حملة - المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

جامعة بيرزيت
BIRZEIT UNIVERSITY
معهد ابراهيم أبو لغد للدراسات الدولية
Ibrahim Abu-Lughod Institute of International Studies

السياسة الصناعية ذات الطابع العسكري وشركات المراقبة الإسرائيلية

ورقة بحثية ضمن كتاب

"الهيمنة الرقمية: الذكاء الاصطناعي والمراقبة والسلطة الرقمية في فلسطين وما بعدها"

إسلام الخطيب

السياسة الصناعية ذات الطابع العسكري وشركات المراقبة الإسرائيلية

إسلام الخطيب

إسلام مرشحة دكتوراه في مناهج البحث الاجتماعي في كلية لندن للاقتصاد والعلوم السياسية. وُلدت ونشأت في لبنان، وهي باحثة فلسطينية لاجئة يتركز عملها على إنتاج المعرفة المناهضة للاستعمار. تربط أبحاثها بين المراقبة والبُنى التحتية للتكنولوجيا العالمية ومنظومات الهيمنة.

يبحث مشروع إسلام كيف تُدمَج تقنيات المراقبة الإسرائيلية في سلاسل توريد التكنولوجيا العالمية. ومن خلال خرائط استقصائية، تتبّع كيف يُعاد تسويق أدوات طُوِّرت للاحتلال وتُدمج داخل أنظمة الحوكمة العالمية تحت مسميات «السلامة العامة» أو «الأمن السيبراني».

مقدمة

تنبع مكانة إسرائيل كقوة سيبرانية عالمية من منظومة محكمة الترابط بين القطاعين العام والخاص، تصل المؤسسة العسكرية والاستخباراتية بقطاع متقدم لتكنولوجيا المراقبة. [1] وقد تشكّل هذا النظام البيئي عبر عقود من الهيمنة الاستعمارية الاستيطانية والاحتلال العسكري، بما يتيح التطوير السريع للأدوات الرقمية وصقلها ونشرها، وهي أدوات مصممة للمراقبة والتصنيف والإزالة. [2] وتُختبر هذه التقنيات أولاً على الفلسطينيين، ولا سيما في غزة والضفة الغربية، ثم تُطوَّر لاحقاً لأغراض التصدير. [3] وكما يجادل لوينشتاين في كتابه الصادر عام 2023 حول فلسطين بوصفها مختبراً، فقد تحوّل الاحتلال الإسرائيلي إلى نموذج مربح من رأسمالية المراقبة. وأصبح الفلسطينيون موضوعاً لما بات يُعرَّف على نطاق واسع بأنه أول إبادة جماعية في العالم مدعومة بالذكاء الاصطناعي. [4]

تجاوزت شركات الأمن الإسرائيلية منذ زمن طويل دور تسليح الأنظمة القمعية، إذ غدت مندمجة في مشاريع أمنية نيوليبرالية تجعل من الخبرة ذات الطابع العسكري رأسمالاً متنقلاً، يتداول عبر الأسواق العابرة للحدود بطرق تعيد إنتاج الهيمنة المتمحورة حول الولايات المتحدة وتعززها. [5] وغالباً ما تدخل الشركات الإسرائيلية إلى أسواق يتجنبها موردون آخرون. [6] ففي أنحاء أمريكا اللاتينية وأفريقيا وآسيا، رسخت إسرائيل مكانة استراتيجية خاصة من خلال تزويد الدول بحزم متكاملة من البنى التحتية العسكرية والرقمية للمراقبة. [7] وقد وفّرت الأراضي الفلسطينية المحتلة واجهة العرض لهذا النموذج: فتقنيات السيطرة على السكان التي صُقلت في القدس الشرقية [8] والضفة الغربية [9] وغزة، [10] من المراقبة البيومترية المستمرة، إلى الشرطة التنبؤية، والجدران عالية التقنية والطائرات المسيّرة، يُعاد تغليفها للتصدير بوصفها منتجات لـ»الأمن الداخلي». [11] وبالفعل، بحلول منتصف العقد الثاني من

1 Privacy International, “Big Tech’s Bind with Military and Intelligence Agencies,” Privacy International, October 1, 2025, https://privacyinternational.org/long-read/5683/big-techs-bind-military-and-intelligence-agencies.

2 Ihab Maharmeh, “AI as a Tool for Settler-Colonial Projects: How Israel Employs AI to Intensify Colonial Dominance under the Pretext of Counterterrorism,” Critical Studies on Terrorism (2025): 1–24, https://doi.org/10.1080/17539153.2025.2603049

3 Antony Loewenstein, The Palestine Laboratory: How Israel Exports the Technology of Occupation around the World (London: Verso Books, 2023).

4 Amber Rahman, “Explainer: The Role of AI in Israel’s Genocidal Campaign against Palestinians,” Institute for Palestine Studies, 2019, https://www.palestine-studies.org/en/node/1656285.

5 Shir Hever, The Privatization of Israeli Security (London: Pluto Press, 2018).

6 Justice For Myanmar, “Israel’s CAA Industries Ltd Suspected to Have Aided and Abetted the Myanmar Military’s War Crimes and Crimes against Humanity,” June 8, 2023, https://www.justiceformyanmar.org/stories/israels-caa-industries-ltd-suspected-to-have-aided-and-abetted-the-myanmar-militarys-war-crimes-and-crimes-against-humanity

7 Who Profits, “Repression & Diplomacy,” Who Profits Research Center, 2022, https://www.whoprofits.org/publications/report/52?repression-diplomacy

8 Sophia Goodfriend, The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights (7amleh – The Arab Center for Social Media Advancement, Summer and Fall 2021), https://7amleh.org/storage/Digital%20Surveillance%20Jerusalem_7.11.pd

9 Amnesty International, “Ban the Scan,” https://banthescan.amnesty.org/opt/

10 Business & Human Rights Resource Centre, “Palantir Allegedly Enables Israel’s AI Targeting amid Israel’s War in Gaza, Raising Concerns over War Crimes,” Business & Human Rights Resource Centre, https://www.business-humanrights.org/en/latest-news/palantir-allegedly-enables-israels-ai-targeting-amid-israels-war-in-gaza-raising-concerns-over-war-crimes/.

11 Rohan Talbot, “Automating Occupation: International Humanitarian and Human Rights Law Implications of the Deployment of Facial Recognition Technologies in the Occupied Palestinian Territory,” International Review of the Red Cross 102, no. 914 (2020): 823–49, https://doi.org/10.1017/s1816383121000746.

القرن الحادي والعشرين، باتت إسرائيل تُعرف بأنها «عاصمة الأمن الداخلي»[12] العالمية، إذ تضم أكبر عدد من شركات تكنولوجيا المراقبة للفرد في العالم. [13]

والأهم من ذلك أن وزارة الدفاع الإسرائيلية تضطلع بدور فاعل في تشكيل هذا النظام البيئي. فمن خلال مديرية البحث والتطوير التابعة لها، المعروفة باسم «مافات» (MAFAT)، تربط وزارة الدفاع الطلب العسكري بالابتكار القائم على الشركات الناشئة، ومحوّلةً الاحتياجات العملياتية إلى مسارات تطوير تكنولوجي. [14] وبوصفها واجهة مشتركة بين الوزارة والجهاز التكنولوجي التابع للجيش الإسرائيلي، تنسّق «مافات» بين كبرى شركات الدفاع، بما في ذلك صناعات الفضاء الإسرائيلية ورافائيل وإلبيت سيستمز، مع دمج الجامعات والجهات الفاعلة في القطاع الخاص ضمن شبكة إنتاج موحّدة. [15]

وبحلول عام 2025، وصل هذا التآزر بين القطاعين العام والخاص مستويات غير مسبوقة، إذ جرى دمج أكثر من 130 شركة ناشئة إسرائيلية مباشرة في عمليات الجيش بعد بدء الحرب على غزة عام 2023،[16] تركّز كثير منها على الذكاء الاصطناعي، والأنظمة الذاتية، وأنظمة الاستشعار. وقد جذبت الشركات الناشئة في مجال التكنولوجيا الدفاعية العاملة مع «مافات» تمويلاً تجاوز مليار دولار أمريكي، أي أكثر مما جذبته في جميع السنوات السابقة مجتمعة. [17] ومع بلوغ الإنفاق العسكري العالمي 2. 7 تريليون دولار، يجري استيعاب التقنيات الدفاعية الإسرائيلية بصورة متزايدة في الأسواق العالمية باعتبارها استثمارات عالية العائد. [18] ومن ثم، تصبح الحرب مجالاً مستقراً للتراكم. [19]

وتعمل حالياً في إسرائيل أكثر من ثلاثين شركة مراقبة، أسّس العديد منها أو يعمل فيها قدامى وحدة 8200، وهي وحدة استخبارات إشارات تتمحور مهمتها حول اعتراض الاتصالات الإلكترونية وتحليل البنى التحتية الرقمية. [20] وتندمج هذه الشركات بعمق في البنى التحتية للبيانات العسكرية، ومتوافقة مع أولويات الدولة، مشكلةً ما تصفه صوفيا غودفريند بأنه «مجمع استخباراتي–صناعي».[21]

وفي إطار هذا التشكيل، تعتمد أنظمة الذكاء الاصطناعي مثل «لافندر» و»غوسبل»

12 Neve Gordon, “Israel’s Emergence as a Homeland Security Capital,” in Surveillance and Control in Israel/Palestine: Population, Territory and Power, ed. Elia Zureik, David Lyon, and Yasmeen Abu-Laban (London: Routledge, 2010), 18.

13 Visualizing Palestine, “Fact Sheet: The Israeli Cyber Industry,” Medium, August 30, 2022, https://visualizingpalestine.medium.com/fact-sheet-the-israeli-cyber-industry-d2a64b43094

14 Dean Shmuel Elmas, “Defense Ministry Orders Boost Israeli Startups,” Globes, January 21, 2026, https://en.globes.co.il/en/article-defense-ministry-orders-boost-israeli-startups-1001532687

15 Al-Shabaka: The Palestinian Policy Network, “Insulation Not Isolation: Israel’s Super-Sparta War Economy,” 2026, https://al-shabaka.org/briefs/insulation-not-isolation-israels-super-sparta-war-economy/

16 Dean Shmuel Elmas, “Israeli Defense Tech Startups Attract over $1b in Investment,” Globes, December 8, 2025, https://en.globes.co.il/en/article-israeli-defense-tech-startups-attract-over-1b-in-investment-1001528671

17 Dean Shmuel Elmas, “Israeli Defense Tech Startups Attract over $1b in Investment,” Globes, December 8, 2025, https://en.globes.co.il/en/article-israeli-defense-tech-startups-attract-over-1b-in-investment-1001528671

18 Lisya Bahar Manoah, “Rising Defense Spending: Fueling a Deep Tech Boom in 2026,” Forbes, March 3, 2026, https://www.forbes.com/councils/forbesfinancecouncil/2026/03/03/rising-defense-spending-fueling-a-deep-tech-boom-in-2026/

19 Michael Kwet, “Digital Colonialism: The Evolution of US Empire,” TNI Longreads, March 4, 2021, https://longreads.tni.org/fr/digital-colonialism-the-evolution-of-us-empire.html

20 7amleh – The Arab Center for the Advancement of Social Media, Israel’s Surveillance Industry and Human Rights: Impact on Palestinians and Worldwide (December 2023), https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf.

21 Sophia Goodfriend, “Militarised AI,” London Review of Books (blog), January 28, 2025, https://www.lrb.co.uk/blog/2025/january/militarised-ai.

و»ويرز دادي» على مجموعات واسعة من بيانات المراقبة لإنتاج قوائم استهداف آلية، فيختصر ذلك الفاصل الزمني بين استخراج البيانات والفعل القاتل، ومن ثم يسرّع وتيرة الغارات الجوية ونطاقها. وكما تقول غودفريند، فإن ذلك يُتاح بفعل تزايد عدم التمييز بين شركات التكنولوجيا ووكالات الاستخبارات. فقد جرى تعبئة جنود احتياط من شركات كبرى، بما في ذلك غوغل ومايكروسوفت وأمازون، في العمليات العسكرية، في الوقت نفسه الذي سهّلوا فيه الوصول إلى البنى التحتية التي يساهمون في بنائها في القطاع الخاص. [22] وهكذا تُدمج منصات الحوسبة السحابية، ونماذج الذكاء الاصطناعي، وأنظمة تخزين البيانات واسعة النطاق مباشرة في سير العمل العسكري، حيث تعالج كميات هائلة من المعلومات لتوجيه قرارات الاستهداف. [23] ولا تتمثل النتيجة في مجرد تقارب بين المجالين المؤسسي والعسكري، بل في انهيار أكثر خطورة: أي تحويل جمع البيانات على نطاق واسع إلى مجال متّسع، لا ينتهي، ودائم الإنتاج للأهداف، بما يكثّف نطاق العنف وإيقاعه.

