جديدة*. (*Predator Still Active, with New Client and Corporate Links Identified*.)

[354] "إنسيكت غروب" (2025)، *لا يزال "بريداتور" نشطاً، مع تحديد عميل جديد وروابط شركات جديدة*. (*Predator Still Active, with New Client and Corporate Links Identified*.)

لبرنامج "بريداتور" يعود إلى العام 2021.[355] وشملت إحدى الصفقات البرنامج كاملاً - بما في ذلك القدرة على استخراج البيانات من بُعد بنقرةٍ واحدةٍ من أجهزة "أندرويد" و"آي أو إس"، وإصابة 20 جهازاً في الوقت نفسه، وتحقيق 400 هجمة حقن ناجحة - مقابل 13.6 مليون يورو. وتضمّن العقد كفالةً لمدة سنةٍ، بالإضافة إلى توفير الأجهزة والبرمجيات اللازمة لتشغيل البرنامج، و"خطة مشروع" أعدّتها "إنتلكسا"، وتدريباً تقنيّاً متعدد الوسائط، ودعماً على مدار الساعة طوال الأسبوع، وقيوداً جغرافية. كما تضمّن العرض مجموعة من "المنتجات والخدمات الاختيارية"، مثل "عقد صيانة" للسنة الثانية بنسبة 25% من قيمة العقد سنوياً (أي نحو 3.4 ملايين يورو)، وخيار استهداف الهواتف خارج بلد العميل، وميزة "الاستمرارية" (أي قدرة البرنامج على "البقاء بعد إيقاف تشغيل الهاتف وإعادة تشغيله") مقابل 2.4 مليون يورو، وحلّاً استخباراتياً عبر "شبكة واي فاي يسمى "SpearHead 360" يُركَّب على مركبة مخصّصة للمهام السرّية"، مقابل 4.5 ملايين يورو.

وفي العام 2022 أيضاً، تسرّب عرض أسعار آخر لأحد منتجات "إنتلكسا" عبر الإنترنت - هذه المرّة لحزمة تحليل بيانات برامج التجسّس "نوفا"، التي توفّر بدورها خاصية استخراج البيانات من بُعد من أجهزة "أندرويد" و"آي أو إس".[356] وقد بيعت "نوفا" بموجب صفقةٍ واحدةٍ بقيمة 8 ملايين يورو، شملت وسيلة اختراقٍ بنقرةٍ واحدة، و10 إصاباتٍ متزامنةٍ عبر أجهزة "أندرويد" و"آي أو إس"، و100 عملية إصابة ناجحة. وكما في صفقة "بريداتور" الأساسية لعام 2021، جرى طرح "نوفا" بحيث يقتصر استخدامه داخل بلد المشغِّل فقط. وكان بإمكان العملاء شراء خاصية الاستمرارية مقابل 3 ملايين يورو لأهداف "أندرويد" و"آي أو إس"، وخيار استهداف الأجهزة في 5 دول إضافية في أي مكان في العالم مقابل 1.2 مليون يورو إضافية (تسمى "نوفا إنترناشونال").[357] كما شملت صفقة "نوفا" كفالةً لمدة سنة، وتوفير الأجهزة والبرمجيات اللازمة لتشغيل المنتج، و"خطة مشروع متكاملة"، وجلسات تدريبية للمشغِّلين. وقد دعمت كلٌّ من باقتَيْ "بريداتور" و"نوفا" القدرة على اختراق الأجهزة التي تعمل بإصدارات "أندرويد" و"آي أو إس" تعود إلى ما يصل إلى 12 شهراً قبل أحدث إصدار.[358]

كما جرى تداول مؤشرات الاختراق وإطار MITRE للهجوم والتكتيكات والتقنيات المشتركة (ATT&CK) المرتبطة ببرنامج "بريداتور" على نطاقٍ واسعٍ، من بينها ما نشرته مجموعة "إنسيكت غروب" في العام 2024.[359]

هجوم بارز

في أواخر العام 2023، نشر مختبر "سيتيزن لاب" تقريراً يحقّق في واحدة من أبرز حالات استخدام "بريداتور"، التي استهدفت سياسياً مصرياً بارزاً.

---

[355] "نيويورك تايمز" (2022). *اقرأ عرض "إنتلكسا" حول أداة التجسس "بريداتور"*. (*Read the Intellexa Pitch on Its Predator Spyware Tool*.) [متاح على الإنترنت] Archive.org متوفر على: https://web.archive.org/web/20250616044003/https://www.nytimes.com/interactive/2022/12/08/us/politics/intellexa-commercial-proposal.html [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[356] Vxunderground. (2022) [منصة "إكس" ("تويتر" سابقاً)] *25 آب/أغسطس، 2022*. متوفر على: https://x.com/vxunderground/status/1562725121277988865 (تم الاطلاع عليه في 20 تموز/يوليو 2025).

[357] مختبر الأمن التابع لمنظمة العفو الدولية (2023). *ملفات "بريداتور": بحث تقني معمّق في منتجات المراقبة لتحالف "إنتلكسا"*. (*Predator Files: Technical deep-dive into Intellexa Alliance's Surveillance Products*.) [متاح على الإنترنت] *منظمة العفو الدولية*. متوفر على: https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/ [تم الاطلاع عليه في 2 آب/أغسطس 2025].

[358] مختبر الأمن التابع لمنظمة العفو الدولية (2023). *ملفات "بريداتور": بحث تقني معمّق في منتجات المراقبة لتحالف "إنتلكسا"*. (*Predator Files: Technical deep-dive into Intellexa Alliance's Surveillance Products*.)

[359] إنسيكت غروب" (2024)، *مشغلو برامج التجسس "بريداتور" يعيدون بناء البنية التحتية متعددة المستويات لاستهداف الأجهزة المحمولة*. (*Predator Spyware Operators Rebuild Multi-Tier Infrastructure to Target Mobile Devices*.)

ففي الفترة الممتدة من أيار/مايو إلى أيلول/سبتمبر 2023، استهدف أحد مشغّلي "بريداتور" النائب المصري السابق أحمد الطنطاوي بعد إعلانه عزمه الترشّح لمنافسة الرئيس المصري عبد الفتاح السيسي في الانتخابات الرئاسية لعام 2024.[360] وأعقب هذا الإعلان اعتقال السلطات المصرية عدداً من أفراد عائلته، ما دفعه إلى القلق بشأن سلامته الرقمية والجسدية.[361] [362] ووفقاً لفيلدستاين وكوت (2023) وتقارير إضافية حلّلتها "سمكس"، لجأت مصر مراراً في عهد السيسي إلى استخدام برامج التجسّس ضدّ المعارضين.[363] ويُعرف السيسي بإدارته لحكومةٍ قمعيةٍ وباستخدامه القبضة الحديدية ضدّ خصومه السياسيين.[364]

وقد سلّم الطنطاوي هاتفه إلى "سيتيزن لاب"، الذي كشفت تحقيقاته عن محاولاتٍ متعدّدةٍ لتثبيت برنامج "بريداتور" عليه. كما أظهرت نتائج التحقيق أنّ اتصال الطنطاوي بالهاتف المحمول، الذي يمرّ عبر شبكة "فودافون مصر"، كان "مُستهدفاً استهدافاً متكرّراً عبر تقنية حقن الشبكة" في الفترة بين آب/أغسطس وأيلول/سبتمبر 2023.[365] فعندما كان يزور مواقع غير آمنة لا تستخدم بروتوكول نقل النص التشعبي الآمن (HTTPS)، كان يُعاد توجيهه تلقائياً إلى مواقع ضارّة عبر جهاز داخل شبكة "فودافون مصر" لتثبيت حمولة "بريداتور" وإصابة هاتفه. ويُبرز هذا الأمر، بحسب "سيتيزن لاب"، مشكلةً أوسع تتعلّق بانعدام الأمن في طبقة الشبكة، حيث تستطيع مصادر التهديد ومشغّلو برامج التجسّس استغلالها لنشر برمجيات خبيثة على أجهزة الضحايا.[366]

كما حاول مشغّلو بريداتور استهداف الطنطاوي عبر الرسائل القصيرة (SMS) وتطبيق "واتساب" باستخدام أساليب الهندسة الاجتماعية، باعتمادهم على رسائل تنتحل عناوين الويب المرتبطة بـ"واتساب". وزُعم في إحدى الرسائل أنّ مستخدماً آخر قد سجّل الدخول إلى حسابه، وأن عليه "إنهاء" الجلسة لحماية حسابه، باستخدام رابطٍ ضارٍّ على الأرجح.[367] وغالباً ما يسعى المهاجمون، في أساليب الهندسة الاجتماعية، إلى دفع ضحاياهم لاتّخاذ قراراتٍ متسرّعة من خلال الإيحاء بأنّ اتّخاذ إجراءٍ

---

[360] ماركزاك، ب.، سكوت-ريلتون، ج.، عبد الرزاق، ب.، ديبرت، ر.، روثليسبيرغر، د.، أنستيس، س. (2023). PREDATOR في الاتصالات: أحمد الطنطاوي مستهدف ببرنامج التجسس Predator بعد الإعلان عن نيته للترشح للرئاسة. [متاح على الإنترنت] *"سيتيزن لاب"*. جامعة تورونتو. متوفر على: https://citizenlab.ca/2023/10/predator-%D9%81%D9%8A-%D8%A7%D9%84%D8%A7%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA-%D8%A3%D8%AD%D9%85%D8%AF-%D8%A7%D9%84%D8%B7%D9%86%D8%B7%D8%A7%D9%88%D9%8A-%D9%85%D8%B3%D8%AA%D9%87%D8%AF%D9%81-%D8%A8/ [تم الاطلاع عليه في 7 آب/أغسطس 2025].

[361] سعفان، ف. (2023). نائب مصري سابق يخطط للترشح للرئاسة، ويقول إن أقاربه أُلقي القبض عليهم. (Egyptian ex-MP Planning Presidential Bid Says Relatives Arrested). *رويترز*. [متاح على الإنترنت] 4 أيار/مايو. متوفر على: https://www.reuters.com/world/africa/egyptian-ex-mp-planning-presidential-bid-says-relatives-arrested-2023-05-04/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[362] "هيومن رايتس ووتش" (2023). *مصر: اعتقالات جماعية تستهدف عائلة نائب سابق وأنصاره*. [متاح على الإنترنت] "هيومن رايتس ووتش". متوفر على: https://www.hrw.org/ar/news/2023/05/06/egypt-mass-arrests-target-family-supporters-ex-mp [تم الاطلاع عليه في 3 آب/أغسطس 2025].

[363] فيلدستاين، س. وكوت، ب. (2023). *لماذا تستمر صناعة برامج التجسس العالمية في الازدهار؟*

[364] منظمة العفو الدولية (2019). *مصر: سلسلة من القوانين الشديدة القسوة "تضفي الشرعية" على حملة القمع غير المسبوق بعد مرور ست سنوات على الإطاحة بمرسي*. [متاح على الإنترنت] متوفر على: https://www.amnesty.org/ar/latest/news/2019/07/egypt-series-of-draconian-laws-legalizes-unprecedented-repression-six-years-since-fall-of-morsi-2/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[365] ماركزاك، ب.؛ سكوت-رايلتون، ج.؛ عبد الرزاق، ب.؛ ديبرت، ر.؛ روثليسبيرغر، د. وأنستيس، س. (2023). "بريداتور" في الأسلاك. (*PREDATOR IN THE WIRES*).

[366] ماركزاك، ب.؛ سكوت-رايلتون، ج.؛ عبد الرزاق، ب.؛ ديبرت، ر.؛ روثليسبيرغر، د. وأنستيس، س. (2023). "بريداتور" في الأسلاك. (*PREDATOR IN THE WIRES*).

[367] ماركزاك، ب.؛ سكوت-رايلتون، ج.؛ عبد الرزاق، ب.؛ ديبرت، ر.؛ روثليسبيرغر، د. وأنستيس، س. (2023). "بريداتور في الأسلاك." (*PREDATOR IN THE WIRES*).

ما ضروري أو في الوقت المناسب، مستغلّين بذلك العوامل العاطفية لدفعهم نحو تنفيذ سلوكٍ معيّن.[368] كما تواصل شخصٌ آخر انتحل صفة مدافعٍ عن حقوق الإنسان مع الطنطاوي عبر "واتساب"، محاولاً إقناعه بالنقر على رابطٍ ضارٍّ مرتبط بحمولات "بريداتور". وقد عزَا "سيتيزن لاب" هذه المحاولات بثقةٍ شبه مطلقة إلى الحكومة المصرية.[369]

وفي شباط/فبراير 2024، قضت محكمةٌ مصريةٌ بإدانة الطنطاوي بتهمة تزوير وثائق انتخابية ومنعته من الترشّح في الانتخابات المقبلة.[370] كما فُرضت عليه غرامةٌ قدرها 20,000 جنيه مصري، وحُكم عليه بالسجن لمدة عامٍ مع وقف التنفيذ. ثمّ صدر في أيار/مايو 2024 حكمٌ جديد بسجنه سنةً مع الأشغال الشاقّة.[371]

3.3. سيلبرايت

"قد يستخدم العملاء بعض حلولنا من بطريقةٍ تتعارض، أو قد يُنظر إليها على أنّها تتعارض، مع مبادئ حقوق الإنسان."

- شركة "سيلبرايت"، من إيداعها نموذج F-20 لدى لجنة الأوراق المالية والبورصات لعام 2024[372]

خلفية الشركة وحضورها في منطقة غرب آسيا وشمال أفريقيا

تُعدّ "سيلبرايت" شركةً متعدّدة الجنسيات وواحدةً من أبرز مزوّدي حلول التحليل الجنائي الرقمي والاستخبارات لصالح أجهزة إنفاذ القانون والحكومات حول العالم. أسّس كلٌّ من آفي يابلونكا ويوفال أفلالو وياورن باراتس الشركة في إسرائيل عام 1999.[373] وعلى عكس شركات المراقبة السيبرانية الأخرى التي يتناولها هذا التقرير، تُعدّ "سيلبرايت" شركةً مساهمةً عامةً مُدرجة في بورصة ناسداك الأميركية، ما يفرض عليها الإفصاح عن بعض المعلومات وفق متطلّبات لجنة الأوراق المالية والبورصات. ووفقاً لأحدث ملفاتها في العام 2024، سجّلت "سيلبرايت" (رمز التداول في ناسداك: CLBT؛ مفتاح

---

[368] آي بي إم (2022) (IBM). *ما هي الهندسة الاجتماعية؟* (*What is Social Engineering?*) [متاح على الإنترنت] IBM. متوفر على: https://www.ibm.com/think/topics/social-engineering [تم الاطلاع عليه في 5 آب/أغسطس 2025].

[369] ماركزاك، ب.؛ سكوت-رايلتون، ج.؛ عبد الرزاق، ب.؛ ديبرت، ر.؛ روثليسبيرغر، د. وأنستيس، س. (2023). "بريداتور في الأسلاك". (*PREDATOR IN THE WIRES*).

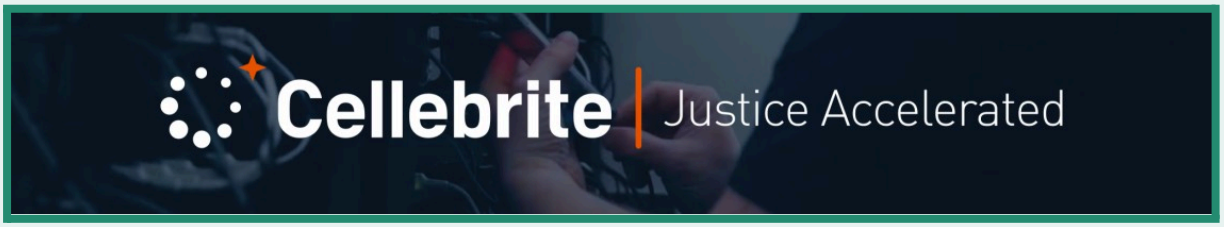
[370] فريق رويترز (2024). المصادر تقول: المرشح الرئاسي المصري السابق طنطاوي مدان بالتزوير. (Ex-Egyptian Presidential Candidate Tantawy Found Guilty of forgery, Sources Say.) *رويترز*. [متاح على الإنترنت] 6 سباط/فبراير. متوفر على: . Available at: https://www.reuters.com/world/africa/ex-egyptian-presidential-candidate-tantawy-found-guilty-forgery-sources-20 /24-02-06 .

[371] سعفان، ف. (2024). مصر تسجن المرشح الرئاسي السابق لمدة سنة مع الأشغال الشاقّة. (Egypt Jails Former Presidential Hopeful for One Year with Labour.) *رويترز*. . [متاح على الإنترنت] 27 أيار/مايو. متوفر على: https://www.reuters.com/world/africa/egypt-jails-former-presidential-hopeful-one-year-with-labour-2024-05-27/ [تم الاطلاع عليه في 6 آب/أغسطس 2025].

[372] شركة "سيلبرايت للذكاء الرقمي م." (2025). *نموذج F-20-Form 20*. (*F.*) [متاح على الإنترنت] لجنة الأوراق المالية والبورصات، ص 20. متوفر على: https://investors.cellebrite.com/static-files/7bf7cec5-50b6-4f1e-99f4-f7f8238e1d2a [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[373] شولمان، س. (2025). *من شركة ناشئة بموارد ذاتية إلى قوة تكنولوجية بقيمة 5 مليارات دولار: الرئيس التنفيذي المنتهية ولايته لشركة "سيلبرايت" يستعرض 19 عاماً من النجاحات والتحديات*. (*From Bootstrapped Startup to a $5B powerhouse: Cellebrite's Outgoing CEO Reflects on 19 Years of Highs and Con*.) [متاح على الإنترنت] "سي تك" (CTech). متوفر على: https://www.calcalistech.com/ctechnews/article/lhck15vtj [تم الاطلاع عليه في 29 آب/أغسطس 2025].

الفهرس المركزي[374] (CIK: 0001854587) إيراداتٍ بلغت 401 مليون دولار، وأرباحاً تشغيلية بلغت 56.9 مليون دولار، ويعمل لديها 1,167 موظفاً حول العالم.[375] وتزعم الشركة أنّ قاعدة عملائها تضمّ نحو 7,000 عميل حول العالم، وأنّ 90% من إيراداتها في الأعوام 2022 و2023 و2024 جاءت من عقودٍ مبرمةٍ مع أجهزة إنفاذ القانون والجهات الحكومية.[376] وتؤكّد "سيلبرايت" أنّ لديها عملاء في أكثر من 100 دولة، كما أفادت بأنّ مبيعاتها في أسواق أوروبا والشرق الأوسط وأفريقيا شكّلت 53.7% من إجمالي إيراداتها في العام 2024.[377] [378]



الصورة 17: شعار سيلبرايت على صفحتها على "لينكد إن".[379]

سيلبرايت تسريع مجرى العدالة	Cellebrite Justice Accelerated

بدأت عروض "سيلبرايت" التجارية بتركيزها على حلول نقل البيانات بين الأجهزة المحمولة.[380] وتُظهر نسخة من موقع الشركة تعود إلى العام 2000 هذا الأمر بوضوح، إذ كانت تُروّج حينها لمنتجها "مبدّل ذاكرة الهواتف الخلوية".[381]

---

[374] هيئة الأوراق المالية والبورصات (2025). نظام جمع البيانات الإلكترونية وتحليلها واسترجاعها (EDGAR) | نتائج بحث الشركات: شركة "سيلبرايت للذكاء الرقمي م." – 0001854587. (EDGAR | Company Search Results: Cellebrite DI Ltd. - 0001854587.) [متاح على الإنترنت] متوفر على: https://www.sec.gov/edgar/browse/?CIK=1854587&owner=exclude [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[375] شركة "سيلبرايت للذكاء الرقمي م." (2025). نموذج *Form 20-F-20* (*F.*). ص 12، 80-86.

[376] شركة "سيلبرايت للذكاء الرقمي م." (2025). نموذج *Form 20-F-20* (*F.*). ص 22، 58.

[377] "سيلبرايت". (2025). *غرفة الأخبار (Newsroom)* [متاح على الإنترنت] متوفر على: https://cellebrite.com/en/newsroom/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[378] شركة "سيلبرايت للذكاء الرقمي م." (2025). نموذج *Form 20-F-20* (*F.*). ص 194.

[379] "سيلبرايت" (2025). الصفحة الرئيسية لشركة "سيلبرايت". (*Cellebrite's home page*.) [لينكد إن]. [تم الاطلاع عليه في 13 آب/أغسطس 2025] متوفر على: https://www.linkedin.com/company/cellebrite/

[380] شولمان، س. (2025). *من شركة ناشئة بموارد ذاتية إلى قوة تكنولوجية بقيمة 5 مليارات دولار. (From Bootstrapped Startup to a $5B powerhouse).*

[381] "سيلبرايت" (2000). *شركة "سيلبرايت م." - جهاز تبادل ذاكرة الهواتف المحمولة. (Cellebrite LTD - Mobile Cellular Phone Memory Exchanger.)* [متاح على الإنترنت] متوفر على: https://web.archive.org/web/20001018130340/http://www.cellebrite.com/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

الصورة 18: موقع "سيلبرايت" في العام 2000 يروّج لأولى خدماته في نقل البيانات

Cellular Phones Memory Exchanger	مبدّل ذاكرة الهواتف الخلوية
Universal Memory Exchanger - UME 12	مبدّل الذاكرة الشامل - UME 12
The UME-12 is an advanced device that allows for the transfer of memory content between a wide range of mobile cellular phones and cellular technologies available in the marketplace today.	يُعدّ جهاز UME-12 أداةً متقدّمةً تتيح نقل محتوى الذاكرة بين مجموعةٍ واسعةٍ من الهواتف الخلوية وتقنيات الاتصالات الخلوية المتوفّرة في السوق اليوم.
The UME-12 enables the exchange of memory content between mobile phones in a simple and reliable manner, thus solving one of the cellular carriers' most important service problem.	يُمكّن جهاز UME-12 من تبادل محتوى الذاكرة بين الهواتف المحمولة بطريقة بسيطة وموثوقة، ما يوفّر حلّاً لإحدى أهمّ مشكلات الخدمة التي تواجه شركات الاتصالات الخلوية.
The UME-12 is developed and produced by: Cellebrite LTD.	أنتجت شركة سيلبرايت المحدودة. جهاز UME-12 وطوّرته.

اتّجهت شركة "سيلبرايت" نحو التحليل الجنائي الرقمي في العام 2007 عندما طرحت جهاز استخراج الأدلة الجنائية العالمي (UFED)، وهو جهازٌ يُستخدم في التحليل الجنائي الرقمي وتصفه الشركة بأنّه "معيار الصناعة للوصول إلى البيانات الرقمية وجمعها بطريقةٍ قانونية".[382]

ومع هذا التحوّل، بدأت "سيلبرايت" بالتوسّع عالمياً واستقطبت استثماراتٍ ضخمة. فقد استحوذت شركتا "فيوتشر ديال" (FutureDial Incorporated) و"صن" (Sun Corporation)، وهما من كبار المساهمين في الشركة، على

[382] "سيلبرايت" (2024). *جهاز "سيلبرايت" الاستخراج الأدلة الجنائية العالمي (UFED) / Cellebrite)* الوصول إلى بيانات الأجهزة المحمولة وجمعها. *LTD - Mobile Cellular Phone Memory Exchanger).* [متاح على الإنترنت] متوفر على: https://cellebrite.com/en/ufed/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

"سيلبرايت" في العام 2007،[383] حيث باع المؤسّسون الثلاثة حصصهم لشركة "صن" مقابل نحو 17.5 مليون دولار.[384] وفي العام 2019، استثمر صندوق "شركاء النمو الإسرائيليون" (Israeli Growth Partners)، المتخصّص في الاستثمارات التكنولوجية، 110 ملايين دولار في "سيلبرايت"، ما رفع قيمة الشركة إلى 440 مليون دولار.[385] وفي كانون الثاني/يناير 2020، وسّعت "سيلبرايت" عروض منتجاتها لتشمل أجهزة الكمبيوتر من خلال شرائها شركة "بلاك باغ تكنولوجيز" (BlackBag technologies)، وهي شركةٌ متخصّصةٌ في التحليل الجنائي الحاسوبي،[386] وحصلت بموجب الصفقة على 25% من أسهمها. كما أعلنت "سيلبرايت" في نيسان/أبريل 2021 عن خطّتها للاندماج مع "شركة تي دبليو سي تيك هولدينغز" (TWC Tech Holdings II Corporation)، ما أتاح إدراجها في بورصة ناسداك،[387] وقُدّرت قيمة الشركة آنذاك بـ2.4 مليار دولار. وفي 16 تموز/يوليو 2024، استحوذت "سيلبرايت" على "شركة خدمات تكنولوجيا الأمن السيبراني" (Cyber Technology Services Inc.) المتخصّصة في خدمات الأمن السيبراني والاستجابة للحوادث، مقابل 3.8 مليون دولار.[388] ومؤخّراً، في حزيران/يونيو 2025، أفادت التقارير بأنّ "سيلبرايت" اشترت شركة

---

[383] "كرانشبيس" (Crunchbase) (بدون تاريخ). *استحواذ "فيوتشر ديال" على "سيلبرايت"*. (*Cellebrite Acquired by FutureDial*.) [متاح على الإنترنت] "سيلبرايت". متوفر على: https://www.crunchbase.com/acquisition/futuredial-acquires-cellebrite--8a593335 [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[384] شولمان، س. (2025). *من شركة ناشئة بموارد ذاتية إلى قوة تكنولوجية بقيمة 5 مليارات دولار*. (*From Bootstrapped Startup to a $5B powerhouse*.).

[385] هازاني، ج. (2025). استحوذ صندوق "شركاء النمو الإسرائيليون" على 25% من شركة التحليل الجنائي للأجهزة المحمولة "سيلبرايت" مقابل 110 ملايين دولار. (IGP Acquires 25% Stake in Mobile Forensics Firm Cellebrite for $110 Million.). *"سي تك"*. [متاح على الإنترنت] https://www.calcalistech.com/ctech/articles/0,7340,L-3764425,00.html [تم الاطلاع عليه في 29 حزيران/يونيو. متوفر على: 17 آب/أغسطس 2025].