تنعكس الديناميات المبيّنة أعلاه في ممارسات شركات المراقبة نفسها، التي غالباً ما تعتمد عملياتها على بُنى تحتية غامضة وملتبسة قانونياً، لا ينكشف كثير منها إلا من خلال الصحافة الاستقصائية أو الطعون القانونية. وتعمل هذه الشركات ضمن نظام عابر للحدود آخذ في الاتساع، بما يجعل استخراج البيانات على نطاق واسع أكثر انتشاراً وأقل تقيداً بالحدود الإقليمية. وتجسّد شركات مثل مجموعة 9500، التي يقودها ضباط سابقون في الاستخبارات الإسرائيلية والممثَّلة في Cybersec Asia 2026 [24]، وهو منتدى إقليمي رئيسي للأمن السيبراني يجمع الحكومات وشركات التكنولوجيا والجهات الأمنية الفاعلة في منطقة آسيا والمحيط الهادئ، كيفية توسيع شركات المراقبة نطاق حضورها عبر الشبكات العابرة للحدود، وتتوافق مع أجندات جيوسياسية أوسع.

واستناداً إلى بيانات من Start-Up Nation Central، إلى جانب تحليل أطر التصدير التابعة لوزارة الدفاع، وقنوات الشراء، والإفصاحات المؤسسية، تحدد هذه الورقة مجموعة مركّزة من الفاعلين العاملين في المجالات المتقاطعة لتقنيات المراقبة والأمن. ولا تستند الورقة إلى مجموعة بيانات واحدة، بل تعتمد على مقارنة وتحديد مصادر متعددة لرسم خريطة لكيفية عمل هذه الكيانات ضمن بُنى اقتصادية وأمنية أوسع. وعلى الرغم من أن هؤلاء الفاعلين يوصفون غالباً بأنهم «شركات ناشئة»، فإن فهمهم على نحو أدق يكون بوصفهم شركات بالمعنى الاقتصادي. فالشركات التجارية الكبرى المسجلة تشير إلى كيان قانوني يمتلك أصولاً ويدخل في عقود، في حين تشير الشركة بالمعنى الاقتصادي إلى التنظيم الكامن للإنتاج، أي تنسيق رأس المال والعمل والتكنولوجيا عبر شبكة من العلاقات التعاقدية[25]. ويُعد هذا التمييز محورياً في التحليل. فمن خلال فحص الشكل القانوني، وهياكل التمويل، والتمثيل الذاتي، وكل ذلك عبر عدسة السياسة الصناعية، تتتبع الورقة البُنى التحتية التي تُفعَّل من خلالها تقنيات المراقبة عبر الحدود.

وتطرح الورقة ثلاث حجج رئيسية. أولاً، تجادل بأن شركات المراقبة مثل «توكا

22 Ibid.

23 Mahmoud Javadi, “Infrastructural Entanglement and Cloud Hyperscalers in Contemporary Warfare: Insights from Ukraine, Israel and Taiwan,” Contemporary Security Policy 47, no. 2 (2026): 469–506, https://doi.org/10.1080/13523260.2025.2593247

24 Cybersec Asia, “Speakers,” Cybersec Asia, accessed February 1, 2026, https://cybersec-asia.net/cybersec-asia-speakers/.

25 Jesús Alfaro Águila-Real, “Corporations Are Not Firms,” Oxford Business Law Blog, May 29, 2017, https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/05/corporations-are-not-firms

غروب» و«كورسايت إيه آي» يجب أن تُفهم بوصفها مكونات متكاملة في السياسة الصناعية الإسرائيلية. وتقليدياً، تشير السياسة الصناعية إلى التشكيل الاستراتيجي للقطاعات الاقتصادية من خلال دعم الدولة، بما في ذلك الاستثمار، والشراء، والتنظيم، وتسهيل التصدير. غير أن هذه السياسة، في الحالة الإسرائيلية، منظمة صراحةً حول الأمن والعسكرة.[26] فشركات مثل «توكا» و«كورسايت إيه آي» لا تقدّم نفسها كمزودين مستقلين للخدمات، بل كفاعلين متفرعين ضمن أنظمة بيئية تربط وكالات الدولة، ورأس المال الخاص، والمؤسسات الدولية. ويتيح لها هذا التموقع أن تعمل كوسطاء يترجمون أولويات الدولة إلى تقنيات قابلة للتسويق، مع توسيع نطاق هذه التقنيات عبر الحدود. ومن ثم، فإن فهم هؤلاء الفاعلين بوصفهم شركات بالمعنى الاقتصادي ينقل التركيز التحليلي بعيداً عن الدولة كوحدة مفردة، نحو البُنى التحتية التي تُنتَج من خلالها المراقبة وتُنشر عبر مجالات مثل الحرب، والشرطة، ومراقبة الحدود.[27]

ثانياً، تجادل الورقة بأن هذا التشكيل القائم على الشركات يسهّل توسّع المراقبة إلى ما وراء الحدود الإقليمية، وينتج أشكالاً من السيطرة لا تقتصر على الحدود المادية. وفي حين شددت الأدبيات القائمة على الكيفية التي تطمس بها الشراكات بين القطاعين العام والخاص التمييز بين البنى التحتية المدنية والعسكرية[28]، تقترح هذه الورقة أن السياسة الصناعية الإسرائيلية تعتمد في الوقت نفسه على الإبقاء على قدر من الفصل الخطابي، على مستوى السردية والتوصيف الذاتي. ويتيح هذا الفصل للشركات الوصول إلى أسواق جديدة، ولا سيما حيث تكون العلاقات السياسية أو الاقتصادية المباشرة مع إسرائيل مقيّدة. ومن خلال التداول العالمي لهذه الشركات، تتمدّد البنى التحتية للمراقبة إلى جغرافيات جديدة، بما يتيح أشكالاً من استخراج البيانات شبه غير محدودة. وبهذا المعنى، فإن توسّع تقنيات المراقبة يفضي أيضاً إلى توسّع في منطق الأمن الإسرائيلي، أي ما يمكن فهمه بوصفه «منطقة أمنية» ممتدة، وهي سردية وأداة رئيسية استخدمتها إسرائيل في السنوات الأخيرة، تتجاوز السياقات المحددة إقليمياً.[29] ومن خلال الوصول إلى بُنى البيانات التحتية العابرة للحدود، تسهم هذه الشركات في توسيع النطاق الذي يمكن ضمنه مراقبة السكان، بمن فيهم الفلسطينيون والمتضامنون معهم، واستهدافهم وإخضاعهم للحكم، تحت الخطاب السائد لـ«الأمن»[30].

ثالثاً، تجادل الورقة بأن مؤسسات التنمية والحوكمة متعددة الأطراف تعمل كواجهات محورية في هذه العملية. فعلى سبيل المثال، توضح حالة «توكا»، المدمجة في مبادرات الحوكمة الرقمية المدعومة من البنك الدولي، وحالة «كورسايت إيه آي»، التي تقيم شراكات مع أجهزة الشرطة في أنحاء أوروبا وآسيا، كيف يُعاد تأطير التقنيات المطوَّرة في سياقات الاحتلال العسكري بوصفها أدوات لـ«بناء القدرات»

26 Seher Bulut, “Israel’s Defense Industry Policy: Security-Centered Transformation, Unregulated Armament and Ethics of Accountability,” CENK 1, no. 2 (2025), https://doi.org/10.5281/zenodo.18082695.

27 Milan Babić, Jan Fichtner, and Eelke M. Heemskerk, “States versus Corporations: Rethinking the Power of Business in International Politics,” The International Spectator: Italian Journal of International Affairs 52, no. 4 (2017): 20–43, https://doi.org/10.1080/03932729.2017.1389151.

28 Joseph F. Getzoff, “Start-up Nationalism: The Rationalities of Neoliberal Zionism,” Politics & Political Theory 38, no. 5 (2020), published March 19, 2020.

29 Binoy Kampmark, “De Facto Occupation: Israel’s Security Zone Strategy,” Countercurrents, April 19, 2025, https://countercurrents.org/2025/04/de-facto-occupation-israels-security-zone-strategy

30 Elia Zureik, “Strategies of Surveillance: The Israeli Gaze,” Jerusalem Quarterly, no. 66 (June 2016): 12, https://doi.org/10.70190/jq.i66.p12

و»الحوكمة الرقمية».[31] ومع أن هذه الدينامية موثّقة في الأدبيات القائمة،[32] توسّع هذه الورقة التحليل من خلال إبراز نشوء أسواق جديدة تتشكل حول التداول العالمي لمنطق الأمن الإسرائيلي، وتوسيع نطاق وصوله العملياتي.

ومن خلال التركيز على «توكا غروب» و»كورسايت إيه آي»، لا تنشغل الورقة بمقارنة المنتجات أو الحصص السوقية، بل تفحص كيفية عمل هذه الشركات ضمن هذا التشكيل الأوسع. إذ تجسّد تشابك المجالات التقنية والعسكرية والسياسية الذي يميّز نظام المراقبة المعاصر، مع الحفاظ على مسافة خطابية استراتيجية عن فاعلي الدولة الإسرائيلية، ولكن ليس عن الأهداف الأوسع التي يسعى هؤلاء الفاعلون إلى تحقيقها.

وتنتظم الورقة في خمسة أجزاء. تبدأ بعرض الإطار النظري والمنهجي. ثم تضع «توكا» و»كورسايت إيه آي» ضمن النظام البيئي السيبراني الإسرائيلي القائم على الشراكة بين القطاعين العام والخاص. ويحلل القسم الثالث كيف تقدم هذه الشركات نفسها للحكومات والمستثمرين والجمهور العالمي، وكيف تعكس هذه السرديات السياسة الصناعية الإسرائيلية وتشكلها في آن واحد.

الإطار المفاهيمي

يبلور هذا القسم الإطار المفاهيمي الذي تُفهم من خلاله الحجج الثلاث المركزية للورقة. ولبناء هذا الإطار، يجمع القسم بين أدبيات دراسات المراقبة، والإمبريالية والاستعمار الرقمي/البياني، مع إسناد التحليل أيضاً في الأدبيات المتعلقة بالسياسة الصناعية، وبالشكل التنظيمي للشركة.

تُعرَّف المراقبة في هذه الورقة بوصفها ممارسةً للحَوكمة وقدرةً مسلَّعة في آن واحد[33] ، أي باعتبارها تجميعاً اجتماعياً–تقنياً [34] يضم معاً وكالات الدولة، والأنظمة القانونية، والبنى التحتية، ومجموعات البيانات، ومسارات العمل/العمالة، والتسويق المؤسسي[35] ويتسق هذا التأطير مع الأعمال التجريبية التي توثق كيف تعمل المراقبة في فلسطين عبر بُنى تحتية متراكبة للسيطرة على السكان،[36], كما يساعد الورقة على توظيف هذه الأعمال بصورة صريحة، وكذلك كيف ترتبط الأنظمة

31 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: PublicAffairs, 2019).

32 Gavin Sullivan, “Law, Technology, and Data-Driven Security: Infra-Legalities as Method Assemblage,” Journal of Law and Society (March 2022), https://doi.org/10.1111/jols.12352.

33 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: PublicAffairs, 2019).

34 Daniel Marciniak, “Infrastructure Shortcuts: The Private Cloud Infrastructure of Data-Driven Policing and Its Political Consequences,” in States of Surveillance: Ethnographies of New Technologies in Policing and Justice, ed. Maya Avis, Daniel Marciniak, and Maria Sapignoli (London: Routledge, 2025).

35 Daniel Marciniak, “Infrastructure Shortcuts: The Private Cloud Infrastructure of Data-Driven Policing and Its Political Consequences,” in States of Surveillance: Ethnographies of New Technologies in Policing and Justice, ed. Maya Avis, Daniel Marciniak, and Maria Sapignoli (London: Routledge, 2025).