[386] ميلر، س. (2020). *"سيلبرايت" تتوسّع إلى الحواسيب عبر استحواذ على شركة "بلاك باغ تكنولوجيز" المتخصصة في الأدلة الجنائية بقيمة 33 مليون دولار* - (*Cellebrite Expands to Computers with $33M Acquisition of BlackBag Technologies Forensics Firm - 9to5Mac*.) [متاح على الإنترنت] 9to5Mac. متوفر على: https://9to5mac.com/2020/01/14/cellebrite-blackball-technologies-acquistino/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[387] "سيلبرايت". (2021). *"سيلبرايت"، المزوّد الرائد في حلول الذكاء الرقمي، ستُدرج في بورصة ناسداك بعد اندماجها مع شركة "تي دبليو سي تيك هولدينغز"*. (*Cellebrite, the Leading Digital Intelligence Solutions Provider, to List on Nasdaq through Merger with TWC Tech Holdings II Corp.*) [متاح على الإنترنت] متوفر على: https://web.archive.org/web/20210429051805/https://www.cellebrite.com/en/cellebrite-to-list-on-nasdaq-through-merger-with-twc-tech-holdings-ii-corp [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[388] S&P Capital IQ(2024). *استحوذت "سيلبرايت للذكاء الرقمي م." على شركة خدمات تكنولوجيا الأمن السيبراني، مقابل 3.8 مليون دولار*. (*Cellebrite DI Ltd. Acquired Cyber Technology Services, Inc. from $3.8 million*.) [متاح على الإنترنت] ماركت سكرينر (MarketScreener.) متوفر على: https://www.marketscreener.com/quote/stock/CELLEBRITE-DI-LTD-126371088/news/Cellebrite-DI-Ltd-acquired-Cyber-Technology-Services-Inc-from-3-8-million-47401771/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

" كوريليوم" (Corellium) الناشئة في مجال المحاكاة الافتراضية للحاسوب، مقابل 200 مليون دولار، لتعزيز قدراتها في اختراق الأجهزة المحمولة المشفّرة.[389] [390] [391]

وحتى العام 2025، تحتفظ "سيلبرايت" بشبكةٍ عالميةٍ تضمّ 12 شركة تابعة في أستراليا والبرازيل وكندا والهند وفرنسا وألمانيا واليابان وسنغافورة والمملكة المتحدة والولايات المتحدة، (بالإضافة إلى مقرّها الرئيسي في بتاح تكفا في إسرائيل).[392] وتدير الشركة أيضاً 14 مكتباً حول العالم.[393]

ووفقاً للبيانات المالية الصادرة عن "سيلبرايت" لعام 2024، تمتلك شركة "صن" 44.3% من أسهم الشركة، بينما تمتلك شركة "ترو ويند كابيتال مانجمنت" (True Wind Capital Management، 5.8%)، وهي الحصّة الناتجة عن اندماج "سيلبرايت" مع "تي دبليو سي تيك هولدينغز". وبذلك، تمتلك الشركتان معاً الحصّة الأكبر من الأسهم العادية.[394]

وعلى الرغم من أنّ "سيلبرايت" لا تبيع برامج تجسّس بحدّ ذاتها، إلّا أنّ منتجاتها الأساسية تُستخدم لاختراق الهواتف المحمولة وأجهزة الحاسوب وتنسخ كامل الهوية الرقمية للأفراد المستهدفين. وتزعم الشركة أنّ منتجاتها تُستخدم بشكلٍ قانونيٍّ ولا يمكن اعتبارها برامج تجسّس، لأنّ استخدامها يأتي بعد وقوع الجرائم.[395] لكنّ هذه الادعاءات ثبت زيفها؛ إذ أفادت تقارير في أواخر العام 2024 بأنّ السلطات الصربية أساءت استخدام تقنيات سيلبرايت لاختراق هواتف نشطاء من دون إثبات ارتكابهم أيّ جرائم.[396]

وتكاد أجهزة استخراج الأدلة الجنائية العالمية (UFED) تستوفي المعايير المعتمدة في هذا التقرير لتُصنَّف كبرامج تجسّس، كما ورد في القسم الثاني. فعلى الرغم من أنّ معظم منتجات "سيلبرايت" تتطلّب وصولاً مادياً إلى الهواتف، إلّا انّ منتج UFED السحابي يتيح استخراج البيانات من بُعد من الأجهزة.[397] وعند الجمع بين ذلك وبين حالاتٍ موثّقةٍ مختلفةٍ أساءت فيها

---

[389] بروستر، ت. (2025). "سيلبرايت" تستحوذ على شركة "كوريليوم" الناشئة في مجال التحليل الجنائي للهواتف مقابل 200 مليون دولار. (Cellebrite to Acquire Phone Forensics Startup Corellium for $200 Million) *فوربس*. [متاح على الإنترنت] 5 حزيران/يونيو. متوفر على: https://www.forbes.com/sites/thomasbrewster/2025/06/05/trump-pardoned-corellium-founder-now-selling-cyber-business-to-cellebrite/ .

[390] تومسون، إ. (2025). "*سيلبرايت" تشتري "كوريليوم" لمساعدة الشرطة على اختراق تشفير الهواتف*. (*Cellebrite Buys Corellium to Help Cops Bust Phone Encryption*.) [متاح على الإنترنت] ذا ريجستير (The Register) متوفر على: https://www.theregister.com/2025/06/05/cellebrite_corellium_merger/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[391] حصل كريس وايد، مؤسس شركة "كوريليوم"، على عفوٍ رئاسي من الرئيس الأميركي دونالد ترامب في العام 2020 عن جرائم إلكترونية ارتُكبت في منتصف العقد الأول من الألفية الثانية. وتشير التقارير إلى أنّه سيتولى منصب المدير التقني في شركة "سيلبرايت" ابتداءً من الربع الثالث من العام 2025، بعد إبرام الصفقة.

[392] شركة "سيلبرايت للذكاء الرقمي م." (2025). *نموذج 20-F (Form 20-F)*. *F.*). ص 76.

[393] "سيلبرايت". (2025أ). *حول "سيلبرايت"*. (*About – Cellebrite*) [متاح على الإنترنت] متوفر على: https://cellebrite.com/en/about/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[394] شركة "سيلبرايت للذكاء الرقمي م." (2025). *نموذج 20-F (Form 20-F)*. *F.*). ص 139.

[395] " سيلبرايت". (2025). "*سيلبرايت" تقدم معلومات حول أعمالها وحلولها – "سيلبرايت"*. (*Cellebrite Provides Facts about Its Business and Solutions - Cellebrite*.) [متاح على الإنترنت] متوفر على: https://cellebrite.com/en/cellebrite-facts [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[396] منظمة العفو الدولية (2024). *صربيا: السلطات تستخدم برامج التجسس وأدوات استخراج بيانات التحليل الجنائي من "سيلبرايت" لاختراق هواتف الصحافيين والنشطاء*. (*Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists (and Activists*

[397] منظمة العفو الدولية (2024). *صربيا: السلطات تستخدم برامج التجسس وأدوات استخراج بيانات التحليل الجنائي من "سيلبرايت" لاختراق هواتف الصحافيين والنشطاء*. (*Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists (and Activists*

دولٌ استبدادية حول العالم استخدام منتجات "سيلبرايت"، خلص هذا التقرير إلى أنّ "سيلبرايت" تُعدّ إحدى شركات المراقبة السيبرانية المثيرة للقلق في منطقة غرب آسيا وشمال أفريقيا.[398] [399]

أما اليوم، فيتولّى يارون باراتس، أحد مؤسّسي "سيلبرايت"، منصب الرئيس التنفيذي لشركة "سبتير" (Septier) المتخصّصة في استخبارات الإشارات، التي أسّسها عام 2000 وتبيع "أنظمة اعتراض الاتصالات وتحليلها" للحكومات وأجهزة إنفاذ القانون. ويبدو أنّ حسابه على "لينكد إن" خاص، لكنّه يُدرجه كرئيس تنفيذي لشركة "سبتير".[400] وقد أُفيد في آب/أغسطس 2023 بأنّ "سبتير" باعت "تكنولوجيا الاعتراض القانوني" لشركة اتصالات هندية،[401] وتُعرف الهند باستخدام تكنولوجيا المراقبة هذه لمراقبة المتظاهرين والمعارضين السياسيين.[402] [403] أمّا آفي يابلونكا فيشغل حالياً منصب الرئيس التنفيذي لشركة "هايبرميديا سيستمز م." (Hypermedia Systems Ltd.)، وهي شركة اتصالات تهدف إلى مساعدة الشركات في تطوير بنيتها التحتية للاتصالات.[404] أما يوفال أفلالو، فقد شارك في تأسيس "هايبرميديا سيستمز" عام 2003 وشغل منصب الرئيس التنفيذي حتى العام 2016، ثمّ شارك في تأسيس شركة "ناتورونغو" (Naturongo)،[405] وهي شركة برمجيات تركّز على الطب البديل.[406]

---

[398] بيدل، س. وديزمخ، ف. (2016). *استخدام برنامج "سيلبرايت" لاختراق الهواتف في ملاحقة معارض تعرّض للتعذيب* (*Phone-Cracking: Cellebrite Software Used to Prosecute Tortured Dissident*). [متاح على الإنترنت] ذا إنترسيبت (The Intercept) متوفر على: https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/ [تم الاطلاع عليه في 29 تموز/يوليو 2025].

[399] غور ميغيدو (2020). *الكشف عن قيام شركة إسرائيلية بتقديم خدمات اختراق الهواتف للمملكة العربية السعودية - أخبار التكنولوجيا* (*Revealed: Israeli Firm Provided phone-hacking Services to Saudi Arabia - Tech News*). [متاح على الإنترنت] هآرتس. متوفر على: https://www.haaretz.com/israel-news/tech-news/.premium-revealed-israeli-firm-provided-phone-hacking-services-to-saudi-arabia-1.9161374 [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[400] باراتس، ي. (2025). *صفحة يارون باراتس الشخصية* (*Yaron Baratz's profile page*). [لينكد إن]. [تم الاطلاع عليه في 17 آب/أغسطس 2025]. متوفر على: https://www.linkedin.com/in/yaron-baratz-50371213/.

[401] باركين، ب.، سريفاستافا، م.، غروس، أ.، كوك، ك. وهيل، أ. (2023). *"البوابة الخلفية" للاتصالات في الهند تجذب شركات المراقبة* (*India's 'Backdoor' Attracts Surveillance Companies*). [متاح على الإنترنت] فاينانشال تايمز. متوفر على: https://www.ft.com/content/adf1cbae-4217-4d7d-9271-8bec41a56fb4 [تم الاطلاع عليه في 9 أيار/مايو 2025].

[402] داس، س. (2020). *التعرف على الوجوه و"الأسرار التجارية": ماذا تفعل قوات الشرطة بالضبط بتقنيات المراقبة؟* (*Facial Recognition and 'Trade Secrets': What Exactly Are Police Forces Doing with Surveillance Tech?*). [متاح على الإنترنت] نيوز18 (News18). متوفر على: https://www.news18.com/news/tech/facial-recognition-and-trade-secrets-what-exactly-are-police-forces-doing-with-surveillance-tech-3145223.html [تم الاطلاع عليه في 29 آب/أغسطس 2025].

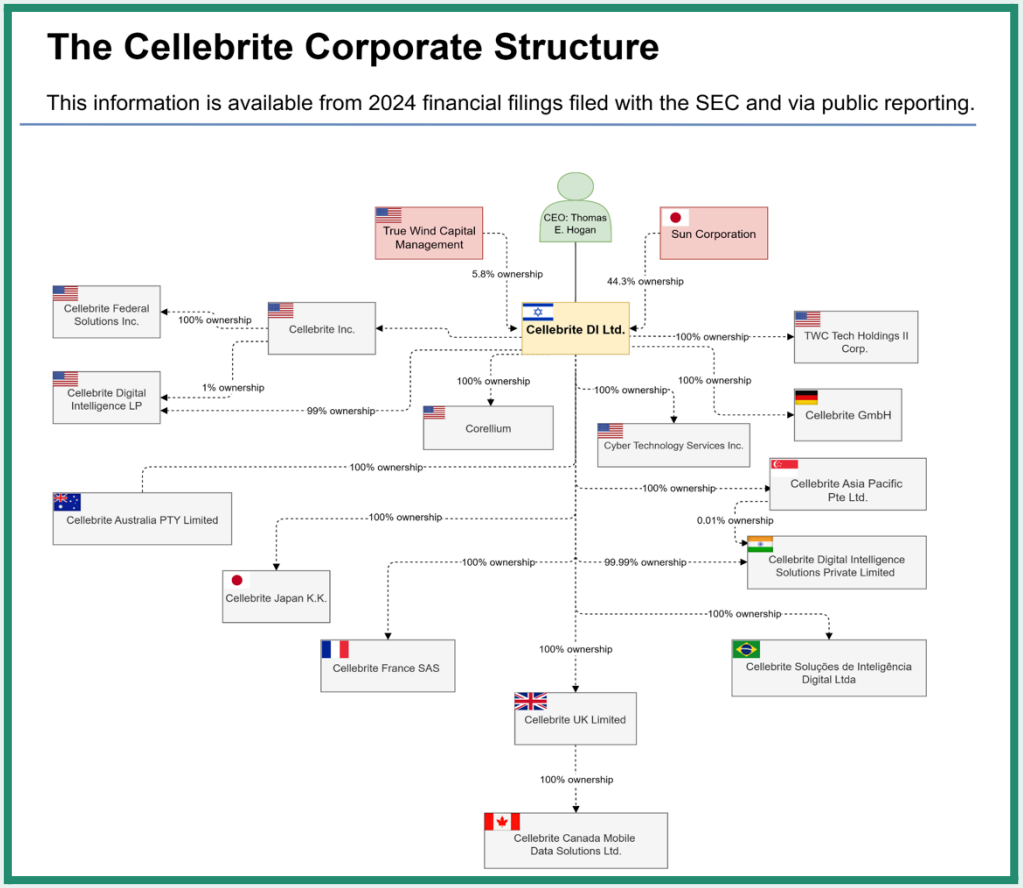
[403] روي، س. (2021). *أنا تحت "المراقبة"، تدّعي النائبة ماهوا مويترا من حزب ترينامول، وتكتب إلى قائد شرطة دلهي* (*I'm under 'Surveillance', Claims Trinamool MP Mahua Moitra, Writes to Delhi Police Chief*). [متاح على الإنترنت] الهند اليوم (India Today) متوفر على: https://www.indiatoday.in/india/story/i-m-under-surveillance-claims-trinamool-mp-mahua-moitra-writes-to-delhi-police-chief-1768959-2021-02-13 [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[404] يابلونكا، أ. (2025). *صفحة آفي يابلونكا الشخصية* (*Avi Yablonka's profile page*). [لينكد إن]. [تم الاطلاع عليه في 17 آب/أغسطس 2025]. متوفر على: https://www.linkedin.com/in/avi-yablonka-831b18/.

[405] "ناتورونغو". (2017). *الشركة – "ناتورونغو"* (*Company - Naturongo*). [متاح على الإنترنت] متوفر على: https://www.naturongo.com/company/ [تم الاطلاع عليه في 17 آب/أغسطس 2025].

[406] أفلالو، ي. (2025). *صفحة يوفال أفلالو الشخصية* (*Yuval Aflalo's profile page*). [لينكد إن]. [تم الاطلاع عليه في 17 آب/أغسطس 2025]. متوفر على: https://www.linkedin.com/in/yuval-aflalo-53aa9a/.

ويتركّز حضور "سيلبرايت" في منطقة غرب آسيا وشمال أفريقيا بشكلٍ رئيسيٍّ من خلال مكتبها في إسرائيل. وتشير البيانات المستقاة من التقارير العامّة إلى أنّ ما لا يقلّ عن خمس دول في المنطقة قد استخدمت أدوات "سيلبرايت" الجنائية.



الصورة 19: الهيكل المؤسسي لشركة "سيلبرايت"

The Cellebrite Corporate Structure	الهيكل المؤسسي لشركة سيلبرايت
This information is available from 2024 financial filings filed with the SEC and via public reporting	تستند هذه المعلومات إلى الملفات المالية لعام 2024 المقدّمة إلى لجنة الأوراق المالية والبورصات ومن خلال التقارير العامة.
Cellebrite Federal Solutions Inc.	شركة سيلبرايت للحلول الفيدرالية
Cellebrite Digital Intelligence LP	سيلبرايت للذكاء الرقمي ش.ت.م.
Cellebrite Australia PTY Limited	سيلبرايت أستراليا ش.خ.م.
Cellebrite Japan K.K.	سيلبرايت اليابان ش.م.
Cellebrite France SAS	سيلبرايت فرنسا ش.م.ب.
100% ownership	100% من الملكية
1% ownership	1% من الملكية
99% ownership	99% من الملكية
100% ownership	100% من الملكية
100% ownership	100% من الملكية
Cellebrite Inc.	شركة سيلبرايت
True Wind Capital Management	ترو ويند كابيتال مانجمنت
5.8% ownership	5.8% من الملكية
100% ownership	100% من الملكية
Corellium	كوريليوم
100% ownership	100% من الملكية
CEO: Thomas E. Hogan	الرئيس التنفيذي: توماس إ. هوغان
Cellebrite DI Ltd.	سيلبرايت للذكاء الرقمي م.
100% ownership	100% من الملكية
Cellebrite UK Limited	سيلبرايت المملكة المتحدة المحدودة
100% ownership	100% من الملكية
Cellebrite Canada Mobile Data Solutions Ltd.	شركة سيلبرايت كندا لحلول بيانات الجوال المحدودة
Sun Corporation	شركة صن
44.3% ownership	44.3% من الملكية
100% ownership	100% من الملكية
Cyber Technology Services Inc.	شركة خدمات تكنولوجيا الأمن السيبراني
100% ownership	100% من الملكية
99.99% ownership	99.99% من الملكية
100% ownership	100% من الملكية
TWC Tech Holdings Corp.	شركة تي دبليو سي تيك هولدينغز
Cellebrite GmbH	سيلبرايت ش.م.م.
Cellebrite Asia Pacific Pte Ltd.	سيلبرايت آسيا والمحيط الهادئ ش.خ.م.
0.01% ownership	0.01% من الملكية
Cellebrite Digital Intelligence Solutions Private Limited	شركة سيلبرايت لحلول الذكاء الرقمي الخاصة المحدودة
100% ownership	100% من الملكية
Cellebrite Solucoes de Inteligencia Digital Ltda	سيلبرايت لحلول الذكاء الرقمي م.

التسويق: "الطرف المملّ"

تقدّم "سيلبرايت" نفسها كشركة تؤدّي دوراً واضحاً ومشروعاً ضمن منظومة العدالة الجنائية. ففي عرضٍ قدّمته للمستثمرين عام 2021، وصفت مهمّتها بـ"حماية الأرواح وإنقاذها، وتسريع تحقيق العدالة، والحفاظ على الخصوصية في المجتمعات حول العالم".[407] وتُصوّر الشركة منتجاتها في مجال التحليل الجنائي الرقمي كحلولٍ تتميّز بأربع وظائف أساسية: جمع البيانات، ومراجعتها، وتحليلها، وإدارتها.[408]

وتزعم "سيلبرايت" أنّها تسدّ فجوةً كبيرةً في مجال السلامة العامة. فبحسب ما تقول، تواجه أجهزة إنفاذ القانون مشكلاتٍ متزايدةٍ تتعلّق بحجم البيانات وتعقيدها، و"العمليات غير الفعّالة"، و"الأخلاقيات والمحاسبة".[409] ومن اللافت أنها تزعم امتلاكها قدرة فريدة على التعامل مع هذه المشكلة المرتبطة بالأخلاقيات والمحاسبة.

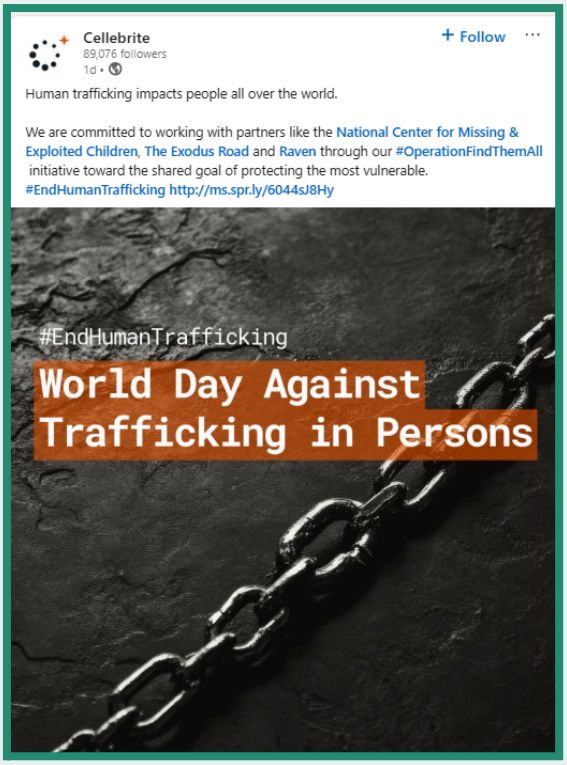
وتحافظ "سيلبرايت" على حضورٍ نشطٍ عبر وسائل التواصل الاجتماعي، بما في ذلك "فيسبوك" و"لينكد إن" ومنصّة "إكس" ("تويتر" سابقاً) و"يوتيوب". وتتبنّى الشركة نهجاً مشابهاً لمجموعة "إن إس أو" في هذا المجال، إذ تتناول في منشوراتها المناسبات المختلفة ذات الصلة بحقوق الإنسان والأعياد الوطنية والأنشطة اليومية لموظفيها. وكما هي الحال مع "إن إس أو"، تعتمد "سيلبرايت" هذه الاستراتيجية في بناء صورتها العامّة لصرف الانتباه عن الجدل الواسع الذي يحيط بها.

---

[407] "سيلبرايت". (2021). عرض للمستثمرين، نيسان/أبريل 2021، العرض 99.2 (Investor Presentation April 2021 Exhibit 99.2) [عرض تقديمي]. لجنة الأوراق المالية والبورصات. نيسان/أبريل متوفر على: https://web.archive.org/web/20211206044245/https://sec.report/Document/0001213900-21-020888/. [تم الاطلاع عليه في 19 آب/أغسطس 2025].

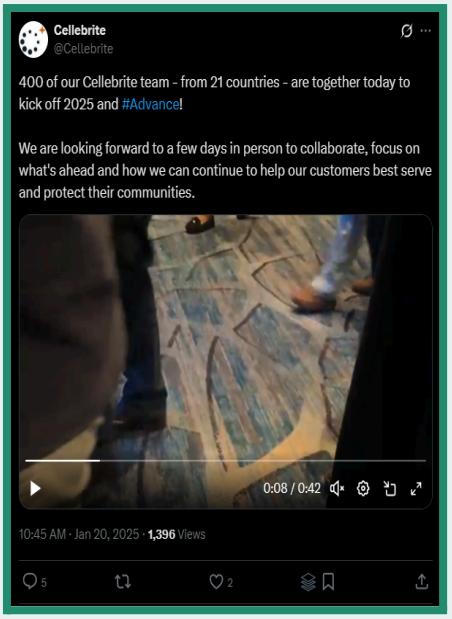
[408] "سيلبرايت". (2021). عرض للمستثمرين، نيسان/أبريل 2021، العرض 99.2 (Investor Presentation April 2021 Exhibit 99.2)

[409] شركة سيلبرايت للذكاء الرقمي م. (2025). *نموذج 20-F-Form* (*F.*). ص 61.

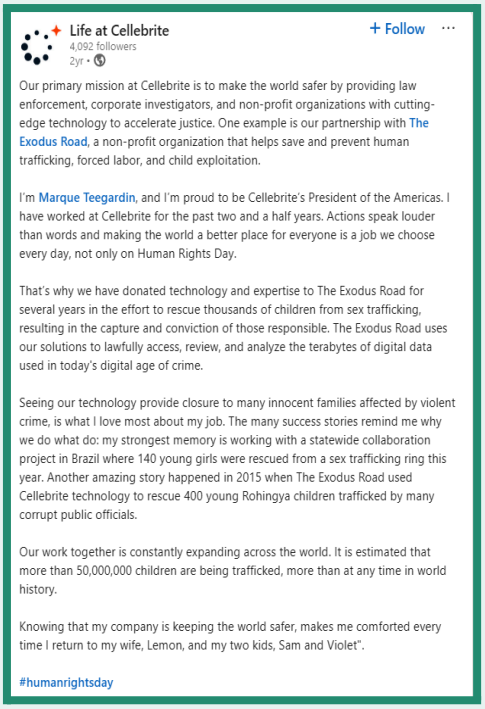


Cellebrite 89,076 followers 1d + Follow	سيلبرايت 89,076متابعاً منشور قبل يوم واحد +متابعة
Human trafficking impacts people all over the world. We are committed to working with partners like the National Center for Missing & Exploited Children, The Exodus Road and Raven through our #OperationFind ThemAll initiative toward the shared goal of protecting the most vulnerable. #EndHuman Trafficking http://ms.spr.ly/6044sJ8Hy	يؤثّر الإتجار بالبشر على الناس في جميع أنحاء العالم. نحن ملتزمون بالعمل مع شركائنا مثل "المركز الوطني للأطفال المفقودين والمستغَلين"، و"إكسودس رود (Exodus Road) و"رايفن" (Raven) من خلال مبادرتنا **#عملية_العثور_عليهم_جميعاً** بهدفٍ مشترك يتمثّل في حماية الفئات الأكثر ضعفاً. #إنهاء_الإتجار_بالبشر http://ms.spr.ly/6044sJ8Hy
#EndHumanTrafficking World Day Against Trafficking in Persons	#إنهاء_الإتجار_بالبشر اليوم العالمي لمكافحة الإتجار بالبشر

Cellebrite 89,075 followers 3w + Follow	سيلبرايت 89,075 متابع منشور قبل 3 أسابيع +متابعة
Happy 4th of July! us To those working on the front lines today, we appreciate your service and sacrifice. Happy Birthday, America! HAPPY 4TH OF JULY	عيد استقلال سعيد في الرابع من تموز/يوليو! إلى جميع العاملين في الصفوف الأمامية اليوم، نحن نُقدّر خدمتكم وتضحياتكم. عيد ميلاد سعيد يا أميركا! عيد استقلال سعيد في الرابع من تموز/يوليو



Cellebrite	سيلبرايت @ سيلبرايت
400 of our Cellebrite team - from 21 countries - are together today to kick off 2025 and #Advance! We are looking forward to a few days in person to collaborate, focus on what's ahead and how we can continue to help our customers best serve and protect their communities.	اجتمع 400 عضو من أعضاء فريق سيلبرايت – من 21 دولة – اليوم لافتتاح العام 2025 وبدء مبادرة #التطوّر! نتطلّع إلى قضاء بضعة أيام معاً للتعاون والتركيز على ما ينتظرنا في المستقبل، وعلى كيفية مواصلة مساعدة عملائنا في تقديم أفضل الخدمات وحماية مجتمعاتهم.
10:45 AM Jan 20, 2025-1,396 Views	10:45 صباحاً – 20 كانون الثاني/يناير 2025 – 1,396 مشاهدة


Life at Cellebrite
4,092 followers
2yr •
+ Follow ···

Our primary mission at Cellebrite is to make the world safer by providing law enforcement, corporate investigators, and non-profit organizations with cutting-edge technology to accelerate justice. One example is our partnership with The Exodus Road, a non-profit organization that helps save and prevent human trafficking, forced labor, and child exploitation.