36 (Nadera Shalhoub-Kevorkian, Security Theology, Surveillance and the Politics of Fear (Cambridge: Cambridge University Press, 2015

الخوارزمية/البيومترية بالضرورات السياسية للتوسع الاستيطاني. [37]

وفي هذا السياق، ولا سيما مع التوسع السريع في تقنيات المراقبة المدفوعة بالذكاء الاصطناعي والمشاريع الإمبريالية التوسعية،[38] عادت السياسة الصناعية إلى الظهور بوصفها ركيزة مركزية من ركائز الحوكمة الاقتصادية المعاصرة. فهي لم تعد تقتصر على الأهداف التنموية أو بهدف الحماية، بل باتت موجَّهة على نحو متزايد نحو ضرورات أمنية وأشكال عسكرية من استراتيجية الدولة. [39] وتبيّن الأدبيات الحديثة أن الحكومات تنشر تدخلات منسقة، تتراوح بين الدعم المالي والمشتريات العامة وضوابط التصدير وتمويل البحث والتطوير، داخل أنظمة إنتاج مدمجة عالمياً، حيث يكون النشاط على مستوى الشركات مدمجاً بعمق في سلاسل قيمة عابرة للحدود. [40] وفي هذا السياق، تعمل السياسة الصناعية، حتى في مجال التكنولوجيا وتحديداً الذكاء الاصطناعي، كآلية لتشكيل أنظمة بيئية كاملة للإنتاج والاستثمار والتكنولوجيا المتقدمة الموجَّهة نحو الحرب، في ظل التداخل المتزايد إلى حدّ عدم القدرة على التمييز بين السياسة الاقتصادية والأمن القومي. [41]

وتبني الورقة على هذه الأدبيات من خلال طرح مفهوم السياسة الصناعية ذات الطابع العسكري، بوصفها شكلاً من أشكال السياسة الصناعية تُنظَّم فيه عملية تطوير القطاعات الاقتصادية وبنيتها وتداولها العالمي صراحةً حول الضرورات العسكرية، ومنطق الأمن، والاستراتيجية الجيوسياسية. [42] وفي الحالة الإسرائيلية، لا يمثل ذلك تطوراً حديثاً، بل بنيةً متجذرة تاريخياً. فكما يجادل طارق دعنا، لا يُعد اقتصاد الحرب الإسرائيلي ظاهرة عارضة أو ظرفية، بل هو اقتصاد ممنهج، متجذر في بناء مؤسسات ذات طابع عسكري قبل قيام الدولة، ومُستدام من خلال تكامل وثيق بين البنى التحتية العسكرية والتكنولوجية والاقتصادية. [43] وبهذا المعنى، تصف السياسة الصناعية ذات الطابع العسكري حالة لا تقتصر فيها الأولويات العسكرية على التأثير في التنمية الاقتصادية، بل تقوم بتنظيمها بصورة فاعلة.

ويتطلب اعتماد عدسة السياسة الصناعية فهماً لكيفية تَشكُّل هذه الآلية ذات الطابع العسكري قانونياً ومالياً وخطابياً. [44] لذلك، تعتمد هذه الورقة تمييزاً مفاهيمياً

37 Sarah Fathallah, "Algorithmic Death-World: Artificial Intelligence and the Case of Palestine," Public Humanities 2 (2026): e7, https://doi.org/10.1017/pub.2025.10113.

38 Neema Iyer, Garnett Achieng, Favour Borokini, and Uri Ludger, Automated Imperialism, Expansionist Dreams: Exploring Digital Extractivism in Africa (Kampala: Pollicy, June 2021), https://pollicy.org/wp-content/uploads/2021/10/Automated-Imperialism-Expansionist-Dreams-Exploring-Digital-Extractivism-in-Africa_2-1.pdf

39 Jostein Hauge, "Industrial Policy Returns as a Weapon of National Security," The Global Currents, December 16, 2025, https://www.theglobalcurrents.com/p/industrial-policy-returns-as-a-weapon.

40 Jostein Hauge, Bruno Houtzager, and Alessandro Julian Hörmann, "The New Economic Nationalism: Industrial Policy and National Security in the United States, China, and the European Union," Geoforum 166 (November 2025): 104382, https://doi.org/10.1016/j.geoforum.2025.104382

41 AI Now Institute, AI Nationalism(s): Global Industrial Policy Approaches to AI, March 12, 2024, https://ainowinstitute.org/publications/research/ai-nationalisms-global-industrial-policy-approaches-to-ai

42 Ulises A. Mejias and Nick Couldry, Data Grab: The New Colonialism of Big Tech and How to Fight Back (Chicago: University of Chicago Press, 2024).

43 Tariq Dana, "Merchants of Death: Israel's Permanent War Economy," Security in Context, January 29, 2024, https://www.securityincontext.org/posts/merchants-of-death-israels-permanent-war-economy.

44 Susannah Glickman, "AI and Tech Industrial Policy: From Post-Cold War Post-Industrialism to Post-Neoliberal Re-Industrialization," AI Now Institute, March 12, 2024, https://ainowinstitute.org/publications/ai-and-tech-industrial-policy-from-post-cold-war-post-industrialism-to-post-neoliberal-re-industrialization

دقيقاً بين «firm» و«company» والفئات القانونية ذات الصلة.[45] فبموجب القانون الإسرائيلي، تُعد «الشركة» Company صيغة قانونية محددة تُسجَّل بموجب قانون الشركات، في حين يعمل مصطلح «شركة كبرى» «corporation» على نحو أوسع كمصطلح جامع يقابل المفهوم القانوني لـ«الشخصية الاعتبارية»، أي شخص قانوني قادر على حيازة الحقوق وتحمل الالتزامات.[46] أما «الشركة الناشئة» Startup فليست فئة قانونية، بل وصف لمرحلة في دورة حياة الشركة يُستخدم في أطر الاستثمار والسياسات العامة. والأهم أن «firm» ليست بحد ذاتها كياناً قانونياً، بل تنظيماً اقتصادياً يقوم على تشكيلة من العقود، وعوامل الإنتاج، وعلاقات الحوكمة التي تنسق رأس المال والعمل والتكنولوجيا.

ويكتسب هذا التمييز أهمية تحليلية حاسمة. فوفقاً لمسجّل الشركات، تُسجَّل كيانات مثل «Corsight AI Ltd» التي تأسست عام 2019 و«Cortica Ltd» تي تأسست عام 2007 رسمياً كشركات خاصة، إلا أنها تعمل كشركات تابعة ضمن شركات/تشكيلات اقتصادية أكبر مدمجة في شبكات معقدة من الاستثمار، وحوكمة الأمن، والتعاقد العابر للحدود، بما في ذلك الاتفاقيات العسكرية. ولا يكفي الشكل القانوني وحده لفهم بنيتها[47] ، التي غالباً ما تنطوي على تشكيلات جماعية، وشركات تابعة، وروابط على مستوى مجالس الإدارة مع مستثمرين وشخصيات سابقة من المؤسسة العسكرية أو الاستخباراتية. وبدلاً من ذلك، يتيح مفهوم «firm» إظهار كيفية عمل هؤلاء الفاعلين كعُقد تشغيلية ضمن اقتصاد أوسع ذي طابع عسكري.

ويزداد ذلك وضوحاً عند النظر إلى البيئة التنظيمية التي تعمل ضمنها هذه الشركات. ففي إسرائيل، تخضع الصادرات الدفاعية لتنظيم وكالة مراقبة الصادرات الدفاعية (DECA) بموجب قانون مراقبة الصادرات الدفاعية لعام 2007، الذي يشترط الحصول على تراخيص لتسويق التقنيات ذات الصلة بالدفاع وتصديرها، ويتماشى مع أنظمة دولية مثل ترتيب فاسنار ونظام مراقبة تكنولوجيا القذائف. وإلى جانب ذلك، تشرف وزارة الاقتصاد على صادرات الاستخدام المزدوج، في حين تخضع الصادرات السيبرانية لمتطلبات متزايدة الصرامة تتعلق بالمستخدم النهائي.[48]

وتُظهر التطورات العالمية الأخيرة في ضوابط التجارة، بما فيها التحديثات التي أُدخلت في أواخر عام 2025، أن ضوابط التصدير هذه لم تعد مقتصرة على التنظيم الوطني، بل أصبحت جزءاً من نظام أوسع للحوكمة الاقتصادية الدولية. فباتت الشركات مُطالبةً الالتزام بمعايير امتثال أكثر صرامة عبر الحدود، بما في ذلك فحوصات أكثر تدقيقاً للمستخدم النهائي، وعمليات العناية الواجبة، والتنسيق مع الأطر التنظيمية للدول الحليفة. ويمدّ ذلك نطاق المسؤولية ليشمل سلسلة التوريد بأكملها، بما يعني أن على الشركات أن تأخذ في الاعتبار ليس فقط الجهة التي تبيع لها مباشرة،

45 Jesús Alfaro Águila-Real, “Corporations Are Not Firms,” Oxford Business Law Blog, May 29, 2017, https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/05/corporations-are-not-firms.

46 Israel Business Connection, “Company Registration,” Israel Business, accessed March 1, 2026, http://www.israelbusiness.org.il/startingyourbusiness/companyregistration.

47 William Hamilton Byrne, Thomas Gammeltoft-Hansen, and Nora Stappert, “Legal Infrastructures: Towards a Conceptual Framework,” German Law Journal 25, no. 8 (2024): 1229–46, https://doi.org/10.1017/glj.2024.78

48 State Comptroller and Ombudsman of Israel, State Comptroller Report 76B (December 2025), https://library.mevaker.gov.il/sites/DigitalLibrary/Documents/2025/2025-12/EN/2025.12-76B-203-EN.pdf

بل أيضاً كيفية استخدام التقنيات ونقلها وتداولها بعد المعاملة الأولية. [49]

وفي هذا المشهد التنظيمي المتزايد التعقيد، يكتسب شكل الشركة بالمعنى الاقتصادي أهمية خاصة. فهؤلاء الفاعلون لا تنحصر أعمالهم في بنية مؤسسية أو إقليمية واحدة؛ بل يعملون من خلال ترتيبات تعاقدية متعددة الطبقات، مثل الشركات التابعة، والشراكات، واتفاقيات الترخيص، والمشاريع المشتركة، ونماذج تقديم الخدمات، وهي ترتيبات يمكن إعادة تشكيلها بحسب البيئات التنظيمية. ويتيح ذلك توجيه التقنيات والخبرات والبيانات عبر قنوات قانونية وجغرافية متعددة، حتى في ظل وجود ضوابط على التصدير. وبدلاً من أن تعمل هذه الشركات ككيانات متكاملة رأسياً، فإنها توزّع عملياتها؛ فقد تُطوَّر المكوّنات الحساسة في كيان، وتُحتفظ بها في كيان آخر، وتُنشر عبر شراكات مع أطراف ثالثة. وما يتشكل هنا هو البنية التحتية المادية لسياسة صناعية ذات طابع عسكري، أي نظام تُنشَر فيه أولويات الدولة الأمنية عبر شركات تقوم بتشغيلها وتوسيعها وعولمتها. وفي هذا التشكيل، يصبح شكل الشركة بالمعنى الاقتصادي الآلية التي تُجعل من خلالها الحرب والمراقبة قابلتين للتوسّع وعابرتين للحدود، بما يحوّل ما قد يبدو نشاطاً تجارياً مجزأً إلى بنية تحتية متماسكة للسيطرة. [50]

وتميل الشركات العاملة في قطاعات السيبرانية والدفاع أو القطاعات المتاخمة للدفاع إلى التسجيل كشركات إسرائيلية خاصة محدودة المسؤولية بهدف التوافق مع متطلبات الترخيص، وغالباً ما تُقسّم التقنيات الخاضعة للرقابة إلى شركات تابعة، أي إلى شركات بالمعنى الاقتصادي، من أجل إدارة التعرض التنظيمي، وتصمّم هياكل حوكمة للتخفيف من المخاطر المرتبطة بالإفصاح عن التقنيات الحساسة. [51] ومن ثم، تعمل السياسة الصناعية ذات الطابع العسكري من خلال شكل الشركة ذاته؛ إذ تصبح الشركات أدوات مؤسسية تُطوَّر من خلالها التقنيات العسكرية، وتُختبر، وتُرخَّص، وتُصدَّر. ولذلك، فإن الشركات، وفق التعريفين الخطابي والقانوني معاً، تعمل في الوقت نفسه كفاعلين اقتصاديين، ووسطاء أمنيين، وأدوات للاستراتيجية الجيوسياسية.

المنهجية

تتطلب دراسة الشركات السيبرانية الهجومية العمل عبر تعتيم منظّم. فهؤلاء الفاعلون يعملون عبر أنظمة مراقبة الصادرات، والشراكات المصنفة، واتفاقيات عدم الإفصاح، ولغة مؤسسية منقّحة عمداً تُخفي كلاً من القدرات وحالات الاستخدام. ويظل الوصول المباشر إلى المعلومات محدوداً، إذ إن العقود الرئيسية غير مفصح عنها، والمواصفات التقنية جزئية، وترتيبات الحوكمة غالباً ما تكون مجزأة عبر ولايات قضائية متعددة. ونتيجة لذلك، لا يمكن للتحليل أن يعتمد على مصدر واحد، بل عليه أن يعيد بناء هذه الأنظمة من خلال آثار متناثرة وغير مكتملة.