I'm Marque Teegardin, and I'm proud to be Cellebrite's President of the Americas. I have worked at Cellebrite for the past two and a half years. Actions speak louder than words and making the world a better place for everyone is a job we choose every day, not only on Human Rights Day.

That's why we have donated technology and expertise to The Exodus Road for several years in the effort to rescue thousands of children from sex trafficking, resulting in the capture and conviction of those responsible. The Exodus Road uses our solutions to lawfully access, review, and analyze the terabytes of digital data used in today's digital age of crime.

Seeing our technology provide closure to many innocent families affected by violent crime, is what I love most about my job. The many success stories remind me why we do what do: my strongest memory is working with a statewide collaboration project in Brazil where 140 young girls were rescued from a sex trafficking ring this year. Another amazing story happened in 2015 when The Exodus Road used Cellebrite technology to rescue 400 young Rohingya children trafficked by many corrupt public officials.

Our work together is constantly expanding across the world. It is estimated that more than 50,000,000 children are being trafficked, more than at any time in world history.

Knowing that my company is keeping the world safer, makes me comforted every time I return to my wife, Lemon, and my two kids, Sam and Violet".

#humanrightsday

الحياة في سيلبرايت

4,092 متابع

منشور من سنتين

+متابعة

مهمّتنا الأساسية في سيلبرايت هي جعل العالم أكثر أماناً من خلال تزويد أجهزة إنفاذ القانون والمحقّقين في الشركات والمنظمات غير الربحية بتكنولوجيا متقدّمة تُسهم في تسريع تحقيق العدالة. ومن الأمثلة على ذلك شراكتنا مع منظمة "إكسودس رود"، وهي منظمة غير ربحية تساعد في مكافحة الإتجار بالبشر والعمل القسري واستغلال الأطفال.

أنا مارك تيغاردن، وأفتخر بكوني رئيس شركة سيلبرايت في أميركا. لقد عملتُ في سيلبرايت على مدى العامين والنصف الماضيَين. نحن نؤمن بأنّ الأفعال أبلغ من الأقوال، وأنّ جعل العالم مكاناً أفضل للجميع هو خيار نتّخذه كلّ يوم، وليس فقط في يوم حقوق الإنسان.

لهذا السبب، قدّمنا التكنولوجيا والخبرة لمنظمة "إكسودس رود" على مدى سنوات، في إطار جهودها لإنقاذ آلاف الأطفال من الإتجار الجنسي، ما أدّى إلى توقيف المتورطين وإدانتهم. وتستخدم "إكسودس رود" حلولنا للوصول القانوني إلى حجمٍ هائلٍ من البيانات الرقمية ومراجعتها وتحليلها في زمن الجريمة الرقمية اليوم.

إنّ مشاهدة تقنياتنا وهي تمنح الأمل لعائلاتٍ بريئةٍ تأثّرت بجرائم عنيفة هي أكثر ما أحبّه في عملي، وتذكّرني قصص النجاح الكثيرة بسبب تأديتنا عملنا: أكثر ما رسخ في ذهني كان من مشروع تعاونٍ على مستوى ولايةٍ في البرازيل، حيث جرى إنقاذ 140 فتاة شابة من شبكةٍ للإتجار الجنسي هذا العام. كما حدثت قصةٌ مميزةٌ أخرى في العام 2015 عندما استخدمت منظمة "إكسودس رود" تقنيات سيلبرايت لإنقاذ 400 طفل من الروهينغا كانوا ضحايا للإتجار من قبل عددٍ من المسؤولين الفاسدين.

عملنا المشترك يتوسّع باستمرار حول العالم. وتشير التقديرات إلى أنّ أكثر من 50,000,000 طفل يتعرّضون للإتجار اليوم، وهو رقمٌ غير مسبوق في التاريخ.

ومعرفتي بأنّ شركتي تساهم في جعل العالم أكثر أماناً تمنحني شعوراً بالراحة في كلّ مرة أعود فيها إلى زوجتي ليمون وطفليّ سام وفايوليت.

#يوم_حقوق_الإنسان

الصور 20-23: تحتفي "سيلبرايت" على منصّتَي "إكس" و"لينكد إن" بالأعياد الوطنية، وتنشر منشوراتٍ تتعلّق بأيام التوعية بحقوق الإنسان، بالإضافة إلى تحديثاتٍ حول الأنشطة اليومية لموظّفيها، في محاولةٍ واضحة لإضفاء طابعٍ إنسانيٍّ على علامتها التجارية وربطها بقضايا حقوق الإنسان.

تسعى "سيلبرايت" بشكلٍ متكرّر إلى ترسيخ هويتها كشركةٍ حريصةٍ كلّ الحرص على حقوق الإنسان والامتثال الصارم للمعايير الأخلاقية. وفي محاولةٍ لمعالجة المخاوف الأخلاقية المحتملة والمرتبطة بمنتجاتها، أعلنت الشركة في 13 أيلول/سبتمبر 2021 عن إنشاء لجنة الأخلاق والنزاهة، وهيئة استشارية للأخلاق.[410] ومن بين الأعضاء السبعة الحاليين في لجنة الأخلاق والنزاهة، يرتبط ستة منهم بشكلٍ مباشرٍ بأجهزة إنفاذ القانون في الولايات المتحدة أو إسرائيل، أو بجيش الاحتلال الإسرائيلي، أو بجهاز الجمارك وحماية الحدود الأميركي.[411] وتضم اللجنة مثلاً الأستاذة في جامعة هارفارد غابرييلا بلوم، التي قد شغلت منصب المستشارة القانونية رفيعة المستوى في جيش الاحتلال الإسرائيلي خلال الانتفاضة الفلسطينية الثانية، وساهمت في تطوير المعايير القانونية التي تحدّد أنواع الاغتيالات المقبولة خارج نطاق القضاء.[412] أما موشيه هالبرتال، وهو عضوٌ آخر في اللجنة، فكان أحد واضعي "مدوّنة الأخلاق" الخاصة بجيش الاحتلال. كما يُعدّ عضو اللجنة دورون هيرمان، الذي يُقدَّم على أنّه "خبير في مجال حماية الأطفال عبر الإنترنت"، من الداعمين البارزين لعمليات إسرائيل في غزة، والتي وصفتها عدّة منظمات حقوقية بأنّها إبادة جماعية.[413] وفي 20 تشرين الأول/أكتوبر 2023، صرّح هيرمان بأنّ "غريتا تونبرغ تدعم تنظيم داعش" بعد أن دعت إلى وقف إطلاق النار في غزة و"تحقيق العدالة والحرية للفلسطينيين" عبر منصّة "إكس".[414]

وعلى صفحة "سيلبرايت" المخصّصة لعرض سياساتها الأخلاقية، تزعم أنّها تطبّق "ضوابط صارمة" لضمان استخدام تقنياتها في التحقيقات القانونية فقط.[415] كما تؤكد أنّها تحظر بيع منتجاتها للدول الخاضعة لعقوبات من الاتحاد الأوروبي أو إسرائيل أو المملكة المتحدة أو الولايات المتحدة، فضلاً عن تلك المدرجة في القائمة السوداء لفرقة العمل المعنية بالإجراءات المالية. ومع ذلك، أفادت تقارير بأنّ الشركة باعت تقنياتها بالفعل إلى دولٍ مُدرجة في قائمة فرقة العمل المعنية بالإجراءات المالية السوداء (مثل ميانمار) وأخرى مُدرجة في قائمتها الرمادية (مثل فنزويلا).[416]

---

[410] "سيلبرايت" (2021أ). "*سيلبرايت" تعلن عن تشكيل لجنة الأخلاق والنزاهة*. (*Cellebrite Announces Formation of Ethics & Integrity Committee*.) [متاح على الإنترنت] سيلبرايت. متوفر على: https://cellebrite.com/en/cellebrite-announces-formation-of-ethics-integrity-committee/ [تم الاطلاع عليه في 19 آب/أغسطس 2025].

[411] "سيلبرايت" (2024). *الأخلاق والنزاهة*. (*Ethics & Integrity*). [متاح على الإنترنت] متوفر على: https://cellebrite.com/en/ethics-integrity/ [تم الاطلاع عليه في 19 آب/أغسطس 2025].

[412] بارشاد، أ. (2018). غابرييلا بلوم الإسرائيلية ساعدت في صياغة قوانين الحرب بالطائرات المسيّرة. بعد ما يقرب من عقدين، تعبر عن ندمها. (*Israel's Gabriella Blum Helped Write the Laws of Drone Warfare. Nearly Two Decades Later, She Has Regrets*). [متاح على الإنترنت] ذا إنترسيبت. متوفر على: https://theintercept.com/2018/10/07/israel-palestine-us-drone-strikes/ [تم الاطلاع عليه في 11 آب/أغسطس 2025].

[413] بتسيلم: المركز الإسرائيلي للمعلومات حول حقوق الإنسان في الأراضي المحتلة (2025). *إبادتنا الجماعية*. (B'Tselem: The Israeli Information Center for Human Rights in the Occupied Territories (2025). *Our Genocide*.) [متاح على الإنترنت] *بتسليم* (*B'tselem*) متوفر على: https://www.btselem.org/publications/202507_our_genocide [تم الاطلاع عليه في 11 آب/أغسطس 2025].

[414] هيرمان، د. (2023) [منصة "إكس" ("تويتر" سابقاً)] 20 تشرين الأول/أكتوبر، 2023. متوفر على: https://x.com/D0ronhe/status/1715409227332669789 (تم الاطلاع عليه في 23 تموز/يوليو 2025).

[415] "سيلبرايت" (2024). *الأخلاق والنزاهة*. (*Ethics & Integrity*).

[416] كرابيفا، ن. وسوجياما، هـ. (2021). ما لا تستطيع شركة التجسس "سيلبرايت" إخفاءه عن المستثمرين. *أخبار وتحديثات "أكسس ناو"* (What Spy Firm Cellebrite Can't Hide from Investors. *Access Now News & Updates*.) متوفر على: https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

الصورة 24: سحابةٌ من الكلمات من صفحة "الأخلاق والنزاهة" على موقع "سيلبرايت" (بعد إزالة الأسماء وكلمة "سيلبرايت"). وكما تفعل شركات بيع برامج التجسّس التجارية الأخرى، تربط "سيلبرايت" نفسها بـ"الأطراف الصالحة" عبر استخدام مصطلحاتٍ تسويقيةٍ مثل "الحلول"، و"الخصوصية"، و"القانون"، و"النزاهة"، و"السلامة"، و"الأمن"، و"حقوق الإنسان".[417]

وتُشير "سيلبرايت" في نموذج F-20 لعام 2024 لدى لجنة الأوراق المالية والبورصات إلى أنّ "العملاء قد يستخدمون المنتجات بطريقةٍ تتعارض، أو قد يُنظر إليها على أنّها تتعارض، مع مبادئ حقوق الإنسان".[418] وتحذّر الشركة مستثمريها من أنّ ذلك قد يضرّ بسمعتها. وعلى الرغم من أنّها تؤكّد سعيها للتعامل فقط مع عملاء يستخدمون منتجاتها بطريقةٍ قانونيةٍ وأخلاقيةٍ، وأنّها قد تمتنع عن الدخول في علاقاتٍ تجارية مع جهاتٍ تتعارض أنشطتها مع "مهمّتنا التنظيمية أو قيمنا"، إلا أنّها تعترف بعد جملتين في الوثيقة نفسها بأنّها لا تستطيع "التحقّق بسهولة أو بسرعة" من استخدام العملاء لمنتجاتها "لأغراضٍ قانونية".[419] وتوضح الشركة أنّها تُلزم العملاء بتوقيع اتفاقية ترخيص المستخدم النهائي التي "تحظر" صراحةً إساءة استخدام منتجاتها أو انتهاك قوانين حقوق الإنسان.[420] وإذا حدث ذلك، تحتفظ "سيلبرايت" بحقّها في إنهاء الترخيص والمطالبة بتعويضاتٍ عن أيّ خسائر تتكبدها.

وفي محاولةٍ لدحض الادعاءات المرتبطة بانتهاكات حقوق الإنسان، تقدّم "سيلبرايت" – على غرار مجموعة "إن إس أو" – صفحة "الخرافات مقابل الحقائق" على موقعها الإلكتروني، وتزعم فيها أنّها ليست شركة اختراق، ولا تدير برامج تجسّس، ولا تمارس أيّ سلوك غير أخلاقي.[421] وتعتمد كثيرٌ من "حقائقها" على تعريفاتٍ مضلّلةٍ للمصطلحات لنفي الادعاءات. فعلى

---

[417] "سيلبرايت" (2024). *الأخلاق والنزاهة*. (*Ethics & Integrity*).

[418] شركة "سيلبرايت للذكاء الرقمي م." (2025). نموذج *Form 20-F-20* (*F.*). ص 20.

[419] شركة "سيلبرايت للذكاء الرقمي م." (2025). نموذج *Form 20-F-20* (*F.*). ص 31.

[420] شركة "سيلبرايت للذكاء الرقمي م." (2025). نموذج *Form 20-F-20* (*F.*). ص 32.

[421] "سيلبرايت". (2025). *"سيلبرايت" تقدم معلومات حول أعمالها وحلولها – "سيلبرايت"*. (*Cellebrite Provides Facts about Its Business and Solutions - Cellebrite*).

سبيل المثال، تذكر الشركة: "الاختراق يعني الوصول غير المصرّح به إلى نظامٍ ما، وهو ما ينطوي على نشاطٍ غير قانوني. لذلك، من غير الدقيق وصف سيلبرايت بأنّها 'شركة اختراق الهواتف'... عندما تُستخدم هذه الحلول بشكلٍ قانوني".[422]

وفي مقابلةٍ أجرتها صحيفة "كلكاليست" في كانون الثاني/يناير 2025 مع يوسي كارميل، المدير التنفيذي السابق لـ"سيلبرايت"، قدّم رؤية حول كيفية تسويق الشركة لهويّتها وعملائها وأهدافها ومنتجاتها. وقد نفى مزاعم ارتكاب أي مخالفاتٍ أو أنّ "سيلبرايت تعمل في منطقة رمادية" من الناحية القانونية، مؤكداً أنّها "تعمل في دولٍ تلتزم بالقانون وتتعاون حصرياً مع وكالات إنفاذ القانون الشرعية. نحن أكثر ملاً ممّا يعتقده الناس". وعند تلخيصه لعمل الشركة خلال مسيرته التي استمرّت عقدين من الزمن، قال: "لو طُلب مني وصف سيلبرايت بكلمة واحدة لكانت آمنة وليست مثيرة للاهتمام".[423]

ومع ذلك، أظهرت منظماتٌ مثل منظمة العفو الدولية،[424] و"أكسس ناو"،[425] ومنظمة الخصوصية الدولية[426] أنّ "سيلبرايت" لا تمتلك معايير جيدة في إيلاء العناية الواجبة بحقوق الإنسان، ما أدّى إلى استخدام دولٍ استبدادية لتقنياتها بطرق تنتهك القانون الدولي، بما في ذلك المساعدة في جمع الأدلة تمهيداً لاعتقال معارضين سياسيين وتعذيبهم. كما تؤكّد منظمة العفو الدولية أنّه حتى إذا كانت منتجات "سيلبرايت" لا تنطبق عليها التعريفات الدقيقة لبرامج التجسّس، إلّا انّها تثير مخاوف جسيمة تتعلّق بحقوق الإنسان، نظراً لقدرتها على تقويض خصوصية الأجهزة بالكامل ومراقبة الاتصالات الخاصة من دون موافقة المستخدم.[427]

---

[422] "سيلبرايت". (2025). *"سيلبرايت" تقدم معلومات حول أعمالها وحلولها – "سيلبرايت"*. (*Cellebrite Provides Facts about Its Business and Solutions - Cellebrite*).

[423] شولمان، س. (2025). *من شركة ناشئة بموارد ذاتية إلى قوة تكنولوجية بقيمة 5 مليارات دولار*. (*From Bootstrapped Startup to a $5B powerhouse*).

[424] منظمة العفو الدولية (2024). *صربيا: السلطات تستخدم برامج التجسس وأدوات استخراج بيانات التحليل الجنائي من "سيلبرايت" لاختراق هواتف الصحافيين والنشطاء*. (*Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists*)

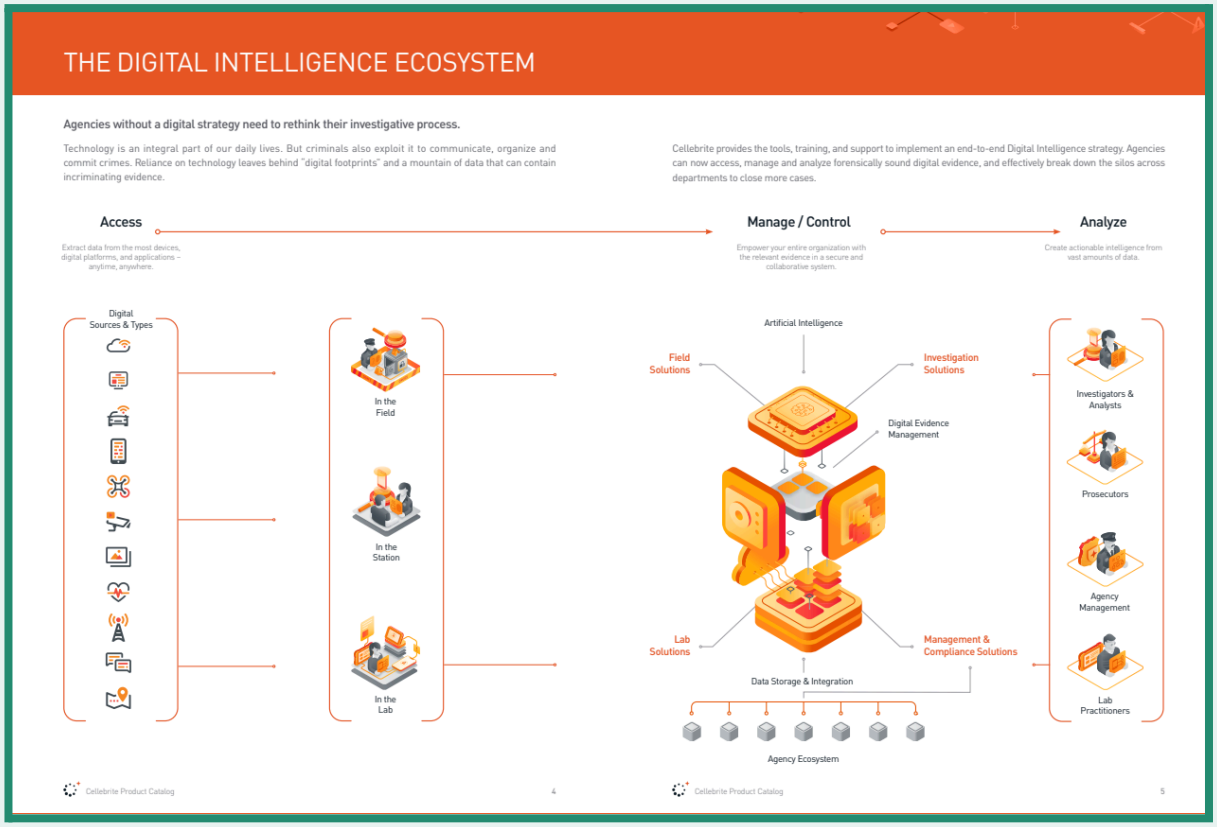
[425] كرابيفا، ن. وسوجياما، هـ. (2021). ما لا تستطيع شركة التجسس "سيلبرايت" إخفاءه عن المستثمرين. *أخبار وتحديثات أكسس ناو* (What Spy Firm Cellebrite Can't Hide from Investors. *Access Now News & Updates*).

[426] منظمة الخصوصية الدولية (2019). شركة المراقبة "سيلبرايت" تكتشف وسيلة استغلال جديدة: التجسس على طالبي اللجوء. *مقالات مطوّلة من منظمة الخصوصية الدولية*. (Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers. *Privacy International Long Reads*.) متوفر على:
https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[427] منظمة العفو الدولية (2024). *صربيا: السلطات تستخدم برامج التجسس وأدوات استخراج بيانات التحليل الجنائي من "سيلبرايت" لاختراق هواتف الصحافيين والنشطاء*. (*Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists*)

المنتجات والقدرات الرئيسية

تقدّم "سيلبرايت" منتجاتها ضمن ثلاث فئاتٍ رئيسية: "الجمع والمراجعة"، و"التحليل والتحقيق"، و"الإدارة والحماية".[428] [429] وتُعرف الشركة أساساً بجهازها الشهير جهاز استخراج الأدلة الجنائية العالمي (UFED)، الذي يُستخدم إلى جانب أداة التحليل المادي (Physical Analyzer)، ويمنح العملاء القدرة على فتح مجموعةٍ واسعةٍ من الأجهزة المحمولة واستخراج البيانات منها لتحليلها. كما توفّر "سيلبرايت" حالياً حلولاً متخصّصة في التصوير الجنائي لأجهزة الحاسوب العاملة بنظامَيْ "ماك" و"ويندوز".



الصورة 25: تستعرض "سيلبرايت" في كتيّب منتجاتها لعام 2020 ما تصفه بـ"نظام الاستخبارات الرقمية المتكامل"، وتوضّح المنتجات التي تنتمي إلى كلّ قسمٍ من أقسام هذا النظام، ما يقدّم لمحةً عن أنواع البيانات التي تستهدفها الشركة.

THE DIGITAL INTELLIGENCE ECOSYSTEM Agencies without a digital strategy need to rethink their investigative process.	النظام البيئي للاستخبارات الرقمية على الوكالات التي لا تعتمد استراتيجية رقمية أن تعيد التفكير في آلياتها التحقيقية.

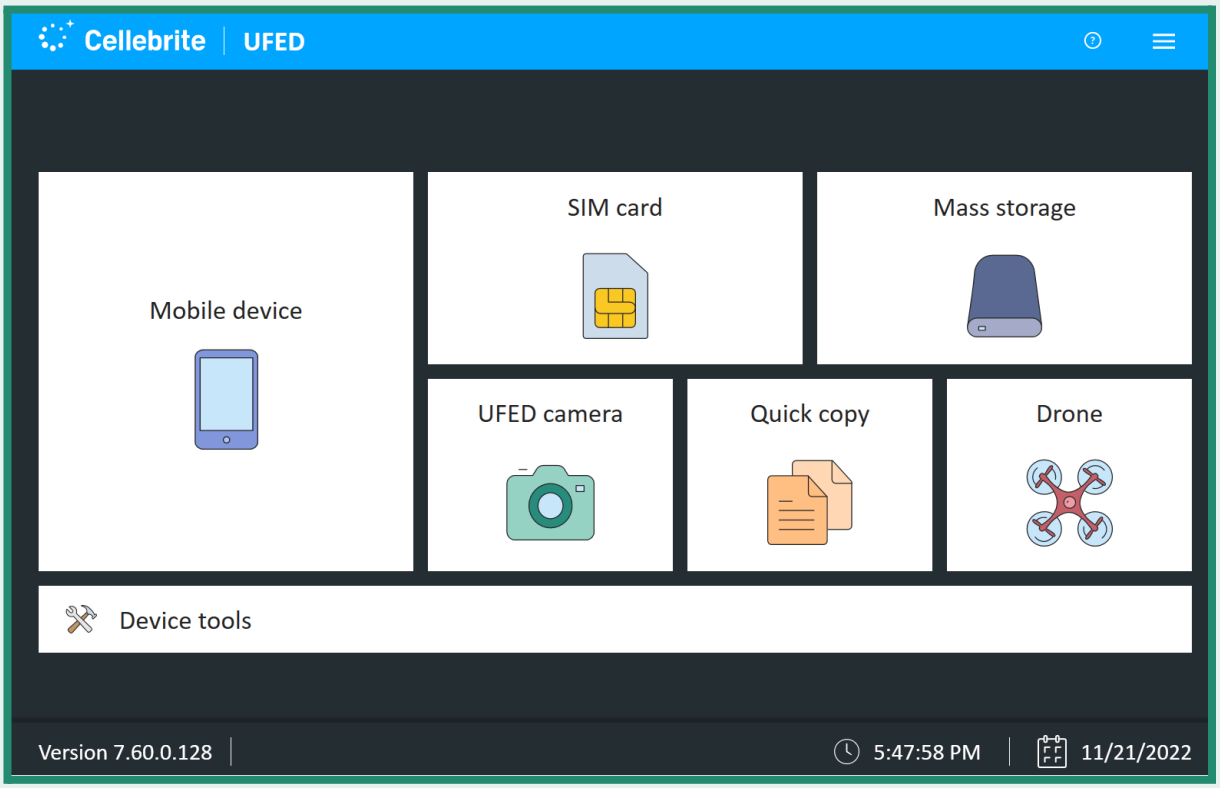
[428] "سيلبرايت" (2023). *الصفحة الرئيسية لشركة "سيلبرايت"*. (*Cellebrite Home Page*.) [متاح على الإنترنت] cellebrite.com. متوفر على: https://cellebrite.com/en/home [تم الاطلاع عليه في 15حزيران/يونيو 2025].

[429] "لقد عبّرت "سيلبرايت" عن هذه الفئات بطرقٍ مختلفة مع الوقت. فعلى سبيل المثال، صنّفت منتجاتها في دليلها لعام 2020 ضمن فئات: "الوصول"، و"الإدارة/التحكم"، و"التحليل".

Technology is an integral part of our daily lives. But criminals also exploit it to communicate, organize and commil crimes. Reliance on technology leaves behind "digital footprints and a mountain of data that can contain incriminating evidence.	فالتكنولوجيا أصبحت جزءاً أساسياً من حياتنا اليومية، غير أنّ المجرمين يستغلّونها بدورهم للتواصل والتنظيم وارتكاب الجرائم. ويخلّف الاعتماد على التكنولوجيا وراءه "بصمات رقمية" وكمّاً هائلاً من البيانات التي قد تحتوي على أدلّة إدانة.
Extract data from the most devices, digital platforms, and applications- anytime, anywhere.	استخرج البيانات من أكبر عدد ممكن من الأجهزة والمنصّات الرقمية والتطبيقات – في أيّ وقتٍ ومن أيّ مكان.
Digital sources and types In the field In the station In the lab	المصادر والأنواع الرقمية في الميدان في المركز في المختبر
Cellebrite provides the tools, training, and support to implement an end-to-end Digital Intelligence strategy. Agencies can now access, manage and analyze forensically sound digital evidence, and effectively break down the silos across departments to close more cases. Manage / Control Empower your entire organization with the relevant evidence in a secure and collaborative system Analyze Create actionable intelligence from vast amounts of data	توفّر سيلبرايت الأدوات والتدريب والدعم اللازم لتنفيذ استراتيجية متكاملة في مجال الاستخبارات الرقمية. وبات بإمكان الأجهزة اليوم الوصول إلى الأدلة الرقمية الموثوقة من الناحية الجنائية وإدارتها وتحليلها، مع تعزيز التعاون بين الأقسام لكشف المزيد من القضايا. الإدارة / التحكّم تمكين المؤسسة بأكملها من الوصول إلى الأدلة ذات الصلة ضمن نظامٍ آمنٍ وتعاوني. التحليل تحويل الكمّ الهائل من البيانات إلى معلوماتٍ استخباراتية قابلة للتنفيذ.
Artificiall intelligence Field solutions Investigative solitions Digital evidence management Lab solutions Management and compliance solutions Data storage and intrlegration Agency ecosystem	الذكاء الاصطناعي حلول ميدانية حلول التحقيق إدارة الأدلة الرقمية حلول المختبرات حلول الإدارة والامتثال تخزين البيانات وتكاملها منظومة الوكالات
Investigators and analysts Prosecuters Agency mangement Lab prractitioners	المحققون والمحلّلون المدّعون العامّون إدارة الوكالات المختصّون في المختبرات

تتضمّن حزمة منتجات UFED أيضاً إمكاناتٍ سحابيةٍ تمكّن العملاء من الوصول إلى المحتوى المخزّن في السحابة والمرتبط بالأجهزة المستهدفة، بما في ذلك البيانات المحذوفة. وتُتيح منتجات إدارة البيانات والتحليل التي تقدّمها "سيلبرايت" – كما تشير منظمة العفو الدولية – تحليل بيانات أهدافٍ متعدّدةٍ في الوقت نفسه، ومساعدة المشغّلين في فهم الشبكات الاجتماعية وشبكات التواصل، وهو ما قد يكون مفيداً في تحليل شبكات المعارضين والصحافيين وأنشطة الاحتجاج.[430]

وتعتمد حزمة UFED على ثغرات يوم الصفر الشديدة التطوّر للوصول إلى الأجهزة المحمولة واستخراج البيانات منها.[431] وبعد حصول العملاء على إمكانية الوصول إلى الجهاز، يستخدمون منتجات سيلبرايت الأخرى لتحليل البيانات وجمع الأدلة الرقمية المتعلّقة بالجرائم المزعومة.



الصورة 26: الشاشة الرئيسية لجهاز UFED كما تظهر على صفحة المنتج في موقع "سيلبرايت".[432]

[430] منظمة العفو الدولية (2024أ). صربيا: *"سجن رقمي": المراقبة وقمع المجتمع المدني في صربيا*. (*Serbia: 'A Digital Prison': Surveillance and the Suppression of Civil Society in Serbia*). [متاح على الإنترنت] *منظمة العفو الدولية*، لندن، المملكة المتحدة: منظمة العفو الدولية، ص 9. متوفر على: https://www.amnesty.org/en/documents/eur70/8813/2024/en/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[431] منظمة العفو الدولية (2024أ). صربيا: *"سجن رقمي": المراقبة وقمع المجتمع المدني في صربيا*. (*Serbia: 'A Digital Prison': Surveillance and the Suppression of Civil Society in Serbia*).

[432] "سيلبرايت" (2024). *"سيلبرايت" UFED | الوصول إلى بيانات أجهزة الهاتف المحمول وجمعها*. (*Cellebrite UFED | Access and Collect Mobile Device Data*)

Cellebrite	سيلبرايت
UFED	جهاز استخراج الأدلة الجنائية العالمي (UFED)
SIM card	شريحة SIM
Mass storage	وحدة التخزين الضخمة
Mobile device	الجهاز المحمول
UFED camera	كاميرا UFED
Quick copy	النسخ السريع
Drone	الطائرة المسيّرة
Device tools	أدوات الجهاز
Version 7.60.0.128	الإصدار: 7.60.0.128
5:47:58 PM	5:47:58 مساءً
11/21/2022	21/11/2022

توفّر "سيلبرايت" لمستخدميها أساليب مختلفة تبعاً لما إذا كان الجهاز المستهدف مقفلاً برمز مرور معروف أم لا.[433] وقد أدّت تسريباتٌ متكرّرة لدلائل استخدام "سيلبرايت" وبرمجياتها إلى دفع الشركة لتغيير الطريقة التي تقدّم بها خدمات فكّ القفل الأكثر تقدّماً، خشية أن يحصل عامة الناس على ثغرات يوم الصفر التي تعتمد عليها في اختراق الأجهزة.[434] وتوفّر الشركة أنواعاً مختلفة من تقنيات الوصول لعملائها في القطاعين العام والخاص، وتتيح أكثر قدراتها تطوّراً – غير المتوفّرة عبر جهاز UFED - للعملاء الذين يرسلون أجهزتهم المستهدفة إلى مختبرات "سيلبرايت".[435]

ووفقاً لتقارير عامة، يبلغ سعر أجهزة UFED الجديدة نحو 6,000 دولار (مع الإشارة إلى أنّ النماذج الأقدم تُباع بأسعارٍ أقل بكثير عبر منصات مثل "إيباي").[436] [437] وفي العام 2022، تسرّب عقدٌ مبرمٌ على الإنترنت بين أحد أقسام الشرطة في الولايات المتحدة وشركة "سيلبرايت"،[438] أظهر أنّ بعض منتجات الشركة تُباع مقابل تكلفة لمرة واحدة مع اشتراكٍ سنوي. وتشير الوثيقة إلى أنّ منتج "سيلبرايت بريميوم" (Cellebrite Premium)، الذي يوفّر قدراتٍ أوسع في فكّ القفل (ولا يظهر حالياً على موقع الشركة)، تبلغ كلفته 14,000 دولار سنوياً مقابل 35 عملية فتح. أما برنامج "باث فايندر"

---

[433] منظمة العفو الدولية (2024أ). *صربيا: "سجن رقمي": المراقبة وقمع المجتمع المدني في صربيا*. (*Serbia: 'A Digital Prison': Surveillance and the Suppression of Civil Society in Serbia*).

[434] "دي دي أو إس سيكريتس" (DDOSSecrets) (2024). *نتائج البحث عن "سيلبرايت" - الهجوم الموزع لحجب الخدمة*. (*Search Results for 'Cellebrite' - Distributed Denial of Secrets*) *[متاح على الإنترنت] متوفر على:* https://ddosecrets.com/search?query=cellebrite [تم الاطلاع عليه في 30 آب/أغسطس 2025].

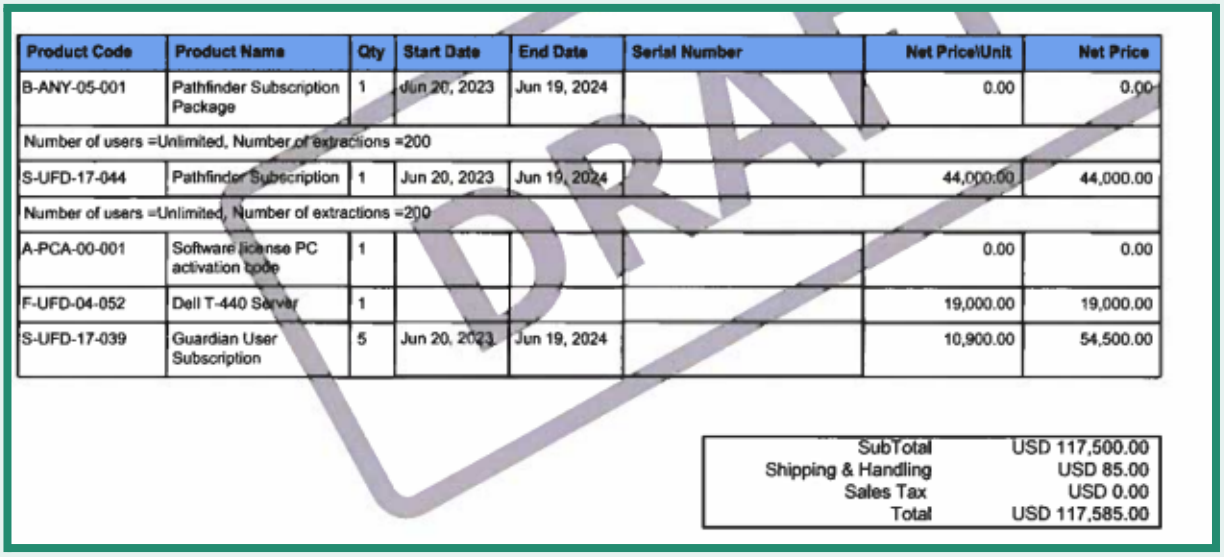
[435] منظمة العفو الدولية (2024أ). *صربيا: "سجن رقمي": المراقبة وقمع المجتمع المدني في صربيا*. (*Serbia: 'A Digital Prison': Surveillance and the Suppression of Civil Society in Serbia*).

[436] سويرينجن، ج. (2019). أداة اختراق الهواتف المفضلة لدى الشرطة تُباع على موقع "إيباي". *مجلة نيويورك: "إنتليجنسر"*. (Cops' Favorite Phone Hacking Tool Is Being Sold on eBay. *NY Mag: Intelligencer*.) [متاح على الإنترنت] متوفر على: https://nymag.com/intelligencer/2019/02/cellebrite-phone-hacking-tool-is-being-sold-on-ebay.html [تم الاطلاع عليه في 27 شباط/فبراير 2022].

[437] "إيباي"(2025). *"سيلبرايت" UFED | بحث "إيباي"*. (*Cellebrite UFED | eBay search*) *[متاح على الإنترنت] متوفر على:* https://www.ebay.com/shop/cellebrite-ufed?_nkw=cellebrite+ufed [تم الاطلاع عليه في 30 آب/أغسطس 2025]

[438] مجهول، (2022). *حزمة عروض أسعار "سيلبرايت" المسرّبة*. (*Leaked Cellebrite Quote Package*) *[متاح على الإنترنت] متوفر على:* https://agenda.canyoncounty.id.gov/SupportDoc/GetSupportingDoc?supportDocID=1023 [تم الاطلاع عليه في 4 آب/أغسطس 2025]

(Pathfinder)، وهو أداة تحليلٍ قائمة على الذكاء الاصطناعي، فتبلغ كلفته 44,000 دولار سنوياً مع تكلفة لمرة واحدة قدرها 19,000 دولار. كما يكلّف منتج "غارديان" (Guardian)، المخصّص لتخزين نتائج التحليل الجنائي في السحابة، نحو 10,900 دولار سنوياً لكلّ وكالة.



Product Code	Product Name	Qty	Start Date	End Date	Serial Number	Net Price/Unit	Net Price
B-ANY-05-001	Pathfinder Subscription Package	1	Jun 20, 2023	Jun 19, 2024		0.00	0.00
Number of users =Unlimited, Number of extractions =200							
S-UFD-17-044	Pathfinder Subscription	1	Jun 20, 2023	Jun 19, 2024		44,000.00	44,000.00
Number of users =Unlimited, Number of extractions =200							
A-PCA-00-001	Software license PC activation code	1				0.00	0.00
F-UFD-04-052	Dell T-440 Server	1				19,000.00	19,000.00
S-UFD-17-039	Guardian User Subscription	5	Jun 20, 2023	Jun 19, 2024		10,900.00	54,500.00

SubTotal	USD 117,500.00
Shipping & Handling	USD 85.00
Sales Tax	USD 0.00
Total	USD 117,585.00

الصورة 27: عرض أسعار مُسرَّب يُظهر التكاليف التقديرية لبعض خدمات "سيلبرايت".[439]

رمز المنتج	اسم المنتج	الكمية	تاريخ البدء	تاريخ الانتهاء	الرقم التسلسلي	السعر الصافي/الوحدة	السعر الصافي
B-ANY-05-001	اشتراك في حزمة باثفايندر	1	20 حزيران/يونيو 2023	19 حزيران/يونيو 2024		0.00	0.00
عدد المستخدمين = غير محدود، عدد عمليات الاستخراج = 200							
S-UFD-17-044	حزمة باثفايندر	1	20 حزيران/يونيو 2023	19 حزيران/يونيو 2024		44,000.00	44,000.00
عدد المستخدمين= غير محدود، عدد عمليات الاستخراج = 200							
A-PCA-00-001	رمز تفعيل ترخيص البرنامج على الحاسوب	1				0.00	0.00
F-UFD_04_052	خادم ديل T-440	1				19,000.00	19,000.00
S-UFD-17-039	الاشتراك بالمستخدم "غارديان"	5	20 حزيران/يونيو 2023	19 حزيران/يونيو 2024		10,900.00	54,500.00

[439] مجهول، (2022). *حزمة عروض أسعار "سيلبرايت" المسرّبة.* (Leaked Cellebrite Quote Package)

المبلغ الإجمالي	$117,500.00
الشحن والتوصيل	$85.00
ضريبة المبيعات	$0.00
المجموع	$117,585.00

هجمات بارزة

في 15 أيار/مايو 2013، داهمت السلطات البحرينية منزل محمد السنكيس، الناشط السياسي وشقيق المعارض عبد الجليل السنكيس الذي اعتُقل لدوره في احتجاجات الربيع العربي، بينما كان محمد ناشطاً بارزاً يدافع عن حقوق الطبقة العاملة والفقراء في البحرين.[440]

أفاد محمد السنكيس بأنّه تعرّض منذ لحظة اعتقاله للتعذيب والضرب، ونُقل إلى مبنى رقم 10 في سجن "جو" البحريني من دون معرفة السبب. كما أُجبر على حلق لحيته بالقوّة وتعرّض لإصابات في الرأس والعنق جرّاء الضرب.[441]

وصادرت الشرطة البحرينية هاتفه أثناء الاعتقال، واستخدمت جهاز UFED لفكّ قفل هاتفه واستخراج بياناته الشخصية. وبحسب موقع "ذا إنترسيبت"، أعدّت المديرية العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني تقريراً عن محتوى هاتف السنكيس باستخدام تقنيات "سيلبرايت"، وقدّمته كدليلٍ في محاكمته بتهمة المشاركة في مؤامرة جنائية.[442] كما استُخدمت تقنيات "سيلبرايت" لتوثيق محادثاته على واتساب وصوره لتقديمها كأدلّة ضده. وقد حُكم عليه بالسجن عشر سنوات،[443] ثمّ نال عفواً ملكياً في نيسان/أبريل 2024 بعد أن قضى أحد عشر عاماً في السجن.[444]

ووفقاً لمنظمة "أكسس ناو"، استُخدمت تقنيات UFED كذلك في ملاحقة ناشطٍ حقوقي آخر تعرّض للتعذيب وحُكم عليه بالسجن لمدة 15 عاماً.[445]

3.4 "سايتو تيك" (المعروفة سابقاً بـ"كانديرو")

"نتطلّع إلى تلبية احتياجاتكم في مجال الاستخبارات السيبرانية بأعلى مستويات النزاهة المهنية".

---

[440] بيدل، س. وديزمخ، ف. (2016). *استخدام برنامج "سيلبرايت" لاختراق الهواتف في ملاحقة معارض تعرّض للتعذيب*. (*Phone-Cracking: Cellebrite Software Used to Prosecute Tortured Dissident*).

[441] بيدل، س. وديزمخ، ف. (2016). *استخدام برنامج "سيلبرايت" لاختراق الهواتف في ملاحقة معارض تعرّض للتعذيب*. (*Phone-Cracking: Cellebrite Software Used to Prosecute Tortured Dissident*).

[442] بيدل، س. وديزمخ، ف. (2016). *استخدام برنامج "سيلبرايت" لاختراق الهواتف في ملاحقة معارض تعرّض للتعذيب*. (*Phone-Cracking: Cellebrite Software Used to Prosecute Tortured Dissident*).

[443] بحريني ليكس (2021). 18 *يوماً على إضراب السجين البحريني محمد السنكيس وسط تردي حالته الصحية*. *[متاح على الإنترنت] بحريني ليكس. متوفر على: https://bahrainileaks.com/%D8%A7%D9%84%D8%B3%D9%86%D9%83%D9%8A%D8%B3/ [تم الاطلاع عليه في 22 آب/أغسطس 2025].*

[444] ريكت، أ. (2025). *البحرين تحتجز ناشطاً بسبب منشورات على وسائل التواصل الاجتماعي في اليوم الأخير من اختبارات ما قبل الموسم للفورمولا 1*. (*Bahrain Detains Activist for Posts on Final Day of F1 pre-season Testing*.) *[متاح على الإنترنت] ميدل ايست آي* Middle East Eye). *متوفر على:* https://www.middleeasteye.net/news/bahrain-detains-activist-social-media-posts-final-day-f1-pre-season-testing [تم الاطلاع عليه في 30 آب/أغسطس 2025]

[445] كرابيفا، ن. وسوجياما، هـ. (2021). ما لا تستطيع شركة التجسس "سيلبرايت" إخفاءه عن المستثمرين. (What Spy Firm Cellebrite Can't Hide from Investors. *Access Now News & Updates*).

- نائب رئيس المبيعات المجهول في شركة "كانديرو" في ختام مقدّمة عرضٍ تجاريٍّ مسرّب، نُشر عام 2020[446]

نبذة عن الشركة

تُعدّ شركة "سايتو تيك م." (סאייטו טק בע"מ، رقم التسجيل: 515126605،[447] المعروفة سابقاً بـ"كانديرو") شركة مراقبة سيبرانية مقرّها في إسرائيل، تأسّست عام 2014 على يد يعقوب فايتزمان وإيرن شورير اللذان عملا سابقاً في مجموعة "إن إس أو"، وقبلها في الوحدة 8200 في الاستخبارات العسكرية السيبرانية التابعة لجيش الاحتلال الإسرائيلي.[448] تبيع "سايتو تيك" برامج تجسّس تستهدف أجهزة الكمبيوتر والخوادم والهواتف المحمولة،[449] وتزعم أنّها تتعامل فقط مع الوكالات الحكومية حول العالم.[450] وفي 3 تشرين الثاني/نوفمبر 2021، فرضت وزارة التجارة الأميركية عقوباتٍ على الشركة لبيعها منتجاتها لحكوماتٍ استخدمتها لـ"استهداف خصومها والمجتمع المدني بشكلٍ خبيث" و"ممارسة القمع العابر للحدود".[451]

وتحيط السرّية الشديدة بأنشطة "سايتو تيك"، ما يجعل تقدير إيراداتها أمراً صعباً. ومع ذلك، تُظهر وثائق دعوى قضائية رفعها موظفٌ كبيرٌ سابق في العام 2020 أنّ الشركة حقّقت إيراداتٍ تُقدّر بنحو 20 مليون دولار في العام 2018، وكانت لديها عقودٌ قيد التفاوض لسنواتٍ متعدّدة بقيمة 367 مليون دولار من أكثر من 60 دولة. كما أشار الموظف إلى أنّ عدد

---

[446] "سايتو تيك" (2020). مقترح برنامج التجسس المسرب لشركة "سايتو تيك. [متاح على الإنترنت] "هآرتس". متوفر على: https://img.haarets.co.il/bs/0000017f-e0a2-d804-ad7f-f1fa63b90000/ba/ac/7c85b9d556b876b2e4a8b6fdafa8/202.00902-161742.pdf

[447] "تشيك آي دي" (2025) (CheckIDد). *"سايتو تيك م." – 515126605. (Saito Tech Ltd - 515126605*). [متاح على الإنترنت] checkID. متوفر على: https://en.checkid.co.il/company/SAITO+TECH++LTD-rMe81mK-515126605 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[448] مغيدو، ج. (2021). نحن على القائمة السوداء الأميركية بسببكم": الصدام القذر بين شركات السلاح السيبراني الإسرائيلية. *"هآرتس"*. ('We're on the U.S. Blacklist Because of You': the Dirty Clash between Israeli Cyberarms Makers. *Haaretz*.) [متاح على الإنترنت] 17 كانون الأول/ديسمبر. متوفر على: https://www.haaretz.com/israel-news/2021-12-17/ty-article-magazine/.highlight/were-on-the-u-s-blacklist-because-of-you-the-clash-of-israeli-cyberarms-firms/0000017f-f195-dc28-a17f-fdb72e9a0000 [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[449] زيف، أ. (2020). *اختراق الهواتف وصفقات بملايين الدولارات في الخليج: الكشف عن الأعمال الداخلية لشركة هجمات سيبرانية إسرائيلية سرّية للغاية.* (*Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*) [متاح على الإنترنت] Haaretz.com. متوفر على: https://www.haaretz.com/israel-news/tech-news/2020-09-07/ty-article/.premium/mobile-spytech-millions-in-gulf-deals-top-secret-israeli-cyberattack-firm-reve/0000017f-e1eb-d568-ad7f-f3eb36390000 [تم الاطلاع عليه في 10 آب/أغسطس 2025].

[450] ماركزاك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزاق، ب.، وديبيرت، ر. (2021). *اصطياد "كانديرو": شركة تجسس مأجورة جديدة تحت المجهر*. (*Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*) [متاح على الإنترنت] *سيتيزن لاب*. جامعة تورونتو. متوفر على: https://utoronto.scholaris.ca/server/api/core/bitstreams/3e255059-7679-48b7-b84a-f5de13929dfc/content [تم الاطلاع عليه في 2 آب/أغسطس 2025].

[451] وزارة التجارة الأميركية (2021). *الوزارة تضيف مجموعة "إن إس أو" وشركات أجنبية أخرى إلى قائمة الكيانات بسبب أنشطة سيبرانية ضارة.* (*Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*)

موظفي الشركة بلغ نحو 150 موظفاً في العام 2020، مقارنةً بـ70 موظفاً في العام 2018 و12 موظفاً فقط في العام 2015.[452] أمّا منصة "بيتش بوك" فتُقدّر عدد موظفي الشركة بـ70 موظفاً.[453]

الصورة 28: صحيفة "هآرتس" تنشر ما يُزعم أنّه شعار شركة "كانديرو" (تصوير: أوفير فاكنين).[454]

ووفقاً لمجلة "فوربس"، كانت مجموعة "فاوندرز غروب" (Founders Group)، التي شارك في تأسيسها عمري لافي، الداعم المالي الرئيسي لشركة "سايتو تيك".[455] وأصبح إسحاق زاك (זק יצחק)،[456] المستثمر الرئيسي والشريك في "فاوندرز غروب"، أكبر مساهمٍ في شركة "سايتو تيك" خلال ستين يوماً فقط من تأسيسها.[457] وكان زاك من أوائل

---

[452] زيف، أ. (2020). *اختراق الهواتف وصفقات بملايين الدولارات في الخليج: الكشف عن الأعمال الداخلية لشركة هجمات سيبرانية إسرائيلية سرّية للغاية.* (*Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*)

[453] "بيتش بوك" (2025). (Pitchbook). "*سايتو تيك*". (*Saito Tech*) *[متاح على الإنترنت] متوفر على:* https://pitchbook.com/profiles/company/437928-67#overview [تم الاطلاع عليه في 30 آب/أغسطس 2025].

[454] زيف، أ. (2020). *اختراق الهواتف وصفقات بملايين الدولارات في الخليج: الكشف عن الأعمال الداخلية لشركة هجمات سيبرانية إسرائيلية سرّية للغاية.* (*Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*)

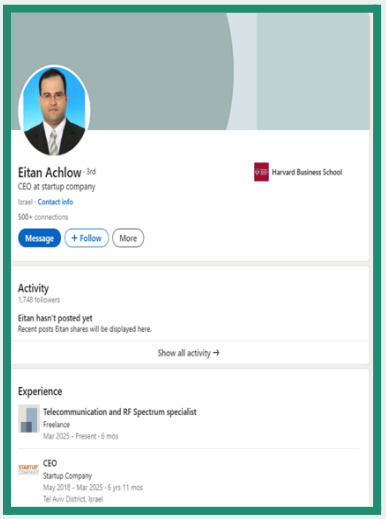
[455] بروستر، ت. (2019). تعرف على "كانديرو" — المرتزقة الغامضون الذين يخترقون أجهزة "آبل" و"مايكروسوفت" لتحقيق الأرباح. مجلة "*فوربس*". (Meet Candiru — the Mysterious Mercenaries Hacking Apple and Microsoft PCs for Profit. *Forbes*) [متاح على الإنترنت] 3 تشرين الأول/أكتوبر. متوفر على: https://www.forbes.com/sites/thomasbrewster/2019/10/03/meet-candiru-the-super-stealth-cyber-mercenaries-hacking-apple-and-microsoft-pcs-for-profit/ [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[456] في التقرير الأول لمختبر "سيتيزن لاب" حول شركة "كانديرو"، ذكر المؤلفون أنّ الاسم العبري لإسحاق زاك كان יעקב، ويبدو أنّ هذه ترجمة خاطئة لـ"إسحاق".ووفقاً للوثائق الرسمية التي حصلت عليها "سمكس"، فإنّ الاسم العبري الصحيح لإسحاق زاك هو יצחק (Yitzkhak) ، وهو الترجمة العبرية الشائعة لاسم إسحاق.

[457] ماركزاك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزاق، ب.، وديبيرت، ر. (2021). *اصطياد "كانديرو": شركة تجسس مأجورة جديدة تحت المجهر.* (*Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*).

المستثمرين في مجموعة "إن إس أو"،[458] ثمّ حصل لاحقاً على مقعدٍ في مجلس إدارة "سايتو تيك". ووفقاً لمختبر "سيتيزن لاب"، عُيّن إيتان أشلو في كانون الثاني/يناير 2019 مديراً تنفيذياً للشركة، وتومر إسرائيلي مديراً مالياً لها.[459]

غيّرت "سايتو تيك" اسمها أربع مرّات منذ تأسيسها عام 2014،[460] وتقوم بتغيير مكاتبها بشكلٍ متكرّر.[461] [462] وهي لا تدير موقعاً إلكترونياً، وتُلزم موظفيها بتوقيع اتفاقيات صارمة بعدم الإفصاح، كما تمنعهم من ذكر جهة عملهم على "لينكد إن"،[463] وحتى المدير التنفيذي إيتان أشلو لا يذكره.[464]



الصورة 29: صفحة إيتان أشلو على "لينكد إن"، التي تُظهر أنّه شغل منصب الرئيس التنفيذي لشركة ناشئة بين عامَيْ 2018 و2025.