49 Shibolet & Co., “Developments in Global Trade Controls: October–December 2025,” Shibolet & Co., January 20, 2026, https://www.shibolet.com/en/developments-in-global-trade-controls-october-december-2025/.

50 Laleh Khalili, “How Empire Operates: An Interview with Laleh Khalili,” Viewpoint Magazine, February 1, 2018, https://viewpointmag.com/2018/02/01/empire-operates-interview-laleh-khalili/.

51 Haim Ravia and Dotan Hammer, “Israel Publishes Draft Bill on National Cyber Protection,” Pearl Cohen, January 28, 2026, https://www.pearlcohen.com/israel-publishes-draft-bill-on-national-cyber-protection/

ولمعالجة هذه القيود، يعتمد هذا البحث مقاربة منهجية متعددة المصادر، تتعامل مع التعتيم ذاته بوصفه شرطاً تحليلياً. ويثبّت البحث نتائجه عبر المقارنة بين المواد المؤسسية، والتقارير الإعلامية، والأطر التنظيمية، والمعرفة المنتَجة من الحركات، لرسم خريطة لكيفية عمل هذه الشركات وكيفية تمثيلها لذاتها. ويشمل ذلك فحص السِيَر الذاتية للمؤسسين، وشبكات رأس المال المغامر، والإيداعات المؤسسية، حيثما توفرت، وتراخيص التصدير، والشراكات بين القطاعين العام والخاص؛ كما يحلل التغطية الإعلامية عبر مصادر عربية وإنجليزية وعبرية؛ ومراجعة حوكمة الصادرات الإسرائيلية من خلال مواد صادرة عن «سيبات» وهيئات الدولة ذات الصلة. كما يستند البحث إلى مخرجات موجَّهة إلى الشركات، مثل عروض المستثمرين، ومقاطع الفيديو الترويجية، والعروض المقدَّمة في معارض الأمن، لفهم الكيفية التي تبني بها هذه الشركات سردياتها العامة، إلى جانب التحليلات النقدية التي ينتجها باحثون ومنظمات معنية بالحقوق الرقمية.

منهجياً، يجمع البحث بين التحليل الموضوعاتي وتحليل الخطاب لفحص الكيفية التي تعرض بها شركات مثل «توكا» و«كورسايت» تقنياتها عبر هذه المواد. ويحدّد التحليل الموضوعاتي المصطلحات المتكررة، في حين يضع تحليل الخطاب هذه المصطلحات ضمن أطر أوسع تُخفي أصول التقنيات ووظائفها. وتنقل هذه المقاربة التركيز بعيداً عن أوصاف المنتجات، نحو المنطق السياسي والاقتصادي الذي يشكّل كيفية عمل هذه الأنظمة في سياقات حوكمة مختلفة.

غير أن هذه المنهجية، بدلاً من أن تحاول تجاوز التعتيم، تعمل من خلالها. فالطبيعة الجزئية والوسيطة للبيانات المتاحة لا تُعامل بوصفها قيداً فحسب، بل بوصفها مؤشراً إلى الكيفية التي تعمل بها هذه الشركات.

لماذا توكا وكورسايت؟

يركّز هذا البحث على «توكا غروب» و«كورسايت إيه آي» لأنهما حالتان كاشفتان من الناحية التحليلية. فـ توكا غروب هي شركة استخبارات سيبرانية تزوّد الحكومات بقدرات للوصول إلى البيانات واستخراجها من الأجهزة المتصلة، بحيث يصبح «الوصول» بحد ذاته كأداة من أدوات الحوكمة. أما كورسايت إيه آي، وهي شركة تابعة لـكورتيكا، فتطوّر أنظمة متقدمة للتعرف على الوجوه مصممة للتحديد، والتتبع، والمراقبة الفورية في سياقات الأمن والشرطة. وتوفر هاتان الشركتان نقطتي دخول ملموستين يمكن من خلالهما تتبع العمليات الأوسع لاقتصاد المراقبة. ولذلك فإن اختيارهما منهجي، إذ تتيحان للورقة فحص الكيفية التي تعمل بها السياسة الصناعية ذات الطابع العسكري عملياً، مع إبقاء الانتباه إلى كونهما لا تمثلان سوى جزء من نظام بيئي أوسع يشمل مؤسسات الدولة، والفاعلين الماليين، والبنى التحتية العسكرية، والأسواق العالمية.

كلتا الشركتين فاعلتان من القطاع الخاص تعملان داخل الدولة وتتجاوزانها في الوقت نفسه. فهما مسجّلتان رسمياً كشركتين خاصتين، لكنهما تعملان كشركات بالمعنى الاقتصادي مدمجتين في شبكات عابرة للحدود من الاستثمار، والتنظيم، وحوكمة الأمن. وهما تحوزان تراخيص تصدير، وتشاركان في منتديات أمنية دولية، وتضعان نفسيهما كشريكين في مجالات مثل الحوكمة الرقمية، وإنفاذ القانون، والأدلة الجنائية، ومراقبة الحدود. ويُعد هذا التموقع محورياً لدورهما ضمن السياسة الصناعية ذات الطابع العسكري، حيث تعملان كوسطاء يترجمون أولويات

الدولة الأمنية إلى تقنيات قابلة للتوسّع والتسويق. ويسمح لهما شكلهما التنظيمي كشركات بالمعنى الاقتصادي بالتحرك عبر ولايات قضائية متعددة، إذ تستندان إلى وجود في عدة دول، بما في ذلك الولايات المتحدة. ويتيح لهما ذلك الاندماج في بيئات مؤسسية متنوعة، والوصول إلى أسواق قد تكون مقيّدة سياسياً في ظروف أخرى.

ومن ثم، فإن نمو شركات مثل توكا وكورسايت يُتاح بفعل التوافق بين أولويات الدولة، ورأس المال الاستثماري، والأطر التنظيمية، بما في ذلك ضوابط التصدير وأنظمة الشراء التي تسهّل دمجهما في الأسواق الدولية.

وفي الوقت نفسه، تكشف هاتان الشركتان كيف تعمل المراقبة بوصفها حوكمة وبنية تحتية في آن واحد. فتنشأ تقنياتهما ضمن سياق إدارة السكان الفلسطينيين والسيطرة عليهم، لكنها تُصمَّم منذ البداية لتكون قابلة للتوسّع والنقل. وما يُطوَّر كآلية للسيطرة يُعاد تشكيله في نموذج معمّم للحوكمة. وبهذا المعنى، توسّع شركات مثل توكا وكورسايت منطق المراقبة إلى سياقات جديدة، بما في ذلك، على سبيل المثال لا الحصر، المملكة المتحدة وكينيا، إلى جانب دول أخرى. ولذلك، فإن التركيز على هاتين الشركتين يتيح للورقة تتبع الكيفية التي تُفعَّل بها السياسة الصناعية ذات الطابع العسكري من خلال شكل الشركة بالمعنى الاقتصادي، مبيّناً كيف تُتداول المراقبة بعد ذلك كسلعة عالمية.

توكا

«توكا» شركة إسرائيلية خاصة «تربط بصورة علنية عوالم الهجوم السيبراني، والاستخبارات النشطة، والمراقبة الذكية». ومنذ تأسيسها عام 2018، جرى تَمَوضُعها كمصدّر أمني قريب من الدولة. وتُدرج توكا رسمياً لدى «سيبات»،[52] وهي مديرية التعاون الدفاعي الدولي التابعة لوزارة الدفاع الإسرائيلية، كمصدّر دفاعي رسمي ضمن فئتي «الدفاع السيبراني» و«الاستخبارات السيبرانية»، وذلك بحسب ما تأكد في عام 2025. وبعبارة أخرى، فإن الدولة الإسرائيلية نفسها تعترف بمنتجات توكا بوصفها جزءاً من محفظة صادراتها الدفاعية.

ومنذ البداية، قدّمت توكا نفسها «كمتجر اختراق متكامل يعمل لصالح الحكومات»[53]، بوصفها شركة تصمّم «الصمود السيبراني» الوطنية ثم تزوّد الأدوات اللازمة لاختراق البنى التحتية ذاتها التي تساعد في بنائها ومراقبتها والتلاعب بها. وهي تقع عند تقاطع ثلاثة اقتصادات: المجمع العسكري–الاستخباراتي الإسرائيلي، ورأس المال المغامر الأمريكي، وتمويل التنمية متعدد الأطراف، بما في ذلك البنك الدولي، وبنك التنمية للبلدان الأمريكية، ووكالات الأمم المتحدة. وتعمل هذه الاقتصادات مجتمعةً على تحويل القدرات السيبرانية الهجومية إلى مشاريع «بناء قدرات» قابلة للتصدير في الجنوب العالمي وبين الدول الحليفة للولايات المتحدة.[54]

52 Thomas Brewster, “Alexa, Are You a Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT,” Forbes, July 15, 2018, https://www./forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies

53 Thomas Brewster, “Alexa, Are You a Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT,” Forbes, July 15, 2018, https://www./forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies

54 Charles Rollet, “a16z-Backed Toka Wants to Help US Agencies Hack into Security Cameras and Other IoT Devices,” Yahoo Finance (originally published in TechCrunch), December 6, 2024, https://au.finance.yahoo.com/news/a16z-backed-toka-wants-help-183623502.html

1. النشأة، والملكية، والموقع

يجسّد فريق تأسيس توكا مسار الانتقال بين المؤسسات العسكرية والاستخباراتية الإسرائيلية وصناعة السيبرانية في القطاع الخاص. [55] فقد شارك في تأسيس الشركة عام 2018 كل من رئيس الوزراء السابق ورئيس الأركان السابق للجيش الإسرائيلي إيهود باراك، والعميد احتياط يارون روزن، الرئيس السابق لهيئة السيبرانية في الجيش الإسرائيلي. [56] وترسّخ المسيرة الطويلة لباراك على رأس الجهاز الأمني الإسرائيلي، بما في ذلك إشرافه على الموساد والاستخبارات العسكرية بصفته وزيراً للدفاع، موقع توكا بقوة في مدار العمليات السرية للدولة. أما روزن، فيجلب خبرة مباشرة في تصميم ونشر القدرات السيبرانية الهجومية والدفاعية لصالح الجيش الإسرائيلي. [57]

وينضم إليهما المؤسسان المشاركان ألون كانتور وكفير والدمن، اللذان يمثلان الجانب «المدني» من النظام البيئي الإسرائيلي لتكنولوجيا الأمن، من خلال مسيرات مهنية بُنيت في شركات مثل «تشيك بوينت» و:سيسكو»، وهي شركات متجذرة بدورها في شبكات الوحدة 8200. [58] ويشغل والدمن حالياً منصب الرئيس التنفيذي. أما المهندس الرئيسي لحزمة الاختراق التابعة لتوكا، موتي زالتسمان، فقد جاء من وحدة التكنولوجيا في مكتب نتنياهو، وعمل على تقنيات استخبارات هجومية؛ وكان مرتبطاً عن قرب بمشاريع تكنولوجية هجومية في عهد نتنياهو قبل أن تُنقَّح سيرته الذاتية بهدوء بعد تغطية نقدية. [59] ويشغل شخصية بارزة أخرى، هي نير بيليغ، منصب نائب الرئيس للمشاريع الاستراتيجية، وكان قد ترأس سابقاً البحث والتطوير في وحدة التكنولوجيا النخبوية [60]التابعة للمديرية الوطنية للسيبرانية، وعمل عن كثب مع تال غولدشتاين (وهو أحد المهندسين الرئيسيين لاستراتيجية إسرائيل السيبرانية في المحافل العالمية مثل المنتدى الاقتصادي العالمي). [61]

وتعمّق قيادة توكا المؤسسية ومجلس إدارتها هذه الروابط. ففي حين تراجع باراك عن دور نشط في الفترة ما بين 2020 و2024 تقريباً، ظل شخصية مركزية أولية ورمزاً للتموضع الاستراتيجي للشركة. ويضم مجلس الإدارة روزن نفسه والمستثمر التكنولوجي ليئور سوزان، وهو ضابط سابق في القوات الخاصة الإسرائيلية تحوّل إلى رأسمالي استثماري. [62] وتسلّط تقارير حديثة لـ «فوربس» مزيداً من الضوء

55 Toka, “Company Leadership,” Toka Group (archived December 19, 2021), https://web.archive.org/web/20211219162602/https://www.tokagroup.com/company#leadership (for former governance structure).