إيتان أشلو – زملاء من الدرجة الثالثة رئيس تنفيذي في شركة ناشئة	Eitan Achlow.3rd

[458] ماركزاك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزاق، ب.، وديبيرت، ر. (2021). *اصطياد "كانديرو": شركة تجسس مأجورة جديدة تحت المجهر* (*Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*).

[459] ماركزاك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزاق، ب.، وديبيرت، ر. (2021). *اصطياد "كانديرو": شركة تجسس مأجورة جديدة تحت المجهر* (*Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*).

[460] ماركزاك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزاق، ب.، وديبيرت، ر. (2021). *اصطياد "كانديرو": شركة تجسس مأجورة جديدة تحت المجهر* (*Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*).

[461] زيف، أ. (2020). *اختراق الهواتف وصفقات بملايين الدولارات في الخليج: الكشف عن الأعمال الداخلية لشركة هجمات سيبرانية إسرائيلية سرّية للغاية* (*Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*)

[462] تأسّست شركة "كانديرو" عام 2014، وغيّرت اسمها في العام 2017 إلى "دي إف أسوشييتس المحدودة" (DF Associates Ltd.) (ד. אפ אסוסיאייטס בע"מ). وفي العام 2018، غيّرت الشركة اسمها مجدداً إلى "غريندافيك سولوشنز المحدودة" (Grindavik Solutions Ltd.) (גרינדוויק פתרונות בע"מ)، قبل أن يصبح اسمها "تافيتا المحدودة" (Taveta Ltd.) (טאבטה בע"מ) في العام 2019. وأخيراً، في العام 2020، غيّرت "تافيتا" اسمها إلى "سايتو تيك المحدودة" (Saito Tech Ltd.) (סאייטו טק בע"מ). ووفقاً لقائمة الكيانات التابعة لمكتب الصناعة والأمن الأميركي، ارتبط اسم "سايتو تيك" أيضاً باسمَيْ "غرينويك سولوشنز" (Greenwick Solutions) و"تاباثا المحدودة" (Tabatha Ltd.)، رغم أنّ الشركة لم تغيّر اسمها الرسمي بالإنكليزية إلى أيٍّ منهما. ويبدو أنّ هذين الاسمين هما مجرّد نقلين صوتيّين بديلين باللغة الإنجليزية لأسماء "غريندافيك سولوشنز" و"تافيتا" بالعبريّة.

[463] زيف، أ. (2020). *اختراق الهواتف وصفقات بملايين الدولارات في الخليج: الكشف عن الأعمال الداخلية لشركة هجمات سيبرانية إسرائيلية سرّية للغاية* (*Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*)

[464] أشلو، إ. (2025). *الصفحة الشخصية لإيتان أشلو* (*Eitan Achlow's profile page*). *[لينكد إن]. [تم الاطلاع عليه في 14 آب/أغسطس 2025]. متوفر على:* https://www.linkedin.com/in/eitan-achlow-788949/?originalSubdomain=il .

إسرائيل معلومات التواصل أكثر من 500 صلة إرسال رسالة +متابعة المزيد كلية هارفارد للأعمال النشاط 1,748 متابعاً لم ينشر إيتان أيّ منشورات بعد.	CEO at startup company Israel Contact info connections +500 Message Follow + More Harvard Business School Activity followers 1.748 Eitan hasn't posted yet
عرض كلّ الأنشطة الخبرة اختصاصي في الاتصالات وطيف الترددات الراديوية عمل حرّ آذار/مارس 2025 – حتى الآن (6 أشهر) الرئيس التنفيذي شركة ناشئة أيار/مايو 2018 – آذار/مارس 2025 (6 سنوات و11 شهراً) منطقة تل أبيب، إسرائيل	→ Show all activity Experience Telecommunication and RF Spectrum specialist Freelance Mar 2025-Present 6 mos STARTUP CEO Startup Company May 2018-Mar 2025-6 yrs 11 mos Tel Aviv District. Israel

وفقاً للملفّات الرسمية للشركة، فإنّ كبار المساهمين في "سايتو تيك" بالترتيب التنازلي هم: إسحاق زاك، يعقوب فايتزمان، إيرن شورير، وشركة "يونيفرسال موتورز إسرائيل م." (Universal Motors Israel Ltd.) (رقم الشركة:

511809071 [465])، شركة "آي.بي.آي تراست مانجمنت" (I.B.I. Trust Management) (رقم الشركة: 515020428[466])، وشركة "إيفن حمدات تراستس 1992 م." (Even Hemdat Trusts 1992 Ltd.) (رقم الشركة: 511678195[467]).[468] ويُعدّ زاك أكبر مساهم في الشركة، كما يُدرج كلٌّ من زاك وشورير وفايتزمان كأعضاء في مجلس إدارتها.

تُعدّ شركة "آي. بي. آي. تراست مانجمنت" شركة استثمارية متخصّصة في إدارة المحافظ المالية، وتعمل شركة "إيفن حمدات تراستس 1992" في المجال نفسه. وكما أشار مختبر "سيتيزن لاب" في تقريره الأوّل عن "سايتو تيك" عام 2021، يبقى من غير الواضح ما إذا كانت هذه الشركات الاستئمانية التي تمتلك الحصص الأكبر تفعل ذلك نيابةً عن موظّفين آخرين.[469] وكان أحد ممثلي شركة "يونيفرسال موتورز إسرائيل" قد شغل مقعداً في مجلس إدارة |"سايتو تيك"، لكنّ دوافع استثمار "يونيفرسال موتورز إسرائيل" في شركة مراقبة سيبرانية غير واضحة. وفي تموز/يوليو 2024، أفادت تقارير بأنّ "يونيفرسال موتورز إسرائيل" باعت حصّتها في "سايتو تيك"، غير أنّها ما زالت تظهر كمساهمٍ في السجلات الرسمية.[470] أما مديرا "إيفن حمدات تراستس" المدرجان في السجلّات فهما غيورا إرديناست[471] وجدعون دوني توليدانو،[472] وكلاهما محاميان.[473] وتشير المعلومات إلى أنّ مكتب المحاماة الذي يديرانه قد مثّل "مجموعة إن إس أو" في السابق أمام القضاء.[474] كما تُدرج أسماء تال دوري، وديفيد تسفي بيرنشتاين، وإيدو كوك كمديرين لشركة "آي. بي. آي. تراست مانجمنت"،[475]

---

[465] "تشيك آي دي" (CheckID) (2025). *"يونيفرسال موتورز إسرائيل م." – 511809071. (Universal Motors Israel Ltd - 511809071.)* [متاح على الإنترنت] CheckID. متوفر على:
https://en.checkid.co.il/company/UNIVERSAL+MOTORS+ISRAEL+LTD-DPvDQK6-511809071 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[466] "تشيك آي دي" (CheckID) (2025). *"آي.بي.آي تراست مانجمنت" – 515020428. (I.B.I. Trust Management - 515020428.)* [متاح على الإنترنت] CheckID. متوفر على:
https://en.checkid.co.il/company/I.B.I.+TRUST+MANAGEMENT-BmQv59r-515020428 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[467] "تشيك آي دي" (CheckID) (2025). *"إيفن حمدات تراستس" – 511678195. (Even Hemdat Trusts 1992 Ltd - 511678195071.)* [متاح على الإنترنت] CheckID. متوفر على:
tps://en.checkid.co.il/company/EVEN+HEMDAT+TRUSTS+1992+LTD-0O0PLGj-511678195 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[468] الهيئة الإسرائيلية للشركات (2025). *معلومات تفصيلية عن الشركة: سجل شركة "سايتو تيك م."* (Company Details Information: Entry for Saito Tech Ltd.)

[469] ماركزاك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزاق، ب.، وديبيرت، ر. (2021). *اصطياد "كانديرو": شركة تجسس مأجورة جديدة تحت المجهر.* (Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus.)

[470] "إنتلجنس أونلاين" (Intelligence Online) (2024). شركة الهجمات السيبرانية الصغيرة "Bindecy" تصمد أمام الأزمة السيبرانية الإسرائيلية. *إنتلجنس أونلاين.* [متاح على الإنترنت] 7 كانون الأول/ديسمبر. متوفر على:
https://www.intelligenceonline.com/surveillance--interception/2024/07/12/small-cyber-offensive-firm-bindecy-resists-israeli-cyber-crisis,110266932-art [تم الاطلاع عليه في 2 آب/أغسطس 2025].

[471] إرديناست، غ. (2025). *الصفحة الشخصية لغيورا إرديناست.* (Giora Erdinast's profile page) *[لينكد إن]. [تم الاطلاع عليه في 14 آب/أغسطس 2025]. متوفر على:* https://www.linkedin.com/in/giora-erdinast-099524167/.

[472] توليدانو، ج. (2025). *الصفحة الشخصية لجدعون دوني توليدانو.* (Gideon Donny Toledano's profile page) *[لينكد إن]. [تم الاطلاع عليه في 14 آب/أغسطس 2025]. متوفر على:* https://www.linkedin.com/in/doni-toledano-04b68326/details/experience/.

[473] "تشيك آي دي" (CheckID) (2025). *"إيفن حمدات تراستس" – 511678195. (Even Hemdat Trusts 1992 Ltd - 511678195071.)*

[474] Legal500 (بدون تاريخ). *حل النزاعات: التقاضي والتحكيم المحلي.* (Dispute Resolution: Local Litigation and Arbitration.) [متاح على الإنترنت] Legal500. متوفر على:
https://my.legal500.fr/c/israel/dispute-resolution-local-litigation-and-arbitration/#ranking-position-1.

[475] "تشيك آي دي" (CheckID) (2025). *"آي.بي.آي تراست مانجمنت" – 515020428. (I.B.I. Trust Management - 515020428.)*

ويبدو أنّهم يشغلون مناصب قيادية[476] أو كشركاء في الشركة.[477] وكانت شركة "أوبتاس إندستري م." (Optas Industry Ltd.)، التي تتّخذ من مالطا مقراً لها،[478] من بين كبار المساهمين السابقين في "سايتو تيك"، وقد شغل أحد مديريها منصب مسؤول الاستثمار في صندوق الاستثمار الخليجي.[479] وتملك "سايتو تيك" شركةً تابعة واحدة معروفة وهي "سوكوتو م." (Sokoto Ltd.) (رقم التسجيل: 515996981[480]).

لا تعكس الوثائق الرسمية للشركة التي حصلت عليها "سمكس" في آب/أغسطس 2025 ما ورد في تقارير إخبارية جديدة تزعم أنّ شركة الاستثمار التكنولوجي "إنتغريتي بارتنرز" (Integrity Partners) قد استحوذت على "سايتو تيك". ففي 2 نيسان/أبريل 2025، أفادت صحيفة "كلكاليست" بأنّ "إنتغريتي بارتنرز" اشترت "سايتو تيك" مقابل 30 مليون دولار، وتعمل على نقل جميع أصولها وموظفيها إلى كيانٍ جديدٍ غير خاضع للعقوبات الأميركية.[481] وتتكوّن "إنتغريتي بارتنرز" من أربعة شركاء هم: كريس غيرتنر،[482] وإلاد يوران،[483] وبات ويلكيسون،[484] وتوماس مورغان جونيور،[485] وجميعهم يبدو أنّ لهم خلفيات في الجيش الأميركي، رغم أنّ مورغان جونيور ويوران لا يدرجان اسم "إنتغريتي بارتنرز" ضمن سيرهم الذاتية على "لينكد إن" (على الرغم من نشاطهما الواضح على المنصّة). ووفقاً لتحليل أجرته "إنسيكت غروب" في آب/أغسطس 2025، تُظهر سجلات WHOIS المرتبطة بـ"سايتو تيك" أنّ أصول الشركة يجري نقلها إلى شركة إسرائيلية خاصة تُدعى "إنتغريتي لابس م." (Integrity Labs Ltd.) (رقم التسجيل: 517081089،[486] אינטגריטי לאבס

---

[476] " آي.بي.آي تراست مانجمنت". (2023). *فريق عملنا – "آي. بي. آي".* (*Our Team - IBI*) [متاح على الإنترنت] متوفر على: https://www.ibi.co.il/en/about/management/ [تم الاطلاع عليه في 30 آب/أغسطس 2025].

[477] بيرنستاين، ت. (2025). *الصفحة الشخصية لتسفيكا بيرنشتاين.* (*Tzvika Bernstein's profile page*). *[لينكد إن]. [تم الاطلاع عليه في 14 آب/أغسطس 2025]. متوفر على:* https://www.linkedin.com/in/tzvika-bernstein-29abba48/

[478] ماركزاك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزاق، ب.، وديبيرت، ر. (2021). *اصطياد "كانديرو": شركة تجسس مأجورة جديدة تحت المجهر.* (*Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*).

[479] "إنتلجنس أونلاين" (Intelligence Online) (2020). شركة "كانديرو" تتلقى دعماً من مستثمرين مرتبطين بقطر. *إنتلجنس أونلاين.* (Candiru Receives Boost from Investors Linked to Qatar. *Intelligence Online*.) [متاح على الإنترنت] 26 آب/أغسطس. متوفر على: https://www.intelligenceonline.com/corporate-intelligence/2020/08/26/candiru-receives-boost-from-investors-linked-to-qatar,109602043-art [تم الاطلاع عليه في 29 آب/أغسطس 2025].

[480] "تشيك آي دي" (CheckID) (2025). *"سكوتو م." – 515996981. (Sokoto Ltd – 515996981). [*متاح على الإنترنت] متوفر على: https://en.checkid.co.il/company/SOKOTO++LTD-W9bZ3yb-515996981 [تم الاطلاع عليه في 28 آب/أغسطس 2025].

[481] كبير، أ. (2025). *شركة التجسس المدرجة على القائمة السوداء "كانديرو" تُستحوذ عليها شركة "إنتغريتي بارتنرز" في صفقة بقيمة 30 مليون دولار.* (Blacklisted Spyware Firm Candiru Acquired by Integrity Partners in $30 Million Deal) [متاح على الإنترنت] "سي تك" (CTech). متوفر على: https://www.calcalistech.com/ctechnews/article/r1er11mi61e [تم الاطلاع عليه في 30 آب/أغسطس 2025].

[482] غيرتنير، ك. (2025). *الصفحة الشخصية لكريس غيرتنير.* (*Chris Gaertner's profile page*.) [لينكد إن] *[تم الاطلاع عليه في 14 آب/أغسطس 2025]. متوفر على:* https://www.linkedin.com/in/chrisgaertner/details/experience/.

[483] يوراد، إ. (2025). *الصفحة الشخصية لألاد يوران.* (*Elad Yoran's profile page*.) [لينكد إن] *[تم الاطلاع عليه في 14 آب/أغسطس 2025].* متوفر على: https://www.linkedin.com/in/eladyoran/.

[484] ويليكسيون، ب. (2025). *الصفحة الشخصية لبات ويليكسيون.* (*Pat Wilkison's profile page*.) [لينكد إن] *[تم الاطلاع عليه في 14 آب/أغسطس 2025]. متوفر على:* https://www.linkedin.com/in/wilkison/.

[485] مورغان جونيور، ت. (2025). *الصفحة الشخصية لتوماس مورغان جونيور.* (*Thomas Morgan Jr.'s profile page*.) [لينكد إن] *[تم الاطلاع عليه في 14 آب/أغسطس 2025]. متوفر على:* https://www.linkedin.com/in/thomas-morgan-jr-b8674519/.

[486] " تشيك آي دي" (CheckID) (2025). *"إنتغريتي لابز م." – 517081089. (Integrity Labs Ltd – 517081089). [متاح على الإنترنت]*. CheckID. متوفر على: https://en.checkid.co.il/company/INTEGRITY+LABS++LTD-Q21OrBv-517081089 *[تم الاطلاع عليه في 28 آب/أغسطس 2025].*

בע~מ) مقرّها في هرتسليا، إسرائيل.[487] كما تشير "إنسيكت غروب" إلى أنّ "إنتغريتي لابس" يديرها شخص يُدعى نفتالي يوران، ويُعرف أيضاً بأسماء مستعارة من بينها إلاد يوران.[488]

وبحسب موقعها الإلكتروني (integrity[.]partners)، يبدو أنّ "إنتغريتي بارتنرز" شريكة أو جزء من شركة "دي إتش سي أكويزيشنز" (DHC Acquisitions)، وهي شركة استحواذ ذات أغراض خاصة (SPAC) اندمجت مع شركة "براند إنغايدجمنت نتوورك" (Brand Engagement Network Inc.) في آذار/مارس 2024.[489] وكانت "دي إتش سي أكويزيشنز" قد جمعت 300 مليون دولار في آذار/مارس 2021 لتمويل أنشطتها.[490] ولم يعُد موقعها نشطاً اليوم، غير أنّ نسخة مؤرشفة منه تعود إلى 6 تشرين الأول/أكتوبر 2024 تُظهر أنّ غيرتنر ومورغان جونيور ووليكيسون شغلوا مناصب الرئيس التنفيذي المشارك، والرئيس التنفيذي المشارك/المدير المالي، والرئيس التنفيذي للعمليات، على التوالي.[491] أما الكيان الناتج عن الاندماج، فيُعرف اليوم باسم "براند إنغايدجمنت نتوورك".[492] وكانت "إنتغريتي بارتنرز" قد دخلت سابقاً في مفاوضاتٍ لشراء مجموعة "إن إس أو" مقابل 300 مليون دولار، لكن الصفقة لم تُستكمل.[493]

ولا تزال تفاصيل عدد الشركات التي تتعامل معها "سايتو تيك" لتوريد منتجاتها أو شحنها غير واضحة. غير أنّ منظمة العفو الدولية أفادت في العام 2024 بأنّ "سايتو تيك" اعتمدت على شركة "هيها الخاصة المحدودة" (Heha PTE Ltd.) في سنغافورة لشحن منتجات برامج التجسّس إلى الشرطة الوطنية الإندونيسية بين أيار/مايو 2020 وكانون الثاني/يناير 2021.[494]

---

[487] "إنسيكت غروب" (2025). *تتبع برنامج التجسس "لسان الشيطان" (Devil's Tongue) التابع لشركة "كانديرو" في عدة دول. (Tracking Candiru's DevilsTongue Spyware in Multiple Countries). [متاح على الإنترنت] "ريكورديد فيوتشر". متوفر على:* https://assets.recordedfuture.com/content/dam/insikt-report-pdfs/2025/cta-2025-0805.pdf [*[تم الاطلاع عليه في 12 آب/أغسطس 2025].*

[488] "إنسيكت غروب" (2025). *تتبع برنامج التجسس "لسان الشيطان" (Devil's Tongue) التابع لشركة "كانديرو" في عدة دول. (Tracking Candiru's DevilsTongue Spyware in Multiple Countries).*

[489] ناسداك (2024). *مساهمو شركة "دي إتش سي أكويزيشنز" يوافقون على الدمج التجاري المعلن سابقاً مع شركة "بين". (DHC Acquisition Corp. Shareholders Approve Previously Announced Business Combination with BEN). [متاح على الإنترنت] متوفر على:* https://www.nasdaq.com/press-release/dhc-acquisition-corp.-shareholders-approve-previously-announced-business-combination [*تم الاطلاع عليه في 30 آب/أغسطس 2025].*

[490] سريفاستافا، م. وفونتانيلّا- خان، ج. (2022) *مجموعة "إن. إس. أو." الإسرائيلية في محادثات بيع مع شركة يديرها جنود أميركيون سابقون. (Israel's NSO Group in Sale Talks with Company Run by ex-US Soldiers).* [متاح على الإنترنت] "فاينانشال تايمز". متوفر على: : https://www.ft.com/content/b4ad167b-cb3a-4e0b-a6a0-bb2608679721 *[تم الاطلاع عليه في 30 آب/أغسطس 2025].*

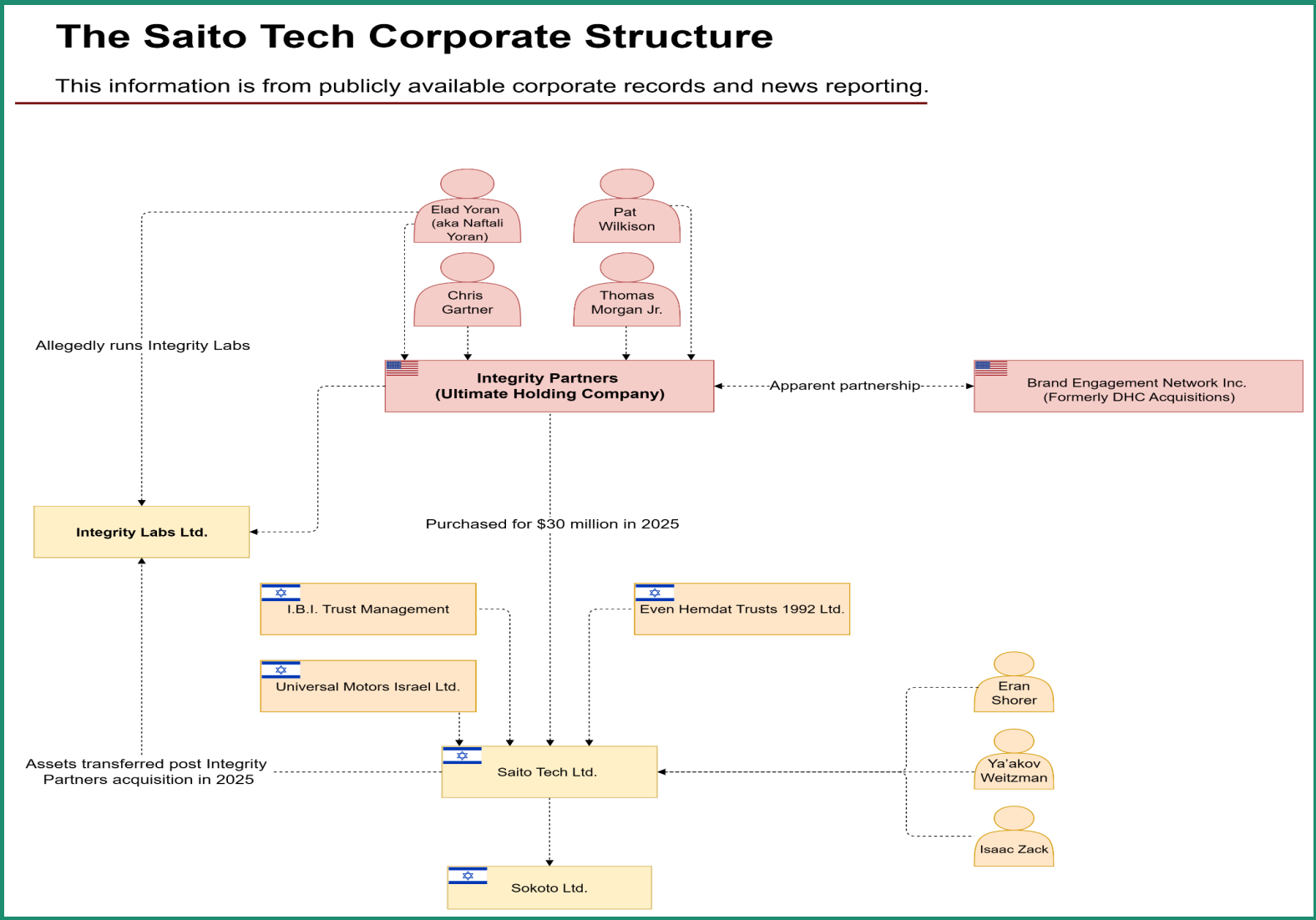
[491] شركة "دي إتش سي أكويزيشنز" (2019). *شركة "دي إتش سي أكويزيشنز" | الاستثمار في الشركات التي تحل تحديات "الميل الأخير" من خلال التكنولوجيا. (DHC Acquisition Corp | Investing in Companies Solving the Challenges of the Last Mile through Technology)* متاح على الإنترنت] متوفر على:
https://web.archive.org/web/20241006015701/https://www.dhcacquisition.partners/#team [*تم الاطلاع عليه في 30 آب/أغسطس 2025].*

[492] ناسداك (2024). *مساهمو شركة "دي إتش سي أكويزيشنز" يوافقون على الدمج التجاري المعلن سابقاً مع شركة "بين". (DHC Acquisition Corp. Shareholders Approve Previously Announced Business Combination with BEN).*

[493] سريفاستافا، م. وفونتانيلّا- خان، ج. (2022) *مجموعة "إن. إس. أو." الإسرائيلية في محادثات بيع مع شركة يديرها جنود أميركيون سابقون. (Israel's NSO Group in Sale Talks with Company Run by ex-US Soldiers).*

[494] منظمة العفو الدولية (2024). *شبكة من المراقبة – الكشف عن شبكة غامضة من صادرات برمجيات التجسس إلى إندونيسيا.* [متاح على الإنترنت] منظمة العفو الدولية، ص 18. متوفر على:
https://www.amnesty.org/ar/latest/news/2024/05/unravelling-a-murky-network-of-spyware-exports-to-indonesia/ [*تم الاطلاع عليه في 29 آب/أغسطس 2025].*

ويُرصد حضور "سايتو تيك" في منطقة غرب آسيا وشمال أفريقيا من خلال مقرّها الرئيسي في إسرائيل وكذلك عبر قاعدة عملائها الإقليميّين. وتشير البيانات المستقاة من التقارير العامّة إلى أنّ ما لا يقلّ عن ست دولٍ في المنطقة قد استخدمت برامج التجسّس التي تنتجها "سايتو تيك".