56 Yasmin Yablonko, “Ehud Barak-Founded Cybersecurity Co Toka Raises $12.5m,” Globes, July 16, 2018, https://en.globes.co.il/en/article-ehud-barak-founded-cybersecurity-co-toka-raises-125m-1001246322

57 Yonah Jeremy Bob, “Ex-IDF Cyber Intel Official: How to Carry Out a Cyber Offense Attack,” The Jerusalem Post, September 14, 2021, https://www.jpost.com/israel-news/ex-idf-cyber-intel-official-how-to-carry-out-a-cyber-offense-attack-677173

58 Corporate Watch, “Check Point Software: Ex-Israeli Military Spooks Profiting from the Cyber Security Industry,” Corporate Watch, November 25, 2019, https://corporatewatch.org/check-point-software-ex-israeli-military-spooks-profiting-from-the-cyber-security-industry/.

59 Jennifer L. Schenker, “Interview of the Week: Tal Goldstein, World Economic Forum Centre for Cybersecurity,” The Innovator, https://theinnovator.news/interview-of-the-week-tal-goldstein-world-economic-forum-centre-for-cybersecurity/.

60 Toka’s ‘About US’ page.

61 Jennifer L. Schenker, “Interview of the Week: Tal Goldstein, World Economic Forum Centre for Cybersecurity,” The Innovator, https://theinnovator.news/interview-of-the-week-tal-goldstein-world-economic-forum-centre-for-cybersecurity/.

62 Samantha Huang, “He Went From Working on a Banana Farm to Selling His First Company to Cisco in the Span of a Decade: Meet Lior Susan, Founding Partner of Eclipse Ventures,” EVCA, March 1, 2021, https://evca.org/content/he-went-from-working-on-a-banana-farm-to-selling-his-first-company-to-cisco-in-the-span-of-a-decade-meet-lior-susan-founding-partner-of-eclipse-ventures.

على اهتمام باراك المستمر بتعبئة رأس المال لصالح توكا إلى جانب محفظته الأوسع من المشاريع. وقبيل الإطلاق العلني للشركة عام 2018، سعى باراك بنشاط لجذب الاستثمار والدعم الاستراتيجي لـ«توكا»، بما في ذلك التواصل مع أفراد ذوي ثروات كبيرة ولديهم صلات حكومية، مقدّماً الشركة صراحةً على أنها «مبنية للحكومات كعملاء». وعلى الرغم من أن هذه الجهود لم تترجم بالضرورة إلى استثمارات مباشرة، فإنها تؤكد كيف جرى تموضع توكا منذ البداية كمؤسسة موجَّهة نحو الدولة، تحتاج إلى رأس المال والوصول السياسي معاً لكي تتوسع. [63]

وترسم قاعدة المستثمرين خريطة مباشرة للتحالفات التكنولوجية والأمنية الأمريكية–الإسرائيلية. وتُعد «Andreessen Horowitz» المعروفة اختصاراً بـ(a16z) من أبرز الداعمين؛[64] ويشغل مؤسسها المشارك مارك أندريسن عضوية مجلس إدارة «ميتا»، وقد ورد اسمه كمدعى عليه في دعاوى خصوصية تتعلق بعدم امتثال ميتا لأوامر تنظيمية أمريكية، بما يبرز كيف تتشابك توكا مع شركات متهمة أصلاً بانتهاكات واسعة النطاق للبيانات. [65] أما Entrée Capital، المذكورة في قسم «المستثمرين» لدى توكا، فيقودها أفياد إيال وران أخيتوف، وتضيف بُعداً آخر من السلالة الاستخباراتية للإشارات، إذ عمل أخيتوف سابقاً في استخبارات الإشارات المعتمدة على الأقمار الصناعية، وشغل مناصب عليا في «أمدوكس» و«كومفرس»، وهما شركتان ارتبطتا بجدالات تجسسية سابقة استهدفت الاتصالات الأمريكية. [66]

وتشير تقارير سابقة لصحيفة «هآرتس» إلى أن عقود توكا لم تكن مدفوعة بالسوق وحده، بل جرى التخطيط لها ودعمها من خلال لجنة مشتركة بين الوزارات أُنشئت في عهد نتنياهو بهدف «تحقيق إمكانات التنمية الدولية» لصالح شركات السيبرانية الإسرائيلية. وعملياً، يعني ذلك أن توكا تُستخدم كأداة من أدوات السياسة الصناعية والخارجية الإسرائيلية. فإدراجها ضمن «سيبات»، وتوظيفها لقدامى الجيش الإسرائيلي والاستخبارات، وتنسيقها مع وزارة الدفاع، كلها أمور تضع توكا كامتداد مخصخص للجهاز السيبراني الهجومي الإسرائيلي، لا كـ «استشارة سيبرانية» محايدة. [67]

وفي أواخر عام 2025، في ظل قيادة الرئيس التنفيذي غريغ سميث، نقلت الشركة مقرها الرئيسي إلى الولايات المتحدة، مع الإبقاء على شركة تابعة في إسرائيل. ويعكس ذلك مرونة شكل الشركة بالمعنى الاقتصادي، إذ تستطيع توكا إعادة تنظيم نفسها عبر الولايات القضائية بما يتماشى مع البيئات الأمنية والتنظيمية والسياسية الرئيسية. [68]

63 Thomas Brewster, “Epstein Could Have Made $100 Million On A Secret Police Tech Investment,” Forbes, February 10, 2026, https://www.forbes.com/sites/thomasbrewster/2026/02/10/epstein-police-surveillance-investments-with-ehud-barak/

64 Andreessen Horowitz, “Investment List,” a16z, accessed April 1, 2026, https://a16z.com/investment-list/

65 Henry Chandonnet, “Marc Andreessen Says Being Controversial Gives His VC Firm an ‘Incredible Competitive Advantage,’” Business Insider, January 12, 2026, https://www.businessinsider.com/marc-andreessen-controversial-competitive-advantage-venture-capital-2026-1

66 James Bamford, “Shady Companies With Ties to Israel Wiretap the U.S. for the NSA,” Wired, April 3, 2012., https://www.wired.com/2012/04/shady-companies-nsa/

67 Omer Benjakob, “This ‘Dystopian’ Cyber Firm Could Have Saved Mossad Assassins From Exposure,” Haaretz, December 26, 2022, https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000.

68 Toka, “Toka Deepens Engagement with U.S. and Allied Government Partners, Names Gregg Smith CEO,” February 26, 2026, https://tokagroup.com/news/toka-deepens-engagement-with-u-s-and-allied-government-partners-names-gregg-smith-ceo

2. من «الاستخبارات القانونية» إلى عسكرة إنترنت الأشياء

تُبنى السردية العامة لتوكا بعناية. فالشركة تزعم أنها «تزوّد أجهزة إنفاذ القانون، والأمن الداخلي، والدفاع، والاستخبارات ببرمجيات ومنصة تساعد على تسريع تحقيقاتها وعملياتها وتبسيطها»[69] ، بحيث تتمكن من «الوصول بصورة قانونية وسريعة وسهلة، إلى المعلومات التي تحتاجها للحفاظ على أمن الناس والأماكن والمجتمعات.» وتركّز موادها التسويقية على مفاهيم مثل «الاختراق الأخلاقي»، و»الاعتراض القانوني»، و»الأدلة الجنائية»، و»حماية البنية التحتية الحيوية»، و»الاستراتيجيات السيبرانية الشاملة»[70]. وتقدّم نفسها كشريك يساعد الحكومات على بناء دفاع سيبراني متكامل، وتأمين المدن الذكية، وتعزيز الصمود الوطني.

ويصف عرضٌ تعريفي للشركة حصل عليه صحفيون من هآرتس شركة «توكا» بأنها تقدم «قدرات كانت سابقاً خارج نطاق الوصول»، من شأنها أن «تحوّل مستشعرات إنترنت الأشياء غير المستغلة إلى مصادر استخباراتية» لتلبية «الاحتياجات الاستخباراتية والعملياتية»[71]. وبلغة الشركة نفسها على موقعها الإلكتروني، تُمكّن توكا عملاءها من:

- اكتشاف كاميرات الأمن والكاميرات الذكية والوصول إليها في «منطقة مستهدفة».
- بث الكاميرات والتحكم بها داخل تلك المنطقة على مدى فترة زمنية.
- استهداف المركبات عبر أنظمة الوسائط المتصلة في السيارات، بما يوفّر «أدلة جنائية واستخبارات خاصة بالسيارات»، بما في ذلك تحديد الموقع الجغرافي للمركبات وحركتها.
- جمع استخبارات بصرية من مقاطع فيديو «مباشرة أو مسجلة».
- تعديل البثين الصوتي والمرئي من أجل «إخفاء الأنشطة في الموقع» أثناء «العمليات السرية».

وتُسوَّق أنظمة توكا بوصفها الأداة التي يمكن لقوة شرطة استخدامها لتتبع «هجوم إرهابي» عن بُعد عبر مدينة ما، من خلال السيطرة على شبكات الكاميرات الحضرية. والبنية التحتية نفسها، بحكم تصميمها، تتيح جمع البيانات البصرية والتلاعب بها بصورة سرية «دون ترك أثر».

وتتمثل الوظيفة الأشد إثارة للقلق في تسويق توكا في القدرة على تعديل أو تزييف أو حذف تسجيلات الفيديو، وكذلك التسجيلات الصوتية، دون ترك أثر جنائي رقمي. ويتيح ذلك للمشغّلين ليس فقط مراقبة مشهد ما، بل محو وجودهم بأثر رجعي، أو فبركة الأدلة، أو حجب عنف الدولة. ويزعزع ذلك فعلياً مفهوم الدليل البصري؛ فإذا أمكن تعديل أي تسجيل من كاميرات المراقبة بصمت، فلن تعود المحاكم ولا الجمهور قادرين على الثقة بما يرونه.

69 'Toka's 'About US page

70 Ibid.

71 Omer Benjakob, "This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure," Haaretz, December 26, 2022, https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000.

تقنياً، يستفيد نموذج توكا الهجومي من أسطح هجوم لاسلكية شائعة. فكثير من أجهزة كاميرات المراقبة وإنترنت الأشياء تعتمد على شرائح مشتركة، مثل (البلوتوث والواي فاي)، يتم الحصول عليها من مصنّعين خارجيين؛ ويمكن تكرار استغلال ثغرة تُكتشف في شريحة واحدة عبر علامات تجارية متعددة. [72] ويعني اهتمام توكا باستهداف الأجهزة عبر الواجهات اللاسلكية أنها تستطيع تنفيذ هجمات تكتيكية موضعية عندما يكون المشغّل قريباً مادياً من الشبكة المستهدفة، أو تنفيذ هجمات عن بُعد عبر الإنترنت إذا كانت البنية التحتية مكشوفة. [73]

وخلافاً لـ«بيغاسوس»، الذي يركز على الهواتف، تتجه توكا نحو اختراق البيئة بأكملها. وتؤكد تقارير صادرة عن «تك كرانش»، من بين جهات أخرى، أن توكا لا تفصح عن الثغرات التي تكتشفها للمورّدين، بل تحتفظ بثغرات «اليوم الصفري» باعتبارها أصولاً استراتيجية. وهذا النموذج التجاري يُبقي المستخدمين حول العالم في حالة انكشاف أمني متعمّد، من أجل الحفاظ على قدرة عملاء الدولة على اختراق أجهزتهم. [74]

وتصرّ تصريحات توكا نفسها على أنها لا تخدم إلا الحكومات «الموثوقة»، أي تلك التي تتمتع بسجلات جيدة في «سيادة القانون» والحريات المدنية، وذلك من خلال «عملية مراجعة واعتماد سنوية صارمة» تسترشد بمؤشرات الفساد والحريات المدنية، وتدعمها جهات استشارية خارجية، (من بينها شخصيات قانونية واقتصادية بارزة مثل بيتر شَك [75] ويعقوب فرنكل[76]). وهذه هي صيغة «التنظيم الذاتي» المألوفة التي استخدمتها مجموعة «إن إس أو» في سياق بيغاسوس: وعدٌ بأن برمجيات التجسس القوية لن تُستخدم إلا لأغراض أمنية «مشروعة»[77]. وكما يرد في موقع الشركة وبياناتها الصحفية السابقة، لا يوجد في شيفرة توكا، أو هيكل حوكمتها، أو إطار ترخيصها، ما يقيّد على نحو ذي معنى كيفية استخدام أدواتها عملياً. وفي غياب ضمانات قابلة للإنفاذ، يمكن لتقنياتها أن تُستخدم بالسهولة ذاتها ضد أي شخص.

ومجتمعةً، تكشف ادعاءات توكا وقدراتها عن نمط واضح. فالسردية العامة تتمحور حول الاستخبارات القانونية، ومكافحة الجريمة، وحماية البنية التحتية الحيوية. أما الواقع التقني فهو مجموعة من الأدوات التي تتيح للدول السيطرة بصمت على الآثار البصرية والرقمية للحياة اليومية والتلاعب بها ومحوها. وأفضل فهم لهذه الشركة هو بوصفها مصنّعاً لقوة قابلة للإنكار؛ فهي تمنح الدول القدرة على رؤية المزيد والتدخل دون أن تكون «مرئية».[78]

72 Keumars Afifi-Sabet, “Critical Supply Chain Flaw Exposes IoT Cameras to Cyber Attack,” IT Pro, June 16, 2021, https://www.itpro.com/security/vulnerability/359899/critical-supply-chain-flaw-exposes-iot-cameras-to-cyber-attack.

73 Globes Correspondent, “Israeli Cybersecurity Co Toka Raises $25m,” Globes, October 28, 2020, https://en.globes.co.il/en/article-israeli-cybersecurity-co-toka-raises-25m-1001347405.

74 Charles Rollet, “a16z-backed Toka Wants to Help U.S. Agencies Hack into Security Cameras and Other IoT Devices,” TechCrunch, December 6, 2024, https://techcrunch.com/2024/12/06/a16z-backed-toka-wants-to-help-us-agencies-hack-into-security-cameras-and-other-iot-devices/.

75 “Peter H. Schuck,” The Org, accessed April 1, 2026, https://theorg.com/org/toka/org-chart/peter-h-schuck.

76 “Yaakov Frenkel,” The Org, accessed April 1, 2026, https://theorg.com/org/toka/org-chart/yaakov-frenkel.

77 John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, “Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware,” Citizen Lab, June 19, 2017, https://citizenlab.ca/research/reckless-exploit-mexico-nso/.

78 Cormac, Rory, and Richard J. Aldrich. 2018. “Grey Is the New Black: Covert Action and Implausible Deniability.” International Affairs 94 (3): 477–494. https://doi.org/10.1093/ia/iiy067.

وتعزز طريقة تمثيل توكا لذاتها في ساحات التصدير الدفاعي الرسمية هذا التموضع. ففي تقاريرها لعام 2025، تعلن الشركة عن نفسها بوصفها مزوّداً لـ«منصات برمجية هي الأولى من نوعها في مجال الأدلة الجنائية الرقمية والاستخبارات»، مستهدفة صراحةً «الحكومات الموثوقة، وأجهزة إنفاذ القانون، والوكالات الأمنية». وتؤكد موادها «الأدوات القانونية للأدلة الجنائية الرقمية وجمع المعلومات الاستخباراتية»، إلى جانب قدرات تتعلق بـ«الاستخبارات المستهدفة» و«العمليات السرية»، مقدّمةً تقنياتها بوصفها أدوات تتيح تحقيقات أسرع، وقابلة للتوسّع، وذات كفاءة عملياتية.[79]

3. الانتشار العالمي

تصرّ توكا، علناً وفي ردودها على التحقيقات، على أنها لا تعمل إلا مع الولايات المتحدة وحلفائها، في قطاعات تشمل الجيش، والأمن الداخلي، ووكالات الاستخبارات، وإنفاذ القانون، وحماية الحدود، وسلطات المدن الذكية.[80] كما تسوّق خدمات استشارية لفرق الاستجابة لطوارئ الحاسوب الوطنية (CERTs)، ولمشغّلي البنية التحتية الحيوية في القطاع الخاص.[81]

جغرافيا العملاء وقطاعاتهم

إسرائيل

الدولة الإسرائيلية هي العميل الأول والتأسيسي لتوكا. وبحلول عام 2021، أفيد بأنها كانت تملك عقوداً بقيمة عدة ملايين من الدولارات مع وكالات أمنية إسرائيلية. وتُنسَّق منتجاتها مع وزارة الدفاع، كما تُعامل موافقات التصدير الخاصة بها كجزء من نظام أوسع لمراقبة الأسلحة في إسرائيل.[82]

نيجيريا

في عام 2020، اختار البنك الدولي توكا لتقديم المشورة للحكومة النيجيرية بشأن تصميم وتعزيز الصمود السيبراني الوطني. وفي إطار هذا المشروع الممول من البنك الدولي، شاركت توكا في بناء أطر الأمن السيبراني في نيجيريا، وقدراتها التقنية، ومهاراتها، بما في ذلك العمل مع فريق الاستجابة لطوارئ الحاسوب الوطني والشركات الخاصة.[83]

79 Cybertoka Ltd. "First-of-their-kind software platforms for digital forensics and intelligence." Company profile in SIBAT (Israel Ministry of Defense) export materials.

80 Thomas Brewster, "Alexa, Are You a Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT," Forbes, July 15, 2018, https://www.forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies/

81 Whitney Webb, "Meet Toka, the Most Dangerous Israeli Spyware Firm You've Never Heard Of," MintPress News, July 21, 2021, https://www.mintpressnews.com/meet-toka-the-most-dangerous-israeli-spyware-firm-youve-never-heard-of/278020/

82 Becky Peterson, "The Founders of a Billion-Dollar Israeli Spyware Startup Accused of Helping Saudi Arabia Attack Dissidents Are Funding a Web of New Companies That Hack into Smart Speakers, Routers, and Other Devices," Business Insider, September 5, 2019, https://www.businessinsider.com/inside-the-israel-offensive-cybersecurity-world-funded-by-nso-group-2019-8.

83 IsraelDefense, "Israel's Toka Advising Nigeria on Cyber Security," February 24, 2020, https://www.israeldefense.co.il/en/node/42066.

مولدوفا

وفي عام 2020 أيضاً، حصلت توكا على عقد ممول من البنك الدولي في مولدوفا لتحديد فجوات الأمن السيبراني في القطاع العام واقتراح استراتيجية لتحسين الجاهزية. وعلى الرغم من أن مولدوفا دولة صغيرة، فإن هذا الانخراط أظهر كيف يمكن لشركات السيبرانية الإسرائيلية أن تستفيد من التمويل متعدد الأطراف للدخول إلى بُنى الدولة التحتية في أوروبا الشرقية. [84]

تشيلي

في عام 2020، اختارت الحكومة التشيلية وبنك التنمية للبلدان الأمريكية توكا لتقديم المشورة بشأن الجاهزية الوطنية للأمن السيبراني وبناء القدرات العملياتية. وتستضيف تشيلي واحدة من أكبر الجاليات الفلسطينية في العالم، وتتمتع بدعم داخلي قوي لفلسطين؛ ولذلك فإن إدخال توكا في الجهاز الأمني التشيلي يحمل دلالة جيوسياسية واضحة بالنسبة إلى إسرائيل. [85]

غانا

كما حصلت توكا على عقد مع البنك الدولي في غانا ضمن برنامج عالمي مماثل لبناء قدرات الأمن السيبراني، موسّعةً بذلك انتشارها في غرب أفريقيا. [86]

المكسيك

تشير بيانات الحكومة المكسيكية إلى أن توكا تعمل بالفعل في المكسيك. وتلاحظ وسائل إعلام إسرائيلية تزايد الاهتمام التجاري الإسرائيلي بالمكسيك في ظل الإدارة الحالية، بما يشير إلى كيفية ربط العقود السيبرانية بتدفقات استثمارية أوسع. [87]

وتشير توكا أيضاً إلى أعمال أو تطوير أسواق في الولايات المتحدة، وألمانيا، وأستراليا، وسنغافورة، وبلجيكا.

استراتيجيات الوصول

إلى جانب العقود الرسمية، عملت قيادة توكا بنشاط على توسيع أسواقها. فقد أفادت تقارير بأن يارون روزن انخرط مع مسؤولين مغاربة في جهود لدخول ذلك السوق. [88] كما كان ممثلو الشركة حاضرين بوضوح في فعاليات أمنية وتكنولوجية مثل «ميليبول»، و«ISS World»، و«جيتكس» في دولة الإمارات العربية المتحدة، ومؤتمرات سيبرانية إقليمية أُطّرت بوصفها منتديات للأمن السيبراني بين إسرائيل

84 Toka, “Toka Awarded World Bank-Financed Contract to Strengthen Moldova’s National Cybersecurity Readiness,” Yahoo Finance, September 10, 2020, https://finance.yahoo.com/news/toka-awarded-world-bank-financed-100000596.html.

85 Toka, “Toka Selected by Chile and Inter-American Development Bank to Assess and Support Chile’s National Cybersecurity Readiness,” GlobeNewswire, May 19, 2020, https://www.globenewswire.com/news-release/2020/05/19/2035462/0/en/Toka-Selected-by-Chile-and-Inter-American-Development-Bank-to-Assess-and-Support-Chile-s-National-Cybersecurity-Readiness.html

86 “Toka Scores $25 Million Series B to Enhance Cybersecurity of Gov’t Organizations,” Israel Defense, October 31, 2020, https://www.israeldefense.co.il/en/node/46195.

87 Jessica Buxbaum, “How Israeli Cyber Weapons Are Taking Over Latin America,” MintPress News, March 3, 2023, https://www.mintpressnews.com/israeli-cyber-weapons-taking-latin-america/283926/.

88 Kenza Filali, “L’Israélien Illuminant cherche à investir le marché marocain de la cyberdéfense d’État,” Le Desk, July 21, 2023, https://mobile.ledesk.ma/enoff/lisraelien-illuminant-cherche-a-investir-le-marche-marocain-de-la-cyberdefense-detat/.

والإمارات وأوروبا الشرقية.[89] وقد أشارت قيادة المبيعات في توكا علناً إلى نشاط في دولة الإمارات وآسيا، بما يتماشى مع اندفاعة إسرائيلية أوسع نحو أسواق السيبرانية في الخليج وآسيا بعد اتفاقيات التطبيع.

ويُعد الانتشار العالمي لتوكا جزءاً من مشروع سياسي أكبر. فقد حددت إسرائيل صراحةً السيبرانية الهجومية بوصفها ركناً من أركان سياستها الصناعية والخارجية.[90] وعلى الصعيد المحلي، تدعم أدوات توكا توسّع المراقبة وتآكل المساءلة. فهي تمكّن السلطات من تحويل المستشعرات الحضرية المنتشرة في كل مكان إلى أنظمة استخبارات مركزية، ومن تتبع المعارضين وترهيبهم، ومن محو السجلات البصرية لعنف الدولة أو فبركتها. أما دولياً، فيمكن استخدام الأدوات نفسها لمراقبة الحركات العابرة للحدود، بما في ذلك شبكات التضامن، واللاجئون، والناشطون. ويكتسب ذلك أهمية خاصة في ضوء التقارير التي تفيد بأن إسرائيل وشركات حليفة لها استخدمت السيبرانية الهجومية لتتبع حركات مثل حركة المقاطعة وسحب الاستثمارات وفرض العقوبات (BDS) وتعطيلها.

وأخيراً، تسهم توكا في تطبيع السيبرانية الهجومية بوصفها شكلاً من أشكال «التنمية». فعندما تُموَّل حِزم اختراق الكاميرات وأدوات محو الأدلة من قبل البنك الدولي أو بنك التنمية للبلدان الأمريكية تحت عنوان «بناء القدرات السيبرانية»، يكون هناك تحوّل سياسي جارٍ، أي أن المراقبة ذات الطابع العسكري تصبح جزءاً من الأدوات القياسية للحوكمة الحديثة. إن تركيز الغضب الموجه إلى «بيغاسوس» يحجب الانتباه على شركات مثل توكا، التي تتوافق أنشطتها بصورة أكثر راحة مع أجندات الأمن الغربية ومتعددة الأطراف، ومن ثم تجذب قدراً أقل من التدقيق. وتتمثل النتيجة في ترسيخ هادئ لنظام مراقبة عالمي تُدمج فيه التقنيات ذات المنشأ الإسرائيلي بعمق في البنى التحتية الأمنية للدول «الحليفة»، غالباً خارج نطاق الرقابة العامة أو السيطرة الديمقراطية.

كورسايت إيه آي

«كورتيكا» هي شركة إسرائيلية للذكاء الاصطناعي انبثقت عن التخنيون عام 2007.[91] وتقدّم نفسها كقوة مدنية في مجال الذكاء الاصطناعي، تطوّر تعلّماً «مستوحى من الدماغ»، غير خاضع للإشراف ثم تفصل هذه التكنولوجيا الأساسية إلى شركات متخصصة بحسب القطاعات: أ) «أوتوبرينز» للقيادة الذاتية، والمدعومة من «بي إم دبليو» و»تويوتا»،[92] ب) «سي ترو» للفحص الآلي للأمتعة والأمن،[93] ج)

89 AP News, “Garry Kasparov at IMPROVATE Cybersecurity Conference Is Talking About Chess, IA and The Queen’s Gambit,” AP News (press release), February 16, 2021, https://apnews.com/press-release/pr-newswire/technology-israel-middle-east-garry-kasparov-government-and-politics-e08751ae82db627107fb60602b63062e.