الصورة 30: الهيكل التنظيمي لشركة "سايتو تيك" في العام 2025

the Saito Tech Corporate Structure	الهيكل التنظيمي لشركة "سايتو تيك"
This information is from publicly available corporate records and news reporting	استُمدت هذه المعلومات من سجلات الشركة المتاحة وتقارير إخبارية منشورة
Elad Yoran (aka Naftali Yoran)	إلعاد يوران (المعروف أيضاً باسم نفتالي يوران)
Pat Wilkison	بات ويلكيسون
Chris Gartner	كريس غارتنر
Thomas Morgan Jr.	توماس مورغان جونيور
Allegedly runs Integrity Labs	يُزعم أنه يدير شركة "إنتغريتي لابز" (Integrity Labs)
Integrity Partners (Ultimate Holding Company)	شركة "إنتغريتي بارتنرز" (شركة قابضة نهائية)
Apparent partnership	شراكة معلنة
Brand Engagement Network Inc. (Formerly DHC Acquisitions	شركة "براند إنغيجمنت نتورك" (المعروفة سابقاً باسم دي إتش سي أكويزيشنز)
Integrity Labs Ltd.	شركة "إنتغريتي لابز" المحدودة
Purchased for $30 million in 2025	تم شراؤها مقابل 30 مليون دولار في عام 2025
I.B.I Trust Management	مجموعة "آي. بي. آي" (IBI) لإدارة صناديق الاستئمان
Even Hamdat Trusts 1992 Ltd.	شركة صناديق إيفن همدات الائتمانية المحدودة 1992
Universal Motors Israel Ltd.	شركة "يونيفرسال موتورز" الإسرائيلية المحدودة
Assets transferred post Integrity Partners acquisition in 2025	تم تحويل الأصول بعد استحواذ شركة "إنتغريتي بارتنرز" في العام 2025
Saito Tech Ltd.	شركة "سايتو تيك" المحدودة
Eran Shorer	إيران شورير
Ya’akov Weitzman	يعكوف وايتزمان
Isaac Zack	إسحق زاك
Sokoto Ltd.	شركة "سوكوتو" المحدودة

التسويق: "الخبراء في التكنولوجيا"

لا تتوفر معلومات كثيرة حول كيفية تسويق شركة "سايتو تيك" لمنتجاتها، ويُعزى ذلك جزئياً إلى شروط السرّية الصارمة التي تتبعها وحضورها المحدود على وسائل التواصل الاجتماعي والإنترنت. ومع ذلك، تكشف بعض المواد التسويقية المسربة عن بعض المعلومات حول الأساليب التي تعتمدها الشركة في التسويق لمنتجاتها.

نشرت صحيفة "هآرتس" في العام 2020 تقريراً عن شركة "سايتو تيك" (باستخدام اسمها السابق "كانديرو")، وتضمَّن التقرير مقترحاً تجارياً مسرّباً نشرته في الأصل صحيفة "ذا مركر".[495] وفي هذا المقترح، وصف نائب رئيس المبيعات، الذي لم يذكر اسمه، قدرات أحد المنتجات بأنها "غير قابلة للتتبع"، وقال: "يقوم هذا الوكيل البرمجي غير القابل للتتبع، وبمجرد نشره، برصد الشبكات التي يتصل بها الهدف ورسم خريطة اتصالها"، وأضاف أن برامج التجسس هذه "تبدأ بتنفيذ مهام لا يمكن اكتشافها لنقل البيانات بشكلٍ غير مصرح، من خلال التلاعب بمكونات الجهاز والبرامج المحلية والسيطرة عليها".[496] ويشير المقترح إلى أن منصة برامج التجسس هذه، والتي تصفها الشركة بأنها "منصة استخبارات سيبرانية متطورة مخصصة لاختراق أجهزة الكمبيوتر، والشبكات، وسماعات الهواتف المحمولة"، قادرة على استهداف أجهزة "ويندوز"، و"آيفون"، و"أندرويد".[497] ويوضح المقترح أن العملاء يمكنهم تشغيل هذا البرنامج في أي مكان في العالم، باستثناء الصين، وإيران، وإسرائيل، وروسيا، والولايات المتحدة.[498] [499] ويبدو أن المقترح يتفاخر أيضاً بقدرات البرنامج على "الهجوم بنقرة واحدة"، وصرّح: "يتم نشر وكلاء برامج [التسلل] الخاصة بالشركة سراً على الهدف (الأهداف)... بأقل قدر من الحاجة للتفاعل مع الجهة المستهدفة." ويختتم نائب الرئيس رسالته التقديمية بالإشارة إلى أن الشركة تسعى لخدمة عملائها "بأعلى مستويات النزاهة المهنية".[500]

على الرغم من أن شركة "سايتو تيك" تتسم بطبيعة انعزالية، يبدو أيضاً أنها شاركت أحياناً في معارض تجارية دولية متخصصة بتقنيات المراقبة. فقد قدمت الشركة ندوة في المعرض العالمي لأنظمة الدعم الاستخباراتي في أوروبا لعام 2021 بعنوان "الهجمات بدون أي نقرة: الكأس المقدسة"، وهو ما يدل على اهتمامها بهذا النوع من الهجمات.[501] [502]

في حين أشارت شركة "سايتو تيك" في المقترح المسرب إلى منتجها باسم "النظام"، لاحظت منظمة العفو الدولية أن "نظام التسلل السيبراني" هذا يُسوَّق تحت اسم "سايروس".[503] وتصف الشركة في المقترح "النظام" بأنه متطور للغاية وفريد من

---

[495] زيف، أ. (2020). *اختراق الهواتف المحمولة وملايين الصفقات الخليجية: الكشف عن الأعمال الداخلية لشركة إسرائيلية سريّة متخصصة في الهجمات السيبرانية* *Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*.

[496] "سايتو تيك" (2020). *مقترح برنامج التجسس المسرب لشركة "سايتو تيك"* *Leaked Saito Tech Spyware Proposal*.

[497] "سايتو تيك" (2020). *مقترح برنامج التجسس المسرب لشركة "سايتو تيك"*.

[498] مارزك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزّاق، ب. وديبرت، ر. (2021). *الكشف عن شركة "كانديرو": بائع آخر لبرامج التجسس المرتزقة يبرز في الواجهة* *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.

[499] أعلنت شركت "مايكروسوفت" أنها عثرت على ضحايا لشركة "كانديرو" في إيران في العام 2021، مما يشير إلى أن شركة "سايتو تيك" قد لا تفرض هذه القيود، أو أن تقنيتها أُستُخدمت بطريقة ما في بلد مدرج على قائمة البلاد محظور التعامل معها.

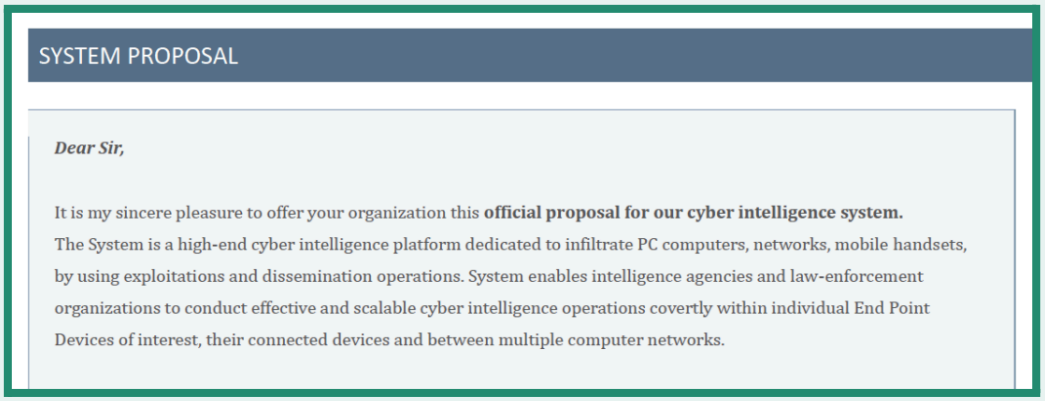
[500] "سايتو تيك" (2020). *مقترح برنامج التجسس المسرب لشركة "سايتو تيك"*.

[501] في حين عثرت منظمة "سمكس" على أدلة على منصة "أرشيف الإنترنت" تشير إلى أن شركة "كانديرو" قدّمت عرضاً، لم تُدرج المنشورات العامة لمعرض أنظمة الدعم الاستخباراتي في أوروبا لعام 2021 اسم الشركة ضمن قائمة مقدمي العروض.

[502] برنامج التدريب العالمي على أنظمة الدعم الاستخباراتي (2021). *معرض أنظمة الدعم الاستخباراتي في أوروبا – جدول الأعمال: 7-9 كانون الأول/ديسمبر*. [متاح على الإنترنت]. متوفر على: https://web.archive.org/web/20211202132420/https://www.issworldtraining.com/ISS_EUROPE/ [تم الوصول إليه في 30 آب/أغسطس 2025].

[503] منظمة العفو الدولية (2024). *شبكة من المراقبة: الكشف عن شبكة غامضة من صادرات برمجيات التجسس إلى إندونيسيا*. ص. 17.

نوعه مستخدمةً عبارات مثل "ثوري"، "ولا مثيل له"، و"شامل"، و"حصري"، و"متقدم"، و"قوي".[504] وأفادت صحيفة هآرتس بأن جزءاً أساسياً من استراتيجية مبيعات شركة "كانديرو" يقوم على اعتمادها على "الوكلاء"، أو الوسطاء، المقيمين في دول العملاء، والذين يساعدون في إتمام الصفقات. ويزعم أنهم يتقاضون عمولة تصل إلى نسبة 15% عن كل صفقة.[505]


SYSTEM PROPOSAL

Dear Sir,

It is my sincere pleasure to offer your organization this **official proposal for our cyber intelligence system.**
The System is a high-end cyber intelligence platform dedicated to infiltrate PC computers, networks, mobile handsets, by using exploitations and dissemination operations. System enables intelligence agencies and law-enforcement organizations to conduct effective and scalable cyber intelligence operations covertly within individual End Point Devices of interest, their connected devices and between multiple computer networks.

الصورة 31: مقترح شركة "كانديرو" المسرب يشير إلى برنامج التجسس باستخدام مصطلح "النظام"[506]

مقترح النظام حضرة السيد المحترم، يسرني أن أقدم إلى منظمتك هذا المقترح الرسمي المتعلق بنظامنا للاستخبارات السيبرانية. يمثل النظام منصة استخبارات سيبرانية متطوّرة ومخصّصة لاختراق أجهزة الحاسوب، والشبكات، وسماعات الهواتف المحمولة، من خلال استغلال الثغرات وتنفيذ عمليات النشر. ويمكّن النظام وكالات الاستخبارات ومنظمات إنفاذ القانون من إجراء عمليات استخباراتية سيبرانية فعّالة وقابلة للتوسع بشكل سري داخل أجهزة نقطة النهاية المستهدفة، وفي الأجهزة المتصلة بها، وبين شبكات الكمبيوتر المتعددة.	SYSTEM PROPOSAL ,Dear Sir It is my sincere pleasure to offer your organization this official proposal for our .cyber intelligence system The System is a high-end cyber intelligence platform dedicated to infiltrate PC computers, networks, mobile handsets, by using exploitations and dissemination operations. System enables intelligence agencies and law-enforcement organizations to conduct effective and scalable cyber intelligence operations covertly within individual End Point Devices of interest, their connected devices and .between multiple computer networks

[504] "سايتو تيك" (2020). *مقترح برنامج التجسس المسرب لشركة "سايتو تيك"* .

[505] زيف، أ. (2020). *اختراق الهواتف المحمولة وملايين الصفقات الخليجية: الكشف عن الأعمال الداخلية لشركة إسرائيلية سريّة متخصصة في الهجمات السيبرانية*.

[506] "سايتو تيك" (2020). *مقترح برنامج التجسس المسرب لشركة "سايتو تيك"*.

على عكس جميع موردي برامج التجسس التجاريين المذكورين في هذا التقرير، لا تسوّق شركة "سايتو تيك" نفسها كشركة تهتم بحقوق الإنسان أو تبيع منتجاتها للدول التي تستوفي معاييرها فقط. وكما ذُكر سابقاً، لا تستثني الشركة من البيع إلا الصين، وإيران، وإسرائيل، وروسيا، والولايات المتحدة فقط. وعندما تواصلت منظمة العفو الدولية معها في العام 2024 للتحقق من معاييرها المتعلقة ببذل العناية الواجبة في مجال حقوق الإنسان، والتأكد مما إذا كانت قد تعاملت مع شركة "هيها" الخاصة المحدودة (Heha PTE Ltd) لنقل برامج تجسس إلى إندونيسيا، أجابت شركة "سايتو تيك" بأنها "تعمل تحت إشراف وكالة مراقبة الصادرات التابعة لوزارة الدفاع الإسرائيلية بموجب قانون مراقبة الصادرات رقم 5766-2007." وجادلت بأنها "ممنوعة قانونياً" من الإفصاح عن أي معلومة تتعلق بأنشطتها أو التراخيص الممنوحة لها.[507] وبهذه الطريقة، تمكّنت شركة "سايتو تيك" ومن خلال التمسك بحق الإنكار المقبول قانونياً من مواصلة عملها بشكلٍ سري.

المنتجات والقدرات الرئيسية

تدّعي شركة "سايتو تيك" أنها تقدم مجموعةً من برامج التجسس المتطورة "غير القابلة للتتبع"، والتي تستهدف أجهزة الهواتف الذكية التي تشغّل بنظامي" آي أو إس" و"أندرويد"، بالإضافة إلى أجهزة الكمبيوتر التي تعمل بنظام "ويندوز".[508] وفي المقترح التجاري، تشير الشركة إلى هذه البرامج باسم "النظام"؛ في حين تسميها منظمة العفو الدولية "سايروس"، وتتتبّعها شركة "مايكروسوفت" تحت اسم برنامج "لسان الشيطان" (Devil's Tongue). ووصف باحثو التهديدات في مايكروسوفت برنامج التجسس الخاص بالشركة بأنه " عبارة عن برمجية خبيثة معقدة ومتعددة الخيوط، مكتوبة بلغة سي C وسي بلس بلس C++ وتتمتع بعدد كبير من الإمكانات الجديدة."[509]

يزعم مقترح الشركة أن برنامج التجسس قادر على استهداف "الإصدارات الأحدث" من نظامي "ويندوز" 10، 64 بت و"ويندوز" 7، 32 بت و64 بت.[510] ويدّعي أيضاً أن البرنامج يستطيع استهداف الإصدارات الحديثة من ثلاثة متصفحات إنترنت رئيسية، من خلال استغلال ثغرات تنفيذ التعليمات البرمجية عن بُعد (RCE)؛ وجمع بيانات مجموعة متنوعة من التطبيقات، وتشمل الموقع، والملفات، وكلمات المرور، وسجل التصفح؛ والتحكّم بكاميرا الضحية وميكروفونها.[511] وتتفاخر الشركة أيضاً بقدرتها على استخراج جميع أنواع البيانات الأساسية من هواتف "سامسونغ غالاكسي"، ومن أحدث إصدارات نظام "آي أو إس" على أجهزة "آيفون"، بما في ذلك الوصول إلى تطبيقات المراسلة والكاميرا والميكروفون[512]. ويبدو أن نسخة البرنامج المخصصة لنظام "ويندوز" قادرة على نقل مجموعة واسعة من الملفات بشكلٍ غير مصرح، بما في ذلك الرسائل من تطبيقات المراسلة المشفرة مثل تطبيق سيغنال (Signal).[513]

تقدم الشركة لعملائها عدة طرق لاختراق الأجهزة، وتشمل ارسال روابط خبيثة تتطلب نقرة واحدة، وتنفيذ هجمات الخصم في الوسط (AiTM).[514] ومن المتعارف عليه أن الشركة تعتمد إلى حد كبير على رسائل بريد إلكتروني تحتوي على روابط

---

[507] منظمة العفو الدولية (2024). *شبكة من المراقبة: الكشف عن شبكة غامضة من صادرات برمجيات التجسس إلى إندونيسيا*. ص. 22.

[508] س"ايتو تيك" (2020). *مقترح برنامج التجسس المسرب لشركة "سايتو تيك"*.

[509] قسم استخبارات التهديدات في شركة "مايكروسوفت" (2024). ممثل المخاطر الهجومي للقطاع الخاص كاراميل تسونامي (Caramel Tsunami). *الأمان الداخلي*. متوفر على:https://www.microsoft.com/en-us/security/security-insider/threat-landscape/caramel-tsunami#section-master-oc2985 [تم الوصول إليه في 29 آب/أغسطس 2025].

[510] "سايتو تيك" (2020). *مقترح برنامج التجسس المسرب لشركة "سايتو تيك"*.

[511] "سايتو تيك" (2020). *مقترح برنامج التجسس المسرب لشركة "سايتو تيك"*.

[512] "سايتو تيك" (2020). *مقترح برنامج التجسس المسرب لشركة "سايتو تيك"*.

[513] مارزك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزّاق، ب. وديبرت، ر. (2021). الكشف عن شركة "كانديرو": بائع آخر لبرامج التجسس المرتزقة يبرز في الواجهة.

[514] "سايتو تيك" (2020). *مقترح برنامج التجسس المسرب لشركة "سايتو تيك"*.

خبيثة تقوم بتنزيل حمولة ضارة على جهاز الضحية.[515] وتوفر الشركة ميزةً إضافية تسعّر بنحو 6 ملايين يورو، وهي طريقة اختراق تعرف باسم "شيرلوك" (Sherlock)، ويقدّر مختبر "سيتيزن لاب" بأنها قد تكون "طريقة لا تتطلب أي نقرة وتعتمد على المتصفح".[516] وأفادت مدونة أمن سيبراني تابعة لجامعة ستراسبورغ في العام 2024 أن تقنية شيرلوك تمثّل سلالة منفصلة من برامج التجسس طورتها شركة إسرائيلية تدعى "إنسا نت" (Insanet) (رقم التسجيل: 516013364[517]). ويمكن لتقنية شيرلوك استهداف الضحايا على أجهزة تعمل بأنظمة "أندرويد" و"آي أو إس" و"ويندوز"، من خلال الاعتماد على "الإعلانات البرمجية" كوسيلة لنشر الحمولات الخبيثة.[518] وذكرت شركة "إنسيكت غروب" (Insikt Group) في العام 2025 أن تقنية شيرلوك تُستخدم للمساعدة في تثبيت حمولات برامج التجسس بشكل سري.[519]

ويبدو أن شركة "سايتو تيك" تبيع إمكانية الوصول إلى مجموعة أدوات التجسس بناءً على عدد الأجهزة التي يمكن استهدافها بشكل متزامن. وعلى عكس مقترحات موردي برامج التجسس التجارية الأخرى الواردة في هذا التقرير، يشير مقترح شركة "سايتو تيك" إلى أن العميل يمكنه شراء عدد غير محدود من محاولات الاستهداف مقابل حوالى 16 مليون يورو، ويحدد حد أقصى لعمليات الاستهداف المتزامنة، وتشمل 10 أجهزة. وتوفر الشركة للعملاء إمكانية استهداف 15 جهازاً إضافياً مقابل 1.5 مليون يورو. ويمكن للعميل دفع مبلغ 5.5 مليون يورو إضافي ليتمكن من استهداف 25 جهازاً آخر في الوقت نفسه، واستخدام هذه الأدوات في خمس دول إضافية. أما القدرة على استهداف تطبيقات معينة مثل تطبيق "سيغنال" أو "فايبر"، فتتطلب دفع رسوم إضافية.

ويسلط مختبر "سيتيزن لاب" الضوء على عنصر مقلق للغاية في المقترح: وهو خيار شراء ميزة إضافية تسمح للعملاء بالوصول إلى صدفة سطر الأوامر عن بُعد مقابل 1.5 مليون يورو، وبالتالي بتنفيذ أوامر برمجية عن بُعد على جهاز الجهة المستهدفة.[520] وقد يمكّنهم ذلك من تحميل بيانات على جهاز الضحية. وتقدّم الشركة حزمة كاملة مقابل مبلغ إجمالي يصل إلى 16.85 مليون يورو، تتضمن وحدات برامج تجسس لأنظمة "ويندوز" و"آي أو إس" و"أندرويد"، وإمكانية تحليل البيانات، ومحاولات نشر غير محدودة، وسعة تصل إلى 10 إصابات متزامنة، وطرق استهداف متعددة، والقدرة على الاستهداف داخل دولة واحدة، والأجهزة اللازمة، وخدمات تسليم النظام، والتدريب ذي الصلة. ومن المعروف أيضاً أن بنية

---

[515] سكوت-ريلتون، ج.، كامبو، إي.، ماركزاك، ب.، عبد الرزاق، ب.، أنستيس، س.، بوكو، جي.، سوليمانو، س. وديبرت، ر. (2022). *فضيحة "كاتالان غايت": عملية تجسس مرتزقة واسعة النطاق ضد الكتالونيين باستخدام برنامجي التجسس "بيغاسوس" و"كانديرو" CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru*. [متاح على الإنترنت]. مختبر *"سيتيزن لاب"*. متوفر على:
https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ [تم الوصول إليه في 12 آب/أغسطس 2025].

[516] مارزك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزّاق، ب. وديبرت، ر. (2021). *الكشف عن شركة "كانديرو": بائع آخر لبرامج التجسس المرتزقة يبرز في الواجهة*.

[517] "تشيك آي دي" (CheckID) (2025). *شركة "إنسا نت" المحدودة (Insanet Ltd) - 516013364*. [متاح على الإنترنت] "تشيك آي دي". متوفر على: https://en.checkid.co.il/company/INSANET++LTD-w6e85Bd-516013364 [تم الوصول إليه في 28 آب/أغسطس 2025].

[518] فرايرموث، ج. (2024). تقنية "شيرلوك"، برنامج التجسس الإسرائيلي المُرعِب، يتجاوز "بيغاسوس" Sherlock, the Terrifying Israeli spyware, Surpassing Pegasus. *مدونة العدالة السيبرانية (Blog Cyberjustice)*. متوفر على الموقع التالي:
https://cyberjustice.blog/2024/01/22/sherlock-the-terrifying-israeli-spyware-surpassing-pegasus/ [تم الوصول إليه في 12 آب/أغسطس 2025].

[519] "إنسيكت غروب" (Insikt Group) (2025). تتبع برنامج التجسس برنامج "لسان الشيطان" (Devil's Tongue) التابع لشركة "كانديرو" في دول متعددة Tracking Candiru's DevilsTongue Spyware in Multiple Countries.

[520] مارزك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزّاق، ب. وديبرت، ر. (2021). *الكشف عن شركة "كانديرو": بائع آخر لبرامج التجسس المرتزقة يبرز في الواجهة*.

برامج التجسس الخاصة بالشركة تعتمد أحياناً على إرسال روابط خبيثة تتظاهر بأنها تابعة لمجموعات مناصرة أو وسائل إعلام أو منظمات المجتمع المدني.[521]

أصدرت شركة "إنسيكت غروب" في آب/أغسطس 2025 تقريراً مفصّلاً عن أنشطة جديدة مرتبطة بشركة "سايتو تيك" وبرنامجها للتجسس المخصص لأنظمة "ويندوز".[522] وتتبع التقرير مجموعات من الأنشطة التي نسبت إلى شركة "سايتو تيك" في المملكة العربية السعودية. ويبدو أن هذه الأنشطة استمرت حتى تاريخ 26 حزيران/يونيو 2025. وكشف التقرير أن تصاميم البنية التحتية التي تعتمدها الشركة تختلف بشكلٍ كبير بين مشغلي برامج التجسس، فيقوم بعض العملاء بإدارة بنية استهداف الضحايا مباشرةً عبر برنامج "لسان الشيطان" (Devil's Tongue)، بينما يعتمد آخرون على "الطبقات الوسيطة في البنية التحتية"، ويستخدم بعضهم شبكة تور (Tor).

الهجمات الكبرى

في 18 نيسان/أبريل 2022، أصدر مختبر "سيتيزن لاب" تقريره الرئيس الثاني حول شركة "سايتو تيك"، والذي تناول بالتفصيل "عملية تجسس مرتزقة واسعة النطاق" استهدفت شعب كتالونيا باستخدام برامجي التجسس "بيغاسوس" و"كانديرو".[523] وبعد أن أجرى المختبر تحليلاً أولياً لبرنامج تجسس "كانديرو"، تمكن فريق المختبر من تحديد ضحية قيد الاستهداف في كتالونيا، وهي خوان ماتامالا. ويُعتبر ماتامالا ناشطاً سياسياً من مدينة جيرونا، ويدير مكتبة ومؤسسة، وكلاهما يهدفان إلى تعزيز الثقافة واللغة الكتالونية وتعليمهما.[524] وأسس ماتامالا أيضاً مؤسسة "نورد" (Nord Foundation)، وهي منظمة غير ربحية تشجّع المواطنين على الانخراط في تقنيات مفتوحة المصدر بطريقة اجتماعية وأخلاقية. وكشف الباحثون عن أدلة على وجود اختراق فعلي في مجموعة من الجامعات الكتالونية، وتمكنوا، بمساعدة تقنيين محليين، من التأكد من أن الجهاز قيد الاختراق يعود لماتامالا نفسه.

عندما أدرك المختبر أن الجهاز قيد الاختراق، تواصل الباحثون مع زملاء ماتامالا في محاولة لإبعاده عن جهاز الكمبيوتر المخترق، تحسباً لاحتمال تعرضه للمراقبة في الوقت الفعلي. وسمح ماتامالا للباحثين بالوصول إلى جهازه، ليتبيّن بعد فحصه أنهم تمكنوا من الحصول على نسخة عاملة من برنامج التجسس التابع لشركة "سايتو تيك". وتعاون المختبر مع شركة "مايكروسوفت" بهدف سد الثغرات الأمنية التي استغلتها الشركة، وهو ما دفع "مايكروسوفت" إلى إصدار تحديث أمني وصل إلى 1.4 مليار جهاز حول العالم.[525]

تبيّن في النهاية أن قصة ماتامالا كانت جزءاً من عملية تجسس أوسع بكثير، استهدف من خلالها مشغلو برامج التجسس عدداً كبيراً من السياسيين وأفراد المجتمع المدني في كتالونيا، بما في ذلك أعضاء كتالونيين في البرلمان الأوروبي وسياسيون محليون. وتعرض ما لا يقل عن ثلاثة كتالونيين آخرين للاختراق ببرنامج "كانديرو" عبر رسائل بريد إلكتروني خبيثة. وأظهرت المراجعات اللاحقة أن ماتامالا نفسه استهدف أيضاً بواسطة برنامج "بيغاسوس" 16 مرة على الأقل بين

---

[521] مارزك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزّاق، ب. وديبرت، ر. (2021). *الكشف عن شركة "كانديرو": بائع آخر لبرامج التجسس المرتزقة يبرز في الواجهة*.

[522] "إنسيكت غروب" (2025). *تتبع برنامج التجسس برنامج "لسان الشيطان" (Devil's Tongue) التابع لشركة "كانديرو" في دول متعددة*.

[523] سكوت-رايلتون، ج.، كامبو، إي.، ماركزاك، ب.، عبد الرزاق، ب.، أنستيس، س.، بوكو، جي.، سوليمانو، س. وديبرت، ر. (2022). *فضيحة "كاتالان غايت": عملية تجسس مرتزقة واسعة النطاق ضد الكتالونيين باستخدام برنامجي التجسس "بيغاسوس" و"كانديرو"*.