90 Freilich, Charles D, Matthew S Cohen, and Gabi Siboni. 2023. Israel and the Cyber Threat. Oxford University Press.

91 NoCamels Team, “Israeli Startup Raises $5M For Facial Recognition Tech That Can Identify Masked Faces,” NoCamels, April 23, 2020, https://nocamels.com/2020/04/israeli-startup-corsight-facial-recognition-tech-masked/.

92 Meir Orbach, “BMW, Toyota Partner With Computer Vision Company Cortica,” Calcalist Tech, September 4, 2019, https://www.calcalistech.com/ctech/articles/0,7340,L-3769653,00.html.

93 SeeTrue, “SeeTrue AI Screening Solution Becomes the First and Only to Receive ECAC Certification for Automated Prohibited Items Detection (APIDS),” PR Newswire, January 8, 2026, https://www.prnewswire.com/apac/news-releases/seetrue-ai-screening-solution-becomes-the-first-and-only-to-receive-ecac-certification-for-automated-prohibited-items-detection-apids-302655629.html.

«فينتيكا» للتحليلات المالية، ومشاريع التصوير الطبي مثل «كورديغايد»، [94] وأخيراً «كورسايت إيه آي»، التي أُطلقت في أواخر عام 2019 بوصفها ذراع التعرف على الوجوه ضمن هذه المحفظة، أي شركة «استخبارات وجوه» أُنشئت لتسويق قدرات الرؤية الحاسوبية لدى «كورتيكا» في مجال المراقبة.[95]

وكورتيكا شركة مملوكة ملكية خاصة، وقد جمعت أكثر من 70 مليون دولار، وتعمل من تل أبيب وحيفا ونيويورك وجنيف.[96] وعلى الرغم من التطبيقات الأمنية الواضحة لمنتجاتها، فإنها غير مدرجة في «سيبات». ويتيح ذلك لكورتيكا أن تقدّم نفسها كشركة ذكاء اصطناعي مدنية، حتى في الوقت الذي تعمل فيه شركاتها المنبثقة مباشرة مع مستثمرين مرتبطين بالدفاع وأجهزة أمن الدولة. [97] فعلى سبيل المثال، أُنشئت كورسايت كمشروع مشترك بين كورتيكا وصندوق «Awz Ventures» الكندي، الذي يقيم شراكة صريحة مع مديرية البحث والتطوير التابعة لوزارة الدفاع الإسرائيلية، ويقوده مسؤولون سابقون في الموساد والشاباك وأجهزة استخبارات أخرى، مع رئيس الوزراء الكندي السابق ستيفن هاربر كمستشار بارز.[98]

1. النشأة، والكوادر، والموقع

تقع كورسايت إيه آي عند تقاطع الخبرة الاستخباراتية الإسرائيلية، والبحث الأكاديمي، ورأس المال الأمني العابر للحدود. وقد شارك في تأسيسها قادة كورتيكا: الرئيس التنفيذي إيغال رايشلغاوز، والدكتورة كارينا أودينايف، وأستاذ التخنيون جوش زئيفي. ورايشلغاوز وأودينايف من قدامى الوحدات التكنولوجية النخبوية في الجيش الإسرائيلي؛ إذ بدأ رايشلغاوز مسيرته في الوحدة 8200، وهي وحدة استخبارات الإشارات والسيبرانية الإسرائيلية. [98] كما يأتي عدد من مهندسي الأبحاث في كورسايت من الوحدة 8200، حاملين معهم خبرة الدولة في المراقبة، والاعتراض، وتحليل البيانات. ويوفّر العمل الأكاديمي لزئيفي الأساس لخوارزميات كورتيكا الجوهرية، بما يمنحها الشرعية العلمية بوصفها «مستوحاة من الدماغ». [99] وعند إطلاقها، كانت كورسايت فريقاً صغيراً، يضم نحو 15 موظفاً موزعين بين إسرائيل والولايات المتحدة، لكنها استفادت من الملكية الفكرية الواسعة لكورتيكا، والتي تشمل أكثر من 250 براءة اختراع، لتدّعي امتلاك حاجز تقني عميق يصعب تجاوزه. [100]

94 Fintica AI, Ltd., “Fintica AI Completes Financial Market Manipulation Detection Pilot for Israel Securities Authority,” PR Newswire, September 14, 2021, https://www.prnewswire.com/il/news-releases/fintica-ai-completes-financial-market-manipulation-detection-pilot-for-israel-securities-authority-301376523.html.

95 Corsight AI, “Corsight AI Becomes First Facial Recognition Provider to Achieve ISO/IEC 42001 AI Management Certification,” March 25, 2025, https://www.corsight.ai/press/corsight-ai-becomes-first-facial-recognition-provider-to-achieve-iso-iec-42001-ai-management-certification/.

96 Cortica Inc., “Cortica Closes $75 Million in New Funding Round and Acquires Springtide Child Development,” PR Newswire, April 18, 2023, https://www.prnewswire.com/news-releases/cortica-closes-75-million-in-new-funding-round-and-acquires-springtide-child-development-301800688.html

97 Rob Watts, “AI in Policing: Doing More with Less,” Corsight AI Blog, September 3, 2025, https://www.corsight.ai/facial-intelligence-uk-policing/.

98 Simon Speakman Cordall, “UK Police to Use AI Facial Recognition Tech Linked to Israel’s War on Gaza,” Al Jazeera, January 28, 2026, https://www.aljazeera.com/news/2026/1/28/uk-police-to-use-ai-facial-recognition-tech-linked-to-israels-war-on-gaza.

99 James Spiro, “Cortica Announces CORDiguide, Medical Spin-Off,” Calcalist Tech, March 9, 2021, https://www.calcalistech.com/ctech/articles/0,7340,L-3897691,00.html.

100 Corsight AI, “Corsight AI Announces U.S. Expansion Due to Market Demand for Leading AI Facial Recognition Technology,” PR Newswire, March 31, 2022, https://www.prnewswire.com/news-releases/corsight-ai-announces-us-expansion-due-to-market-demand-for-leading-ai-facial-recognition-technology-301514859.html.

وتجعل بنية الحوكمة والاستشارات في الشركة نسبها الأمني واضحاً. فيارون أشكنازي، مؤسس «Awz Ventures»، يشغل مقعداً في مجلس إدارة «كورسايت» بصفته شريكاً مديراً؛ وهو ضابط سابق في الشاباك قضى عقداً في قسم حماية الشخصيات المهمة.[101] أما عضو مجلس الإدارة الآخر، اللواء احتياط غيورا آيلاند، فقد ترأس سابقاً مديرية العمليات في الجيش الإسرائيلي، ثم تولى رئاسة مجلس الأمن القومي الإسرائيلي.[102] وكان رون تيبرغ-شاحار، الذي شغل مبكراً منصب مدير العمليات، ضابطاً في الدفاع السيبراني في الجيش الإسرائيلي.[103] ويُدمج هذا التركيز من الشخصيات العسكرية والاستخباراتية السابقة كورسايت في النظام البيئي الأمني نفسه الذي يحكم الاحتلال والعمليات العسكرية الإقليمية.

وفي الوقت نفسه، جمعت كورسايت طبقة قيادية ذات واجهة دولية مصممة لجعل الشركة مقبولة لدى الجهات التنظيمية في أوروبا وأمريكا الشمالية. فقد عيّنت توني بورتر، المفوض السابق لكاميرات المراقبة في المملكة المتحدة، كبيراً لمسؤولي الخصوصية للإشراف على النشر «الأخلاقي»[104]. ولهذا السبب، تتحدث كورسايت إيه آي، بوصفها شركة بالمعنى الاقتصادي، بلغتين في آن واحد: داخلياً، لغة أمن الدولة والقدرات ذات المستوى العسكري؛ وخارجياً، لغة الأخلاقيات، والامتثال، و«الذكاء الاصطناعي المسؤول».

2. من «استخبارات الوجوه» إلى السيطرة على السكان

تطوّر كورسايت ما تسميه حلول «استخبارات الوجوه»، أي أنظمة التعرف على الوجوه التي تحلل الفيديو المباشر أو المسجل من الكاميرات لتحديد هوية الأفراد بسرعة عالية وفي ظروف غير مثالية. وتستوعب منصتها الرئيسية، «Fortify»، تدفقات الفيديو، وتبني قوالب بيومترية من الوجوه، ثم تطابقها مع قوائم المراقبة لإصدار تنبيهات فورية عندما يظهر شخص محل اهتمام أو عندما يدخل شخص ما إلى منطقة محظورة.[105]

ومن الناحية التقنية، تزعم الشركة أن خوارزمياتها، المستمدة من محرك الذكاء الاصطناعي المستقل التابع لكورتيكا، قادرة على التعرف على الأفراد حتى عندما يكون أقل من نصف الوجه مرئياً، أو عندما يكون الشخص متحركاً، أو محجوباً جزئياً، أو يرتدي قناعاً أو خوذة. وخلال جائحة كوفيد19-، سوّقت كورسايت هذه القدرة بقوة باعتبارها ميزة تميّزها، إذ أعلنت عن القدرة على تحديد هوية الأفراد الذين يرتدون الكمامات بدقة، دعماً لإنفاذ الحجر الصحي، والمساعدة في تتبع المخالطين. وتُباع القدرة نفسها اليوم كميزة في مجالات إنفاذ القانون، ومراقبة الحدود، ونشر أنظمة «المدينة الآمنة»، حيث قد يغطي الناس وجوههم أو تلتقطهم الكاميرات في إضاءة ضعيفة ومن زوايا حادة.[106]

101 Awz Ventures, "The Awz Story," accessed April 1, 2026, https://www.awzventures.com/awz-story/.

102 Maj. Gen. (res.) Giora Eiland, "Author Page," Begin-Sadat Center for Strategic Studies, accessed April 1, 2026, https://besacenter.org/author/geiland/.

103 Ron Tiberg-Shachar," The Org, accessed April 1, 2026, https://theorg.com/org/saiflow/org-chart/ron-tiberg-shachar"

104 Biometrics and Surveillance Camera Commissioner, Biometrics and Surveillance Camera Commissioner's Annual Report 2023 to 2024, December 2, 2024, https://www.gov.uk/government/publications/biometrics-and-surveillance-camera-commissioner-report-2023-to-2024/biometrics-and-surveillance-camera-commissioners-annual-report-2023-to-2024-accessible

105 Corsight AI, "Fortify," accessed April 1, 2026, https://www.corsight.ai/product-fortify/.

106 Corsight, "Corsight AI Facial Intelligence in Retail," YouTube video, February 14, 2024, https://www.youtube.com/watch?v=GXDjkwWetpg.

وتشير كورسايت إيه آي إلى تقييمات مستقلة، مثل اختبار التعرف على الوجوه الذي أجرته وزارة الأمن الداخلي الأمريكية عام 2020، لإظهار أن نظامها جاء ضمن المراتب العليا من حيث الدقة، بما في ذلك في ظروف ارتداء الكمامات. [107] وتصر كورسايت، من خلال ورقة كتبها توني بورتر نفسه، على أن نماذجها غير متحيزة للعرق، والجندر، والعمر، متناولةً بذلك الأداء التمييزي الموثق جيداً لكثير من أنظمة التعرف على الوجوه. [108]

ومنذ نشأتها، عملت كورسايت إلى جانب الوكالات العسكرية والاستخباراتية الإسرائيلية، التي أصبحت من أوائل الجهات التي تبنّت أنظمتها. وتقر الشركة بأن كثيراً من عمليات النشر هي عمليات سرية تخص «وكالات استخبارات ووحدات خاصة لإنفاذ القانون».[109]

ويُعد أحد أوضح الأمثلة على ذلك الأراضي الفلسطينية المحتلة. فقد أظهرت تقارير منظمة العفو الدولية أن تقنية التعرف على الوجوه التي تطورها كورسايت تُستخدم من قبل الاستخبارات العسكرية الإسرائيلية لبناء قواعد بيانات بيومترية للفلسطينيين والحفاظ عليها. [110] وخلال الحرب على غزة، حمل الجنود كاميرات مزودة ببرمجيات كورسايت عند نقاط التفتيش وعلى مسارات الإخلاء، حيث كانوا يمسحون وجوه الفلسطينيين دون موافقة، ويقارنون تلك الصور بقوائم المراقبة.