[524] مارزك، ب.، سكوت-رايلتون، ج.، بيردان، ك.، عبد الرزّاق، ب. وديبرت، ر. (2021). *الكشف عن شركة "كانديرو": بائع آخر لبرامج التجسس المرتزقة يبرز في الواجهة*.

[525] مختبر "سيتيزن لاب" (2017). *هل كنت لتنقر – قصة من مختبر "سيتيزن لاب" Would You click? — A a Story by the Citizen Lab*.
[متاح على الإنترنت] مختبر "سيتيزن لاب": متوفر على: https://catalonia.citizenlab.ca/ [تم الوصول إليه في 11 آب/أغسطس 2025].

آب/أغسطس 2019 وتموز/يوليو 2020، وأن إجمالي عدد الأفراد الذين استُهدفوا ببرامج التجسس أثناء هذه العملية بلغ 65 شخصاً.[526]

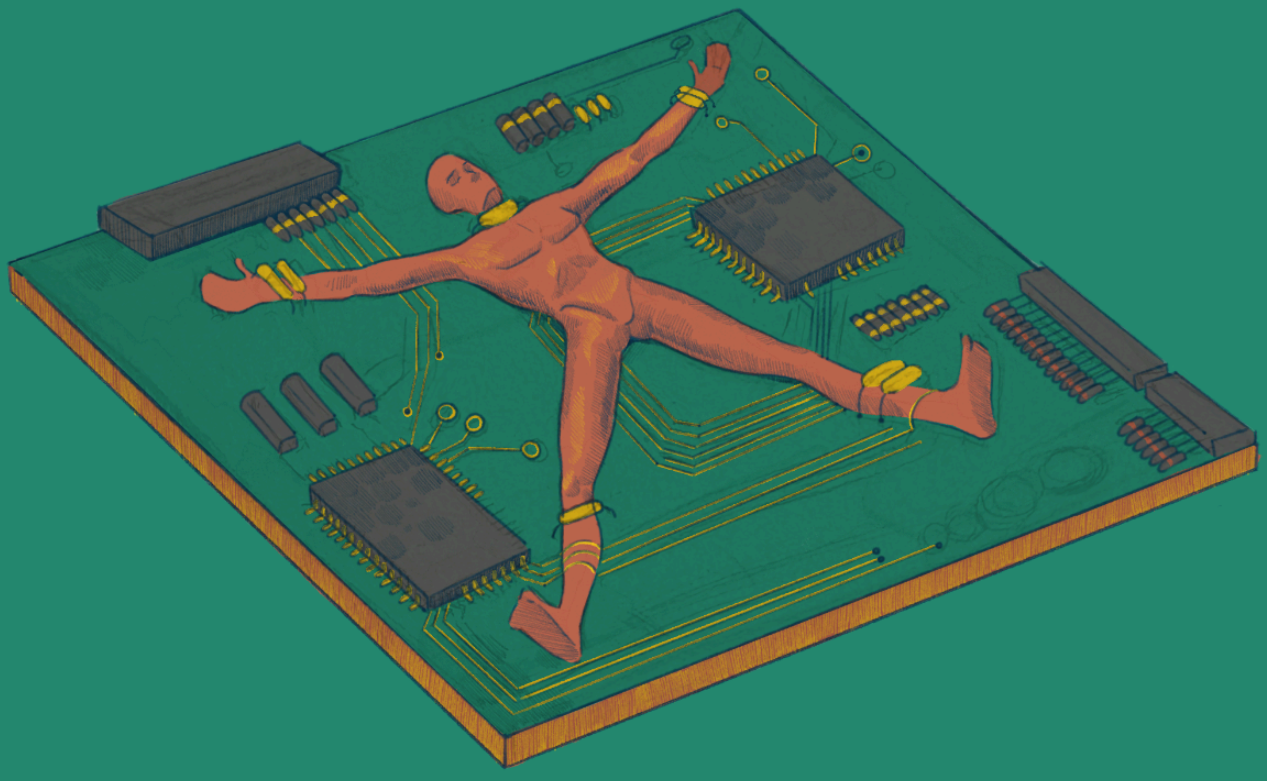
تُشير التقارير إلى أن إصدارات برنامج التجسس التابع لشركة "سايتو تيك"، والتي استهدفت أفراداً في كتالونيا، قد صممت لتوفير "إمكانية وصول واسعة النطاق" إلى أجهزة الضحايا، بما في ذلك القدرة على النقل غير المصرح لبيانات الملفات وسجلات التصفح، ومراقبة رسائل تطبيقات المراسلة المشفرة وتحميلها.[527]

وعلى الرغم من صعوبة إثبات ذلك بشكل قاطع، يشير المختبر إلى أن العملاء الذين استخدموا برامج مجموعة إن إس أو وشركة "سايتو تيك" قد يكونون مرتبطين بالحكومة الإسبانية، لا سيما في ظل السياق السياسي القائم بين إسبانيا وكتالونيا.

[526] سكوت-ريلتون، ج.، كامبو، إي.، ماركزاك، ب.، عبد الرزاق، ب.، أنستيس، س.، بوكو، جي.، سوليمانو، س. وديبرت، ر. (2022). *فضيحة "كاتالان غايت": عملية تجسس مرتزقة واسعة النطاق ضد الكتالونيين باستخدام برنامجي التجسس "بيغاسوس" و"كانديرو"*.

[527] سكوت-ريلتون، ج.، كامبو، إي.، ماركزاك، ب.، عبد الرزاق، ب.، أنستيس، س.، بوكو، جي.، سوليمانو، س. وديبرت، ر. (2022). *فضيحة "كاتالان غايت": عملية تجسس مرتزقة واسعة النطاق ضد الكتالونيين باستخدام برنامجي التجسس "بيغاسوس" و"كانديرو"*.

الجزء الرابع: التركيز على تأثير برامج التجسس على حقوق الإنسان: دراسة حالة لمنظمة "سمكس"



أمنياً، ويسعون للسيطرة على السردية الرقمية.[528] ويبدو أنهم أصبحوا أيضاً قادرين على مراقبة الاتصالات الخاصة في جميع أنحاء اليمن. وكشف مشروع مكافحة التطرف في تشرين الأول/أكتوبر 2023 أن الحوثيين قادرون على مراقبة الاتصالات عبر وحدة تعريف المشترك (SIM)، المستخدمة للاتصال بشبكات الهواتف اليمنية المحلية، بالإضافة إلى المعرّفات الفريدة للأجهزة، بفضل سيطرتهم على مشغلي شبكات الاتصالات.[529] وعلى الرغم من عدم وجود دليل قاطع على استخدامهم لمنتجات موردي برامج التجسس التجارية، تشير التقارير إلى أن الحوثيين والمجموعات المتحالفة معهم اعتمدوا على البرمجيات الخبيثة للتجسس على أهداف سياسية. وكشفت شركة "إنسيكت غروب" في تشرين الثاني/نوفمبر 2018 عن نشاط مشبوه بالإضافة إلى تولي "سمكس" دور مراقب لحقوق الإنسان الرقمية في منطقة غرب آسيا وشمال أفريقيا، تدير المنظمة أيضاً مختبر التدقيق الجنائي الرقمي (DFL) لمراقبة التهديدات الرقمية والتعامل معها. وفي العام 2024، تعامل المختبر مع حالة استهداف طالت صحافي يمني ونفذتها جهات قائمة بالتهديد. وتبرز هذه الحالة كيف يمكن لبرامج التجسس أن تؤثر على حقوق الإنسان في المنطقة، وتدمير حياة الأفراد.

في 4 حزيران/يونيو 2024، تواصل صحافي يمني معروف مع مختبر التدقيق الجنائي الرقمي بعد أن اعتقل مرتين، وتعرض لتجربة وصفها لمنظمة "سمكس" بأنها "اختراق". وسوف تحرص المنظمة على الحفاظ على سرية هويته خوفاً من تعرضه لأي انتقام. و**قامت سلطات الحوثيين في صنعاء باعتقال هذا الصحافي** في العام 2018، ثم تكرر ذلك في العام 2022 بسبب تغطيته لأحداث الحرب في اليمن وأنشطة الحوثيين. وأجبرته على توقيع وثيقة تمنعه من ممارسة مهنة الصحافة في اليمن إلى أجل غير مسمى. ولأنه اعتقد أن هاتفه قد تم اختراقه، أجرى **عملية** إعادة ضبط المصنع لجهازه المحمول قبل التواصل مع **المنظمة.** وفي نهاية المطاف، **تبيّن أن** اهتمام سلطات الحوثيين بأنشطته ارتبط ارتباطاً وثيقاً بالحرب الأهلية التي عصفت باليمن لأكثر من عقد من الزمن.

الحرب الأهلية في اليمن

اندلعت الحرب الأهلية الدامية في اليمن في تموز/يوليو 2014، ووصفتها الأمم المتحدة بأنه "واحدة من أسوأ الأزمات الإنسانية في العالم.[530] وكشفت الأمم المتحدة أن هذه الحرب أسفرت عن مقتل أكثر من 377,000 يمني، بما في ذلك 10,000 طفل، وتشريد أكثر من 4 ملايين شخص، وتدمير نسبة 54% من سبل عيش السكان، ودفع 15.6 مليون يمني إلى حالة من "الفقر المدقع." [531]

---

[528] جمال بلعياشي (2025). *كيف يشن الحوثيون في اليمن حملة قمع رقمية؟* [متاح على الإنترنت] المراقبون – قناة فرانس 23. متوفر على: https://observers.france24.com/en/middle-east/20250605-yemen-houthis-campaign-digital-repression-midri. [تم الوصول إليه في 22 آب/أغسطس 2025].

[529] مشروع مكافحة التطرف (2023). *استخدام الحوثيين للتكنولوجيا من أجل القمع.* [متاح على الإنترنت] الصفحتين 7-8. متوفر على: https://www.counterextremism.com/sites/default/files/2023-09/The%20Houthis%20Use%20of%20Technology%20for%20Repression_Oct%202023.pdf. [تم الوصول إليه في 25 آب/أغسطس 2025].

[530] الأمم المتحدة في اليمن (2021). *التقرير السنوي لفريق الأمم المتحدة القطري في اليمن: UN Yemen Country Results Report: 2021.* [متاح على الإنترنت] الأمم المتحدة في اليمن، ص. 6. متوفر على: https://yemen.un.org/sites/default/files/2022-04/Yemen_UNCT%20Annual%20Report%202021_.pdf [تم الوصول إليه في 27 آب/أغسطس 2025].

[531] الأمم المتحدة في اليمن (2021). *التقرير السنوي لفريق الأمم المتحدة القطري في اليمن: 2021.*

بعد أن قام الرئيس اليمني السابق عبد ربه منصور هادي بتخفيض الدعم على الوقود في تموز/يوليو 2014، اندلعت احتجاجات كبيرة في جميع أنحاء صنعاء.[532] وبعد ذلك سيطر الحوثيون، وهم جماعة مسلحة من الطائفة الشيعية الزيدية متحالفة مع إيران، على عدة مناطق في العاصمة.[533] وبعد فشل المفاوضات، اقتحم المتمردون الحوثيون القصر الرئاسي وسيطروا عليه في كانون الثاني/يناير 2015، ما دفع هادي وحكومته إلى الاستقالة.[534] بعد ذلك بوقت قصير، شنّ تحالف بقيادة السعودية في آذار/مارس 2015 حملة غارات جوية على الحوثيين، ترافقت مع حملة عزلة اقتصادية.[535] وعلى الرغم من هذه الحملات، تمكن الحوثيون من السيطرة على صنعاء في كانون الأول/ديسمبر 2017. وبحلول أواخر العقد الماضي، أصبح من الواضح أن إيران تقدم دعماً عسكرياً واستراتيجياً للحوثيين، ولا سيما نظراً لامتلاكهم أسلحة ثقيلة متطورة يُرجح أنها صنعت في إيران. [536] [537] واستمر الحوثيون في توسيع نطاق سيطرتهم، على الرغم من الهجوم الكبير الذي شنه التحالف على مدينة الحديدة في العام 2018. وتصاعدت حدة القتال في العام 2021 عندما شن الحوثيون هجوماً باتجاه مدينة مأرب، على الرغم من التوصل إلى وقف إطلاق نار بقيادة الأمم المتحدة في العام 2022.

وبعد أن شنت إسرائيل حملة الإبادة الجماعية على غزة، بدأ الحوثيون في شن هجمات ضد إسرائيل وضد شحنات تجارية مرتبطة بها. وقد دفع ذلك الولايات المتحدة إلى بدء حملة قصف جوي ضد الحوثيين، الأمر الذي دفع الحكومة والقوات الحكومية المتحالفة مع السعودية إلى التفكير، وفقاً للتقارير، في شن هجوم جديد على مواقع سيطرة الحوثيين. [538] [539] وبحلول نيسان/أبريل 2025، سيطر الحوثيون على نحو ثلث اليمن، وحكموا المناطق التي يعيش فيها حوالى نسبة 80% من السكان. [540]

منذ سيطرة الحوثيين على أجزاء واسعة من اليمن، أطلقوا حملة قمع رقمية. وفي أيار/مايو 2025، أشارت قناة فرانس 24 إلى هذا التوجه، وأفادت بأن الحوثيين يحظرون أنواعاً معينة من الخطاب الإلكتروني باعتباره تهديداً على الإنترنت من داخل اليمن، مما يشير إلى احتمال استخدامهم لبرامج الإعلانات وبرامج التجسس. [541] وفي أيار/مايو 2023، حقّقت الشركة

---

[532] زيدان، أ. (2025). *الحركة الحوثية | اليمن، التاريخ، القائد، والأهداف | موسوعة بريتانيكا, Houthi Movement | Yemen, History, Leader, & Goals | Britannica*. [متاح على الإنترنت] www.britannica.com. متوفر على:
https://www.britannica.com/topic/Houthi-movement [تم الوصول إليه في 27 تموز/يوليو 2025]

[533] زيدان، أ. (2025). *الحركة الحوثية | اليمن، التاريخ، القائد، والأهداف | موسوعة بريتانيكا*.

[534] مركز العمل الوقائي (CPA) (2025). *الصراع في اليمن وأزمة البحر الأحمر Conflict in Yemen and the Red Sea*. [متاح على الإنترنت] موقع تعقب الصراعات العالمية. متوفر على: https://www.cfr.org/global-conflict-tracker/conflict/war-yemen [تم الوصول إليه في 27 آب/أغسطس 2025].

[535] زيدان، أ. (2024). *الحرب الأهلية في اليمن | [من العام 2015 حتّى الآن] | موسوعة بريتانيكا | Yemeni Civil War | [2015-present] Britannica*. [متاح على الإنترنت] www.britannica.com. متوفر على: https://www.britannica.com/event/Yemeni-Civil-War [تم الوصول إليه في 20 آب/أغسطس 2025].

[536] زيدان، أ. (2025). *الحركة الحوثية | اليمن، التاريخ، القائد، والأهداف | موسوعة بريتانيكا*.

[537] أبو الأسرار، ف. (2022). *حرب الحوثيين ومستقبل اليمن*. [متاح على الإنترنت] معهد الشرق الأوسط، ص. 5. متوفر على:
https://www.mei.edu/sites/default/files/Alasrar%20-%20The%20Houthis'%20war%20and%20Yemen's%20future.pdf [تم الوصول إليه في 2 آب/أغسطس 2025].

[538] أوكونور، ت. وفينج، ج. (2025). *الحوثيون يحذرون السعودية والإمارات من "العواقب الوخيمة" في حال دعم عملية برية ضدهم*. [متاح على الإنترنت] مجلة نيوزويك. متوفر على:
https://www.newsweek.com/houthis-warn-saudi-arabia-uae-will-pay-price-if-they-back-new-offensive-2060728. [تم الوصول إليه في 27 آب/أغسطس 2025].

[539] إيدون، ب. (2025). ميليشيات يمنية قد تخطط لشن هجوم بري ضد الحوثيين. *فربس* [متاح على الإنترنت] 3 أيّار/مايو. متوفر على:
https://www.forbes.com/sites/pauliddon/2025/05/03/yemeni-militias-may-be-planning-a-ground-offensive-against-the-houthis/. [تم الوصول إليه في 27 آب/أغسطس 2025].

[540] أوكونور، ت. وفينج، ج. (2025). *الحوثيون يحذرون السعودية والإمارات من "العواقب الوخيمة" في حال دعم عملية برية ضدهم*

[541] "إنسيكت غروب" (2018). *الأبعاد الأساسية للحرب الأهلية في اليمن: السيطرة على الإنترنت Underlying Dimensions of Yemen's Civil War: Control of the Internet*. [متاح على الإنترنت] Recordedfuture.com. متوفر على:
https://www.recordedfuture.com/research/yemen-internet-activity [تم الوصول إليه في 25 آب/أغسطس 2025].

في مجموعة تقوم بالتهديد السيبراني ويرجّح أنها موالية للحوثيين، ووجدت أنها استخدمت فيروس حصان طروادة للوصول عن بعد (RAT)، وهو نوع من برمجيات التجسس التي تمكّن المستخدم من التحكم بالأجهزة عن بُعد بشكلٍ سري، لاستهداف أفراد المجتمع المدني وقطاع التنمية.[542] وبالتالي، بعد أن قام الحوثيون بتطوير أجهزة المراقبة، باتوا يعتقلون بشكل متكرر أعضاء المجتمع المدني والصحافيين الذين يعارضون السردية الرسمية.[543]

الحادثة

في 7 أيار/مايو 2024، تلقّى الصحافي إشعاراً عبر بريده الإلكتروني على حساب "جيميل" يفيد بأن رقم هاتفه المسجّل في حسابه على منصة ياهو قد تغيير. وكان الصحافي يعتمد على حساب ياهو كبريد إلكتروني أساسي، ويستخدم حساب جيميل كحساب احتياطي. ويشترك برقم هاتفه المسجّل على حساب ياهو في الشركة اليمنية العمانية المتحدة للاتصالات (يو)، والتي يسيطر عليها الحوثيون. وبعد أن استولت الجهات القائمة بالتهديد على حساب ياهو، قامت على الفور بإعادة تعيين كلمة المرور، وربط الحساب بحساب آخر، وتغيير البريد الإلكتروني الاحتياطي، وإضافة عناوين بريد جديدة، فضلاً عن تغيير الاسم وتاريخ الميلاد المرتبطين بالحساب.

أولاً، غيّرت الجهات القائمة بالتهديد اسم حساب الصحافي إلى "محمد عبد الكريم"، ثم إلى اسم آخر لم تتمكن منظمة "سمكس" من تحديده. بعد ذلك، حذفوا حسابه الاحتياطي على "جيميل"، وقاموا بربطه بحساب منفصل على "فيسبوك" ينتحل شخصيته. وربط هذا الحساب المزيّف بصفحة أخبار رياضية يمنية يبلغ عدد متابعيها أكثر من 283,000 شخص.

[542] "إنسيكت غروب". (2023). *"أويل ألفا": مجموعة يُرجّح أنها موالية للحوثيين تستهدف كيانات في مختلف أنحاء شبه الجزيرة العربية OilAlpha: a Likely Pro-Houthi Group Targeting Entities across the Arabian Peninsula*. [متاح على الإنترنت] ص. 2. متوفر على: https://assets.recordedfuture.com/insikt-report-pdfs/2023/cta-2023-0516.pdf. [تم الوصول إليه في 25 آب/أغسطس 2025].

[543] جمال بلعياشي (2025). *كيف يشن الحوثيون في اليمن حملة قمع رقمية؟*

الصورة 32: صفحة الرياضة اليمنية على "فيسبوك" التي تم ربطها بالحساب المزيّف

في تلك اللحظة، أدرك الصحافي أنه فقد القدرة على الوصول إلى رقم هاتفه. وأفاد أفراد عائلته بأنهم لم يتلقوا مكالماته، في حين لاحظ هو أن وحدة تعريف المشترك في وضعية X، ما يشير إلى وجود خلل في الاتصال بشركة الاتصالات. وفضلاً عن تمكن الجهات القائمة بالتهديد من الوصول بوضوح إلى اسماء المستخدمين وكلمات المرور الخاصة به والسيطرة عليها، نجحت أيضاً في اعتراض عملية المصادقة متعددة العوامل، وتمكنت من الوصول إلى جميع حساباته على وسائل التواصل الاجتماعي، وحاولت حذف هذه الحسابات وجميع محتوياتها.

حاول الصحافي التواصل مع شركة الاتصالات لاستعادة إمكانية الوصول إلى رقم هاتفه اليمني ووقف هذه الهجمات، ولكن من دون جدوى. وعلى مدار الأشهر الأربعة التالية، تهربت الشركة منه ولم تقدم أي تحديثات فعلية. بعد ذلك، لجأ إلى مختبر آخر للأدلة الجنائية الرقمية، والذي تواصل مع "فيسبوك" نيابة عنه، وتمكن من استعادة حسابه. ولكن بمجرد أن علمت الجهات المخترقة باستعادته للحساب، حاولت استرجاعه من خلال تسجيل الدخول من أجهزة كان الصحافي قد سجل دخوله منها سابقاً، وإضافة بريد إلكتروني مزيف يشبه بريده بغرض إعادة تعيين كلمة المرور، والتواصل مع "فيسبوك" للادعاء بأنه شخص منتحل يحاول سرقة الحساب. وأرسلت هذه الجهات بطاقة هويته الوطنية إلى "فيسبوك"، مما دفع المنصة إلى مطالبته بإثبات هويته. وعلى الرغم من استجابته، لا تزال المنصة تقيّد حسابه حتى اليوم. وبسبب ذلك، اضطر الصحافي إلى إنشاء حساب جديد على "فيسبوك". وفي وقت لاحق، تمكّن بمساعدة المختبر الآخر من استعادة بقية حساباته الأخرى.

استناداً إلى التحليل الجنائي للبيانات التي تمكنت منظمة "سمكس" من جمعها بعد إعادة ضبط هاتف الصحافي، يرجّح مختبر التدقيق الجنائي الرقمي، باحتمالية ضعيفة، أنه استُهدف بسلالة غير معروفة من برامج التجسس، بهدف الحصول على بيانات الدخول إلى حساباته على وسائل التواصل الاجتماعي. ولا تستطيع المنظمة التأكد من ذلك، إلا أن الصحافي أفاد أنه لم يضغط على أي روابط خبيثة، ولم يتلق رسائل مشبوهة، ولم يشارك بياناته مع أي شخص غير موثوق. وتقدّر منظمة "سمكس" أيضاً، باحتمالية ضعيفة، أن الجهات القائمة بالتهديد قد حصلت على معلوماته ورموز المصادقة متعددة العوامل، عبر استخدام برمجيات خبيثة، مثل برامج تسجيل مفاتيح الكتابة (كي لوغر)، أو من خلال تقنيات اختراق، مثل هجمات الخصم في الوسط.[544]

هدد هذا الهجوم بتدمير سنوات من العمل التي كرّسها الصحافي لبناء حضوره على شبكات التواصل الاجتماعي. وعند مناقشة تأثير الهجوم عليه وعلى عمله، قال لـمنظمة "سمكس":

"شعرت وكأنني فقدت كل ما بنيته على مدى سنوات طويلة من العمل الشاق والجهد. فأنا أعمل منذ العام 2009 بشكل مستمر في مجال [الإعلام]، وتبخر كل هذا الجهد في لحظة واحدة... لسوء الحظ... بسبب هذا الاختراق، فقدت السيطرة على كل شيء."

بالنسبة للصحافي، شكّل حضوره على وسائل التواصل الاجتماعي ثمرة ما بناه طوال مسيرته المهنية. ولذلك أراد مقاومة الاختراق. ولكن، عندما سيطرت الجهات القائمة بالتهديد على حساباته على وسائل التواصل الاجتماعي، هددته بنشر معلوماته الشخصية علناً إذا لم يتوقف عن التحدث عن هذه الحادثة. ومكّنتها عملية الاختراق أيضاً من سرقة معلومات تتعلق بمصادره الصحافية، وهددته بنشرها. ولّدت هذه الحادثة لدى الصحافي شعوراً دائماً بالذعر والخوف الشديدين. وعند الحديث عن تجربته السابقة مع الاحتجاز لدى الحوثيين، صرّح لمنظمة "سمكس":

"كشخص سبق احتجازه، كنت أعيش في قلق دائم. في اليمن، بعد أن اعتقلت مرتين بسبب عملي الصحافي. في المرة الثانية... أُجبرت على توقيع تعهد بعدم ممارسة أي نشاط صحافي في المستقبل، تحت تهديد الإعدام... وحتى بعد أن أطلق سراحي، ظللت أعيش في حالة خوف إلى أن غادرت اليمن في النهاية."

---

[544] تشير برامج تسجيل مفاتيح الكتابة إلى برمجيات خبيثة ترصد ما يكتبه المستخدمون على جهاز الكمبيوتر أو الهاتف المحمول، ويمكنها تتبع نشاطهم من خلال التقاط صور للشاشة. وتشير هجمات الخصم في الوسط إلى تقنية اختراق تحاول فيها الجهات القائمة بالتهديد بإجبار جهاز الضحية على التواصل مع أنظمة خبيثة، ليتمكنوا من الحصول على معلومات عن المستخدم المستهدف.

تغيرت حياته بالكامل بعد تعرضه للاستهداف والمراقبة الرقميين. فقد غادر اليمن على الفور، وانتقل إلى مصر، ثم لبنان، قبل أن يستقر في النهاية في فرنسا، حيث يقيم حتى اليوم. ويَعتقد أنه تعرض لمحاولة استهداف جديدة بعد فترة قصيرة من مغادرته اليمن، إذ واجه هجوماً سيبرانياً آخراً أثناء إقامته في مصر. وشعر بحاجة ملحة إلى تحديث إجراءات الأمان الرقمية طوال فترة تنقله: فغيّر كلمات المرور، واستبدل جميع أجهزته الإلكترونية، وبدأ باستخدام عناوين بريد إلكتروني جديدة في كل دولة زارها. ومع ذلك، تغير أسلوب عمله بشكل يكاد لا يُصدق عمّا كان عليه في السابق. فبعد أن كان يعتمد علناً على منصات التواصل الاجتماعي لنشر أعماله، أصبح اليوم "أكثر تحفظاً في التواصل وأقل ظهوراً على المنصات العامة" بهدف الحفاظ على سلامته الشخصية. وقال: "لقد ترك الهجوم أثراً نفسياً ومهنياً واضحاً [عليّ]."

وفي حين لا يستطيع محللو مختبر التدقيق الجنائي الرقمي في منظمة "سمكس" تحديد موردي برامج التجسس التجارية الذين قاموا بتشغيل هذه السلالة من برامج التجسس حتى الآن، إلا أنهم يقدّرون، باحتمالية ضعيفة واستناداً إلى التحليل الأولي، أنه استهدف ببرامج مراقبة. ويأمل المختبر في جمع معلومات إضافية حول هذه الحالة ونشر تفاصيل إضافية في وقت لاحق. لقد دمر هذا الاستهداف مسيرته المهنية على المدى القصير، وأجبره على الفرار من بلده على المدى الطويل، ما قضى على أي إحساس بالأمان المالي والنفسي الذي كان يعرفه سابقاً. ويبدو أن برامج التجسس أدت دوراً أساسياً في تقويض حرية الصحافة والتعبير في اليمن، وتسببت في الوقت ذاته بإسكات صحافي وتدمير مسيرته المهنية.

يشعر الصحافي أن حياته انقلبت رأساً على عقب. ومنذ الهجوم الأول، لم يعد يعرف السلام. ومع ذلك، وبعد أن اختطف مرتين وواجه تهديداً بالإعدام، لم يكن هذا الهجوم إلا مجرد محاولة أخرى لإسكات أي شخص يجرؤ على تحدي أصحاب السلطة.

الأفكار الختامية

حققت منظمات الرقابة، والجهات الدولية الإدارية، والباحثون المستقلون تقدماً كبيراً في كشف انتشار برامج التجسس في العالم، وطالبوا موردي برامج التجسس التجارية بوقف بيعها. وقامت لجنة "بيغا" التابعة للاتحاد الأوروبي، والتي تولت التحقيق في برامج "بيغاسوس" وسلالات أخرى من برامج التجسس، بتسليط الضوء الضروري على آليات عمل مجموعة "إن إس أو".[545] وقدمت منظمة العفو الدولية، ومنظمة أكسس ناو (Access Now)، ومختبر "سيتيزن لاب"، ومنظمة "هيومن رايتس ووتش"، وغيرها من المجموعات، مساهمات جنائية لا تحصى ولا تعد. وحققت هذه الجهود نتائج ملموسة في مواجهة برامج التجسس: إذ توقف كبار موردي برامج التجسس التجارية مثل شركة "فين فيشر" (FinFisher) وشركة "كوادريم" عن العمل. وتعهد عدد كبير من كبار المستثمرين في مجال الأمن السيبراني (طوعاً) بعدم الاستثمار في برامج التجسس، أو بسحب استثماراتهم المقدمة لموردي برامج التجسس التجارية، وأصبح الاستثمار في شركات مثل مجموعة "إن إس أو" يعتبر، في كثير من الأحيان، مضراً بالسمعة، خصوصاً بعد فرض حكومة الولايات المتحدة عقوبات عليها.[546] وفي مثال حديث، سحب صندوق الثروة السيادي النرويجي، والذي تزيد قيمته عن تريليون دولار أمريكي، جميع استثماراته في شركة برامج التجسس الإسرائيلية "كوغنيت" في العام 2022 بعد اتهامها بارتكاب "انتهاكات خطيرة للغاية لحقوق

---

[545] إينت فيلد، ص. *تقرير التحقيق في ادعاءات الانتهاكات وسوء الإدارة في تطبيق قانون الاتحاد الأوروبي بشأن استخدام برامج التجسس "بيغاسوس" وبرامج المراقبة المماثلة REPORT of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware*.

[546] فرانشيسكي-بيكييراي، ل. *تعهّد المستثمرين بمكافحة برامج التجسس تقوّضه استثماراتهم السابقة في شركة أمريكية متخصصة في تطوير البرمجيات الخبيثة Investors' Pledge to Fight Spyware Undercut by past Investments in US Malware Maker*. [متاح على الإنترنت] موقع تك كرانش. متوفر على: https://techcrunch.com/2024/03/22/us-cyber-investors-pledge-spyware-is-off-limits-with-a-catch/ [تم الوصول إليه في 22 آذار/مارس 2024].

الإنسان."[547] ويبدو أن الضرر المترتب على السمعة يتزايد أيضاً بالنسبة لصانعي برامج التجسس. وكما ورد في القسم 3.1، تكبدت مجموعة "إن إس أو" خسائر فادحة بعد الكشف عن تحقيقات تتعلق ببرامجها، واعتبر عدد من المستثمرين أن الشركة فقدت، في مرحلة ما، قيمتها العملية. وفرضت وزارة الخزانة الأمريكية أيضاً عقوبات على عدد من صانعي برامج التجسس، وتشمل معظم الجهات التي تناولها هذا التقرير.

وعلى الرغم من هذه التغييرات المشجعة، لا يبدو أن استخدام برامج التجسس يشهد أي تباطؤ. وبينما تتزايد الإدانات الموجهة إلى موردي برامج التجسس التجارية، لم يتوقفوا عن بيع منتجاتهم. وعلى خلاف ذلك، تشير الأدلة إلى العكس تماماً: إذ أصبحوا يخبؤون أعمالهم، ويلجؤون إلى تغيير أسمائها التجارية، ويحجبون أنشطتهم من خلال طبقات متعددة من الهياكل الإدارية، ويدّعون الالتزام بمعايير حقوق الإنسان، في حين يواصلون فيه بيع برامجهم لحكومات تسيء استخدامها وتوظفها للقمع. وأشار فيلدستاين وكوت في العام 2023، إلى أنه، وعلى الرغم من وقف أعمال بعض كبار موردي برامج التجسس التجارية بسبب قضايا مثيرة للجدل، ظهر عدد كبير من الموردين الصغار لسد هذه الفجوة في السوق وبيع منتجات تجسس مشابهة.[548]

علاوة على ذلك، تشدد "مؤسسة كارنيغي للسلام الدولي" على أن الدول الديمقراطية لم تلتزم التزاماً كاملاً بالحظر على بيع برامج التجسس واستخدامها. وفي حين يفرض الاتحاد الأوروبي لوائح تنظيمية صارمة على المنتجات ذات الاستخدام المزدوج، مثل برامج التجسس، تعتمد بعض الدول الأوروبية معايير أقل صرامة في تنفيذها، ما يسمح لموردي برامج التجسس التجارية بالتحايل على اللوائح التنظيمية ومواصلة عملهم في جميع أنحاء أوروبا (وبشكل أوسع، في العالم).[549] وتمثّل الولايات المتحدة مثالاً آخر على ذلك. فعلى الرغم من العقوبات التي فرضتها حكومتها على عدد من كبار موردي برامج التجسس التجارية، فإنها لا تزال تحتفظ بعقود سارية المفعول مع بعض الموردين. ويُشير ذلك إلى أن العقوبات والقوانين التي تحظر برامج التجسس، فضلاً عن التقارير التي تحقق في استخدام هذه التكنولوجيا، لا تكفي للحد من أنشطة موردي هذه البرامج، سواء في منطقة غرب آسيا وشمال أفريقيا أو خارجها. ولا نستطيع التأكد من مدى إحداث هذه العقوبات أثراً مستداماً على قدرة هؤلاء الموردين على الاستمرار في العمل. وعلى سبيل المثال، نشر باحثو شركة "إنسيكت غروب" في 5 آب/أغسطس 2025 بحثاً جديداً تتبّع استخدام برامج التجسس التابعة لشركة "سايتو تيك" في السعودية، على الرغم من العقوبات المفروضة عليها.[550] وبالتالي، تدعو منظمة "سمكس" المدافعين عن حقوق الإنسان، والحكومات في جميع أنحاء العالم، والمستثمرين إلى مواجهة انتشار برامج التجسس ومكافحتها، نظراً لأنها تكنولوجيا تنتهك حقوق الإنسان في جوهرها.

ولكن، لا يرجّح أن تتوقف شركات برامج التجسس ببساطة عن بيع منتجات البرمجيات الخبيثة المربحة لمجرد مطالبة منظمات الدفاع عن حقوق الإنسان بذلك. وبالتالي، تشدد منظمة "سمكس" على ضرورة اعتماد الفئات المعرّضة للخطر (مثل المدافعين عن حقوق الإنسان، وأعضاء المجتمع المدني، وغيرهم) في منطقة غرب آسيا وشمال أفريقيا أفضل ممارسات الأمن السيبراني، لتمكينهم من حماية أنفسهم على النحو الأفضل من برامج التجسس. وتماشياً مع توصيات منظمة العفو الدولية ومنظمة التخوم الإلكترونية، تحثّ منظمة "سمكس" على اتباع الإرشادات التالية:[551] [552]

---

[547] شولمان، س. *شركة "كوغنايت" تعاني من تداعيات القرار بعد إخراجها من استثمارات صندوق الثروة السيادي النرويجي Cognyte Reeling after Being Dropped by Norway Sovereign Wealth Fund*. [متاح على الإنترنت] موقع صحيفة كالكاليست تيك. متوفر على: https://www.calcalistech.com/ctechnews/article/r1yexabyi [تم الوصول إليه في 27 آب/أغسطس 2025].

[548] فيلدستاين، س.، وكوت، ب. (2023). *لماذا تستمر صناعة برامج التجسّس العالمية في الازدهار؟* Why Does the Global Spyware Industry Continue to Thrive?

[549] فيلدستاين، س.، وكوت، ب. (2023). *لماذا تستمر صناعة برامج التجسّس العالمية في الازدهار؟*

[550] "إنسيكت غروب" (2025). *تتبع برنامج التجسس برنامج "لسان الشيطان" (Devil's Tongue) التابع لشركة "كانديرو" في دول متعددة*.

[551] منظمة العفو الدولية (2023). *ما هي برمجيات التجسس وماذا يمكنكم فعله لحماية أنفسكم؟ - مختبر الأمن التابع لمنظمة العفو الدولية* [متاح على الإنترنت] مختبر الأمن التابع لمنظمة العفو الدولية. متوفر على: https://securitylab.amnesty.org/latest/2023/12/what-is-spyware-and-what-can-you-do-to-stay-protected/.

[552] منظمة التخوم الإلكترونية (التاريخ غير متوفر). *أساسيات الدفاع عن النفس ضد الرقابة*. [متاح على الإنترنت] مشروع الدفاع عن النفس ضد الرقابة. متوفر على: https://ssd.eff.org/module-categories/basics [تم الوصول إليه في 11 آب/أغسطس 2025].

- إعداد خطة أمنية لاستخدام الإنترنت؛
- المواظبة على تحديث أنظمة تشغيل الهواتف المحمولة وأجهزة الكمبيوتر، وبرامج التصفح على شبكة الإنترنت؛
- تفعيل إعدادات الأمن المتقدمة على الأجهزة، مثل "حالة الإغلاق" (Lockdown Mode) على أجهزة أبل؛
- الحرص على تجنب النقر على الروابط أو فتح المستندات المرسلة من غرباء؛
- مراقبة أي تغييرات في أداء الجهاز، والانتباه إلى أي سلوك غير معتاد قد يشير إلى إصابته ببرمجيات خبيثة؛
- استخدام شبكة افتراضية خاصة (VPN) من شركة موثوقة بشكلٍ دائم؛
- تغيير إعدادات الخصوصية في حسابات التواصل الاجتماعي لرفع مستوى الخصوصية، وتوخي الحذر عند قبول طلبات الصداقة أو المتابعة الجديدة؛
- تشفير الأجهزة متى أمكن ذلك؛
- تفعيل خاصية المصادقة الثنائية (2FA)؛
- استخدام تطبيقات مراسلة مشفرة بالكامل مثل سيجنال؛
- اختيار كلمات مرور قوية وفريدة لكل حساب؛
- إدارة كلمات المرور باستخدام برامج مخصصة لذلك.

توصي منظمة "سمكس" بمواصلة إجراء أبحاث حول موردي برامج التجسس التجارية العاملين في منطقة غرب آسيا وشمال أفريقيا، مع التركيز بشكل خاص على الشركات الصغيرة والمتخصصة. فتعتبر المعلومات المتاحة علناً عن أنشطتهم محدودة للغاية، ويمكن تحقيق فائدة كبيرة من خلال تحديث المعرفة حول الموردين والبرامج العاملة حالياً في المنطقة. وعلى الرغم من أن المعركة ضد برامج التجسس لا تزال طويلة ولم تحسم بعد، فهذا لا يعني أنها ستبقى كذلك إلى الأبد.

الملحق "أ"

البيانات وعرض مرئي لحوادث برامج التجسس في خلال السنوات الأربع عشرة الماضية

أنشأت منظمة "سمكس" جدولاً يضم حوادث برامج التجسس التي وقعت في خلال السنوات الأربع عشرة الماضية، بالاعتماد على أحدث مجموعة بيانات نشرها فيلدستاين وكوت في العام 2023. وللاطلاع على العرض المرئي لهذه البيانات، يرجى زيارة منصة Datarwapper عبر هذا الرابط.

ملاحظة عن شركة "ميمينتو لابز"

تحكي شركة "ميمينتو لابز" قصة معقدة. فكما ورد في القسم 2.4، تحتل الشركة المرتبة الثانية (بالتساوي مع شركة أخرى) من الناحية التقنية ضمن مجموعة البيانات هذه. ومع ذلك، فإن آخر حادثة أبلغ عنها علناً وارتبطت بهذه الشركة وقعت قبل عقد من الزمن. وبناءً على منهجية هذا التقرير، لو اقتصر التحليل على السنوات الخمس الأخيرة فقط، فلن تظهر الشركة إطلاقاً.

في أعقاب تعرّض شركتها السابقة "هاكينغ تيم" (Hacking Team) لعملية اختراق شهيرة، وتورطها بالتالي في فضيحة كبيرة في العام 2015، أفادت وسائل إعلام كبرى أن شركة "ميمينتو لابز" واجهت صعوبات كبيرة في إعادة بناء نفسها بعد سنوات من الحادثة.[553] وعلى الرغم من أنها كانت تعتبر عملاقاً في مجال الاختراق وتمتلك عقوداً في جميع أنحاء العالم، لم تعد هذه الشركة اللاعب الأساسي الذي كانت عليه في السابق. ومع ذلك، يبدو أنها لا تزال نشطة، على الرغم من عدم ارتباطها بأي حوادث كبيرة لبرامج التجسس في خلال العقد الماضي. وتدرج في ما يلي بعض الأدلة التي تشير إلى استمرار نشاط هذه الشركة في منطقة غرب آسيا وشمال أفريقيا:

- اعتبرت شركة "هاكينغ تيم" إحدى أكثر الشركات استخداماً في منطقة غرب آسيا وشمال أفريقيا، إذ امتلكت عقوداً مع ثماني حكومات في المنطقة على الأقل قبل تعرضها للاختراق في العام 2015.[554]
- في العام 2016، اشترت المملكة العربية السعودية حصة قدرها 20% في شركة "هاكينغ تيم" لمساعدتها على تجنّب الإفلاس الكامل، على الرغم من تعرضها للاختراق في العام 2015، ما يثير تساؤلات حول دوافع السعودية للاستمرار في العمل معها.[555]
- في العام 2028، أفاد باحثو شركة الأمن السيبراني السلوفاكية "إسيت" (ESET) أنهم اكتشفوا آثاراً جديدة للمنتج الرئيس لشركة "هاكينغ تيم"، وهو نظام التحكم عن بُعد، وكان هذا النظام قيد التشغيل قبل عام واحد من استحواذ المستثمر السويسري "إن ذا سايبر" (InTheCyber) على الشركة وإعادة تسميتها إلى "ميمينتو لابز" في العام 2019.[556]
- وفي العام 2023، أفادت صحيفة "نويه تسوريشر تسايتونغ" السويسرية بأن المستثمر إن ذا سبير سعى بنشاط إلى بيع منتجات التجسس في الإمارات العربية المتحدة، بشكل مباشر وعبر موزعين في دبي. وقد ظهرت الشركة أيضاً مرتين ضمن قائمة العروض التقديمية في المعرض العالمي لأنظمة الدعم الاستخباراتي لعام 2023 في دبي. وأوضح تقرير الصحيفة أن الشركة امتلكت حتى العام 2023 عقد ساري المفعول مع شركة التوزيع "أس آي تي المحدودة" (S.A.T. Trading LLC)، التي تتخذ من دبي مقراً لها وتسوق منتج "تاكتيكال إكسيكيوتور" (Tactical Executor) الذي طورته شركة "ميمينتو لابز"، وهو منتج يتفاخر بقدرته على اختراق أنظمة "ويندوز" المشفرة.[557]

---

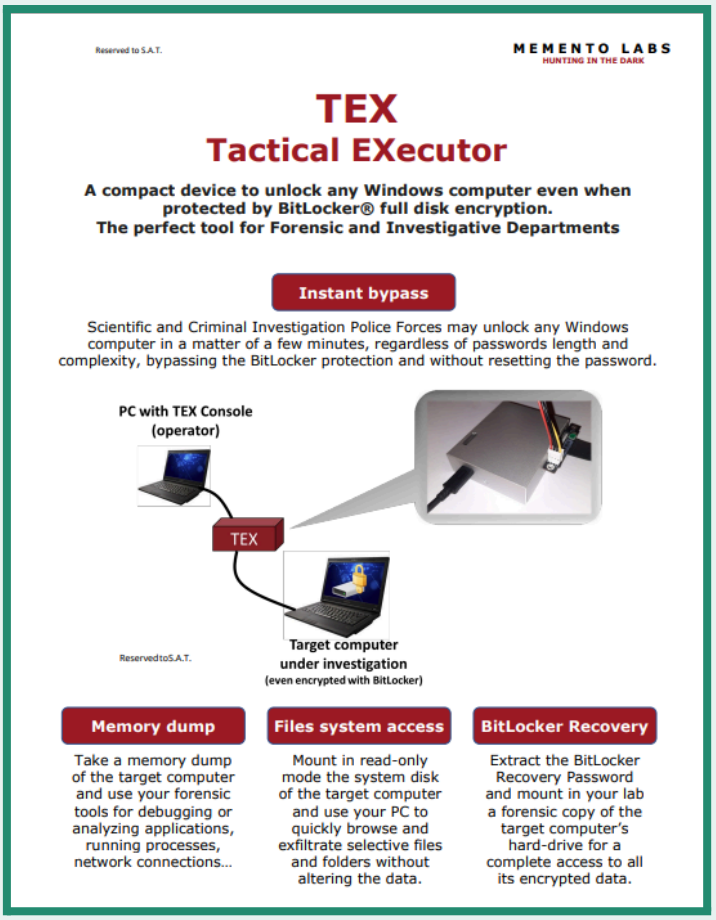
[553] كوكس، ج. فرانشيسكي-بيكييراي، ل. (2020). *شركة "ميمينتو لابز"، الاسم الجديد لشركة "هاكينغ تيم"، تواجه صعوبات Memento Labs, the Reborn Hacking Team, Is Struggling*. [متاح على الإنترنت] موقع "فايس" (VICE). متوفر على: https://www.vice.com/en/article/memento-labs-the-reborn-hacking-team-is-struggling/. [تم الوصول إليه في 19 تموز/يوليو 2025].

[554] فيلدستاين، س.، وكوت، ب. (2023). *لماذا تستمر صناعة برامج التجسّس العالمية في الازدهار؟*

[555] فرانشيسكي-بيكييراي، ل. (2018) شركة "هاكينغ تيم" لا تزال مستمرة بفضل مستثمر مجهول من المملكة العربية السعودية Hacking Team Is Still Alive Thanks to a Mysterious Investor From Saudi Arabia. [متاح على الإنترنت] موقع "فايس" (VICE). متوفر على: https://www.vice.com/en/article/hacking-team-investor-saudi-arabia/ تم الوصول إليه في 15 تموز/يوليو 2025].

[556] كافكا، ف. *اكتشاف آثار جديدة لشركة "هاكينغ تيم" قيد التشغيل الفعلي New traces of Hacking Team in the wild*. [متاح على الإنترنت] شركة "إسيت". متوفر على: https://www.welivesecurity.com/2018/03/09/new-traces-hacking-team-wild/.

[557] لوكاس مادير (2023). *شركة سويسرية تبيع برامج تجسس لأجهزة المخابرات العربية Swiss company sells spy software to Arab intelligence services*. [متاح على الإنترنت] صحيفة "نويه تسوريشر تسايتونغ". متوفر على:



الصورة 33: منشور دعائي من كانون الأول/ديسمبر 2022 يُقدّم معلومات عن منتج جديد من شركة "ميمينتو لابز"، كما أوردته صحيفة" نويه تسوريشر تسايتونغ" في 2023.

Reserved to S.A.T.	مملوك لشركة التوزيع أس آي تي المحدودة
MEMENTO LABS - HUNTING IN THE DARK	شركة ميمينتو لابز – الصيد في الخفاء
TEX Tactical EXecutor A compact device to unlock any Windows computer even when protected by BitLocker® full disk encryption. The perfect tool for Forensic and Investigative Departments	تي آكس تاكتيكال إكسيكيوتور (Tactical Executor) جهاز مدمج لاختراق أي جهاز كمبيوتر يشغّل بنظام "ويندوز"، حتى في حال كان محمياً بتشفير القرص الصلب الكامل "بت لوكر" (BitLocker®). يمثّل الأداة المثالية لإدارات التحليل الجنائي والتحقيق
Instant bypass	تجاوز فوري

https://www.nzz.ch/english/a-swiss-company-is-selling-spy-software-to-arab-intelligence-services-the-federal-government-supports-them-ld.1739341 [تم الوصول إليه في 17 تموز/يوليو 2015].

Scientific and Criminal Investigation Police Forces may unlock any Windows computer in a matter of a few minutes, regardless of passwords length and complexity, bypassing the BitLocker protection and without resetting the password.	**يمكن لقوات الشرطة المختصة بالتحقيق العلمي والجنائي اختراق أي جهاز كمبيوتر يشغّل بنظام "ويندوز" في غضون دقائق معدودة، بصرف النظر عن طول كلمة المرور أو مدى تعقيدها، من خلال تجاوز حماية نظام بت لوكر ومن دون الحاجة إلى إعادة تعيين كلمة المرور.**
PC with TEX Console (operator) TEX Target computer under investigation (even encrypted with BitLocker)	**حاسوب التحكم بجهاز تي آكس (الجهة المشغّلة)** **جهاز تي آكس** **حاسوب الجهة المستهدفة بالتحقيق (حتى في حال كان مشفراً ببرنامج بت لوكر)**
Memory dump: Take a memory dump of the target computer and use your forensic tools for debugging or analyzing applications, running processes, network connections...	**نسخ الذاكرة:** **احصل على نسخة من ذاكرة جهاز الكمبيوتر المستهدف واستخدم أدواتك الجنائية لتحليل وإزالة كل خلل في التطبيقات، والعمليات الجارية، واتصالات الشبكة، وغيرها.**
Files system access : Mount in read-only mode the system disk of the target computer and use your PC to quickly browse and exfiltrate selective files and folders without altering the data.	**الوصول إلى نظام الملفات:** **قم بتركيب قرص النظام الخاص بالجهاز المستهدف في وضع القراءة فقط على جهازك لتصفح الملفات والمجلدات المحددة بسرعة واستخراجها من دون تعديل البيانات.**
BitLocker Recovery: Extract the BitLocker Recovery Password and mount in your lab a forensic copy of the target computer's hard-drive for a complete access to all its encrypted data.	**استعادة تشفير بت لوكر** **استخرج مفتاح استعادة تشفير بت لوكر وقم بتركيب نسخة جنائية من القرص الصلب الخاص بالجهاز المستهدف في مختبرك للوصول بشكلٍ كامل إلى جميع بياناته المشفرة.**

- شاركت شركة "ميمينتو لابز" بشكلٍ فعلي في المعرض العالمي لأنظمة الدعم الاستخباراتي لعام 2025، وروّجت في خلاله لـ "قدرات سيبرانية هجومية رائدة مخصصة لأجهزة الهواتف المحمولة."[558] وتشير كل هذه الأدلة مجتمعةً إلى أن شركة "ميمينتو لابز"، وعلى الرغم من أنها قد لا تحقق النجاح ذاته الذي حققته شركتها السابقة "هاكينغ تيم"، لا تزال تسعى لجذب العملاء في منطقة غرب آسيا وشمال أفريقيا.

[558] المعرض العالمي لأنظمة الدعم الاستخباراتي (التاريخ غير متوفر). *المعرض العالمي لأنظمة الدعم الاستخباراتي لعام 2025 في الشرق الأوسط وأفريقيا: أنظمة الدعم الاستخباراتي لعمليات المراقبة الإلكترونية، ومتابعة وسائل التواصل الاجتماعي/الإنترنت المظلم، والكشف عن التهديدات السيبرانية* [منشور]. [متاح على الإنترنت] متوفر على: https://www.issworldtraining.com/iss_mea/brochure01.pdf.

الصورة 34: العرض التقديمي لشركة "ميمينتو لابز" في المعرض العالمي لأنظمة الدعم الاستخباراتي للعام 2025.

الأربعاء، 12 شباط/فبراير 2025 13:00-13:45	Wednesday, 12 February 2025 13:00-13:45
شبح في الهيكل: قدرات سيبرانية هجومية رائدة مخصصة لأجهزة الهواتف المحمولة	Ghost In the Shell: Cutting Edge Offensive Cyber Capabilities For the Mobile World
عرض مقدّم من شركة ميمينتو لابز	Presented by Memento Labs

أسئلة المقابلة

أجرت منظمة "سمكس" مقابلات مع عدة ضحايا يعتقدون أنهم تعرضوا لهجمات من جهات تهديد متقدمة، بما في ذلك برامج التجسس المحتملة. وتدرج في ما يلي الأسئلة التي وجهتها المنظمة لهم بعد أن تواصلوا مع مختبر التدقيق الجنائي الرقمي:

الخلفية الأساسية

1) من أين أنت/أين نشأت؟

الهجوم

2) ماذا حدث لك؟
3) متى لاحظت لأول مرة أن هناك مشكلة؟ ماذا لاحظت تحديداً؟ ماذا فعلت في تلك اللحظة؟
4) هل سمعت عن الاختراقات الإلكترونية، أو برامج التجسس، أو المراقبة الحكومية قبل هذا الهجوم؟
5) هل اتخذت أي احتياطات على الإنترنت قبل هذا الهجوم؟

الأثر

6) كيف أثر هذا الهجوم السيبراني على حياتك؟
7) كيف أثر على نمط حياتك؟
8) هل اضطررت لتغيير أسلوب حياتك استجابةً للهجوم؟
9) كيف تعيش الآن بعد أن مررت بهذه التجربة؟