أما في الخارج، فإن الغالبية الساحقة من عمليات النشر تتم في مجالات إنفاذ القانون، ومراقبة الحدود، ومراقبة البنية التحتية الحيوية، مثل شبكات كاميرات المراقبة في المدن، والمطارات، والمناجم والبنوك، والمعابر الحدودية، والفعاليات العامة. [111] [112]

وبهذا المعنى، تعمل «كورسايت» كنقطة لقاء في تمديد منطق الأمن الإسرائيلي إلى ما وراء الحدود الإقليمية. فهي توسّع نطاق الممارسات الأمنية الإسرائيلية إلى ولايات قضائية جديدة، وتعيد توزيع القوة لصالح الدول والجهات المؤسسية التي تنشر هذه الأنظمة، في حين تضع الأفراد والمجتمعات في أماكن أخرى كأهداف للمنطق نفسه من المراقبة، والتصنيف، والسيطرة.

3. الانتشار العالمي

يرسم توسّع كورسايت خريطة الطلب العالمي على البنية التحتية للمراقبة، ويعكس استراتيجية إسرائيل الأوسع في تصدير تقنيات الأمن بوصفها شكلاً من أشكال الدبلوماسية، والتنمية، وبناء النفوذ. [112] وتفيد الشركة بأن لديها عمليات

107 Tony Porter, "Facial Recognition Technology: Blasting the Bias Narrative Out of the Water?," Biometric Technology Today 2022, no. 12 (2022), https://doi.org/10.12968/S0969-4765(22)70622-4.

108 Tony Porter, "Facial Recognition Technology: Blasting the Bias Narrative Out of the Water?," Biometric Technology Today 2022, no. 12 (2022), https://doi.org/10.12968/S0969-4765(22)70622-4.

109 Sheera Frenkel, "Report Reveals Google & Corsight Technologies' Role in Israel's Expansive Facial Recognition Program in Gaza," Business & Human Rights Resource Centre, March 27, 2024, https://www.business-humanrights.org/en/latest-news/report-reveals-google-corsights-technologies-role-in-israels-expansive-facial-recognition-program-in-gaza/.

110 Amnesty International, "Israel/OPT: Israeli Authorities Are Using Facial Recognition Technology to Entrench Apartheid," May 2, 2023, https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/.

111 Corsight AI, "Facial Recognition at Airports," accessed April 1, 2026, https://www.corsight.ai/airports/.

112 This is well-highlighted in a paper by Lior Tabansky, "Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy," NATO Cooperative Cyber Defence Centre of Excellence, 2018, https://ccdcoe.org/uploads/2018/10/Art-04-Towards-a-Theory-of-Cyber-Power-the-Israeli-Experience-with-Innovation-and-Strategy.pdf.

نشر في أكثر من خمسين دولة، غالباً من خلال مدمجين محليين ومشاريع «المدينة الآمنة» التي تربط بين الإضاءة الذكية، والكاميرات، والتحليلات. [113]

1.3 منطقة جنوب غرب آسيا وشمال أفريقيا

قادت «Awz» التوسع نحو أسواق الخليج التي فتحتها اتفاقيات أبراهام. فقد أنشأت «Awz» شركة تابعة في دولة الإمارات العربية المتحدة لتوجيه تقنيات الأمن الإسرائيلية، بما في ذلك كورسايت، من خلال ابرام عقود إماراتية وإقليمية. [114] وقد أقرّ مسؤولون تنفيذيون في كورسايت بوجود محادثات مع قوات شرطة خليجية، بما يتماشى مع جهود أوسع لوضع إسرائيل كمزوّد رئيسي لمراقبة المدن الذكية والحدود لدول مثل الإمارات العربية المتحدة والمملكة العربية السعودية. [115]

2.3 أفريقيا

في أفريقيا، تدخل كورسايت إلى حد كبير من خلال الشراكات. ففي ناميبيا، أصبحت «Schoemans Technologies» موزعها الحصري، مسوّقةً أنظمة التعرف على الوجوه للحكومة والمؤسسات. [116] وفي جنوب أفريقيا، دمجت شركة الأمن «E-Thele» خوارزميات «كورسايت» في أنظمة مراقبة للمناجم والبنوك، لمراقبة الوصول إلى المواقع ذات القيمة العالية. [117]

3. 3 آسيا والمحيط الهادئ

في الفلبين، نشرت مدينة سانتا روزا منصة كورسايت ضمن مبادرة «المدينة الآمنة»، حيث شغّلت عمليات مسح فورية وجنائية رقمية عبر شبكة كاميرات المراقبة التابعة لها لرصد الأشخاص المطلوبين والتعرف على الأفراد المفقودين. [118] كما سعت كورسايت إلى الحصول على فرص في الهند، حيث وقّعت مذكرة تفاهم مع مؤسسة الإلكترونيات التابعة لولاية آسام (AMTRON) لإنشاء مركز تميز للتعرف على الوجوه في غواهاتي لعملاء الحكومة الهندية. [119] وتستهدف شراكة مع الموزع السنغافوري «Netpoleon» أسواق جنوب شرق آسيا على نحو أوسع، من خلال الجمع بين خوارزميات كورسايت والمدمجين الأمنيين المحليين لإدخال التعرف على الوجوه في البنى التحتية للأمن الحضري والوطني. [120]

113 Iain Overton, "Corsight's Crisis: Why British Police Forces Must Rethink Their Israeli Facial Recognition Partners," Action on Armed Violence (AOAV), July 7, 2025, https://aoav.org.uk/2025/corsights-crisis-why-british-police-forces-must-rethink-their-israeli-facial-recognition-partners/.

114 Brigitte Bureau, "Stephen Harper Involved in Company Looking to Arrange Sale of Surveillance Tech to UAE," CBC News, September 29, 2021, https://www.cbc.ca/news/politics/harper-united-arab-emirates-surveillance-technology-1.6192281.

115 "Israelis Pour into UAE for Business and Pleasure," Ynetnews, December 9, 2020, https://www.ynetnews.com/travel/article/Bk00xPYRiD.

116 Corsight AI, "Corsight AI Announces Strategic Partnership With Schoemans Technologies in Namibia," Business Wire, January 30, 2025, https://www.businesswire.com/news/home/20250130146143/en/Corsight-AI-Announces-Strategic-Partnership-With-Schoemans-Technologies-in-Namibia.

117 eThele, "Partners," accessed April 1, 2026, https://www.ethele.co.za/partners/.

118 Corsight AI, "Santa Rosa Safe City Enhances Public Safety with Corsight AI's Unique Facial Intelligence Technology," Business Wire, September 26, 2024, https://www.businesswire.com/news/home/20240926379646/en/Santa-Rosa-Safe-City-Enhances-Public-Safety-with-Corsight-AIs-Unique-Facial-Intelligence-Technology.

119 "Corsight AI Partners for Facial Recognition Projects in India," Biometric Update, August 19, 2021, https://www.biometricupdate.com/202108/corsight-ai-partners-for-facial-recognition-projects-in-india.

120 Corsight AI, "Leading Facial Recognition Technology Provider, Corsight AI, Announces Netpoleon as Distribution Partner for Asia," PR Newswire, May 12, 2021, https://www.netpoleons.com/news/leading-facial-recognition-technology-provider-corsight-ai-announces-netpoleon-as-distribution-partner-for-asia.

3. 4 أوروبا

يكمن حضور كورسايت في أوروبا من خلال المطارات، والمستشفيات، والشرطة. وتفيد الشركة بأن لديها عمليات نشر في عدة مطارات ومرافق رعاية صحية أوروبية ضمن أنظمة التحكم في الوصول والأمن. [121] وفي المملكة المتحدة، اعتمدت شرطة إسيكس نظاماً حياً للتعرف على الوجوه مبنياً على تقنية كورسايت، مستخدمةً كاميرات في الفعاليات العامة ومحطات النقل لمسح الحشود واعتقال المشتبه بهم. وتقدّم قيادة كورسايت في المملكة المتحدة، المؤلفة من شخصيات سابقة في تكنولوجيا الشرطة، هذه العمليات بوصفها ممتثلة تماماً للأنظمة الوطنية، رغم المخاوف المتعلقة بالحريات المدنية. [122]

3. 5 الأمريكتان

تُعد أمريكا اللاتينية من مناطق النمو الرئيسية. ففي البرازيل، عقدت كورسايت شراكات مع شركات مثل «Teltex» و«Segurimax» لنشر مراكز للتعرف على الوجوه عبر كتائب شرطة ولاية ساو باولو. [123] ودمجت شركة الإضاءة الذكية الإسرائيلية «Juganu» نظام كورسايت في أعمدة إنارة «ذكية» على جسر الصداقة بين البرازيل وباراغواي، بحيث تلتقط وجوه المسافرين ولوحات أرقام المركبات وتبث تلك البيانات إلى سلطات الحدود، في مثال على مراقبة بيومترية منسوجة داخل بنية تحتية تبدو محايدة، أي الإضاءة، لكنها تعمل كوحدة لجمع البيانات. [124] وفي باراغواي، رخّصت «Grupo Vázquez» خوارزميات كورسايت لإدماج التعرف على الوجوه عبر أعمالها المتنوعة وبيع الخدمات لوكالات حكومية. [125]

وفي المكسيك، عقدت كورسايت شراكة مع شركة الأمن «ISEG» لتركيب تقنية التعرف على الوجوه في ثلاثة مستشفيات في مونتيري، ضمن شبكة الرعاية الصحية «Auna»، لمراقبة وحدات العناية المركزة وغيرها من المناطق الحساسة. [126] كما ارتبطت كورسايت بالشرطة الفيدرالية المكسيكية ووكالات إقليمية أخرى. [127] وفي كولومبيا، نفذت شرطة بوغوتا الحضرية تجربة عام 2023 باستخدام كورسايت للتعرف على مشتبه بهم من لقطات كاميرات المراقبة. وفي أنحاء الأمريكتين، يتكرر النمط نفسه: الدمج في الشرطة، ومراقبة الحدود، والمستشفيات، والمواقع التجارية عالية القيمة، تحت شعار التحديث والكفاءة . [128]

ويقود توسّع كورسايت استراتيجية إعلانية تجمع بين الاعتمادات الأمنية النخبوية

121 "EU AI Pact Sets New Standards for Ethical AI Use Across Europe," Biometric Update, September 13, 2024, https://www.biometricupdate.com/202409/eu-ai-pact-sets-new-standards-for-ethical-ai-use-across-europe

122 Robert Booth, and Mark Wilding. "Essex Police Pause Facial Recognition Camera Use After Study Finds Racial Bias." The Guardian, March 19, 2026. https://www.theguardian.com/technology/2026/mar/19/essex-police-pause-facial-recognition-camera-use-study-racial-bias

123 Corsight AI. "Corsight AI Partners with Segdboa to Provide São Paulo Military Police with Facial Intelligence Capabilities." Business Wire, June 19, 2024. https://www.businesswire.com/news/home/20240619024171/en/Corsight-AI-Partners-with-Segdboa-to-Provide-So-Paulo-Military-Police-with-Facial-Intelligence-Capabilities.

124 Techtime. "Juganu Made the Brazil-Paraguay Border Safer." Techtime, July 2, 2020. https://techtime.news/tag/smart-city/.

125 Business Wire. "Corsight AI Partners with ITTI from Grupo Vázquez to Enhance Security, Efficiency, and User Experience with Facial Intelligence." Financial Post, September 2, 2024. https://financialpost.com/pmn/business-wire-news-releases-pmn/corsight-ai-partners-with-itti-from-grupo-vazquez-to-enhance-security-efficiency-and-user-experience-with-facial-intelligence.

126 Corsight AI. "Corsight AI Partners with ITTI from Grupo Vázquez to Enhance Security, Efficiency, and User Experience with Facial Intelligence." Security Journal Americas, September 2024. https://securityjournalamericas.com/partnership-for-facial-intergration/

127 Ibid.

128 IFSEC Insider. "Bogotá Police Using Facial Recognition to Enable Arrest of Murder and Theft Suspects." IFSEC Global, November 8, 2023. https://www.ifsecglobal.com/video-surveillance/bogota-police-using-facial-recognition-to-enable-arrest-of-murder-and-theft-suspects/

والخطاب الأخلاقي. فالشركة تبرز أداءها «بالمستوى العسكري» ونسبها إلى الوحدة 8200 عند البيع للأجهزة الأمنية، بينما تؤكد الأخلاقيات، والامتثال للخصوصية، ووجود منظم بريطاني سابق للمراقبة عند مخاطبة الجمهور والجهات التنظيمية في الديمقراطيات الليبرالية.[129] وعلى الرغم من هذه الروابط المؤسسية العميقة مع الجيش الإسرائيلي، أكد الرئيس التنفيذي لكورسايت علناً أن الشركة «لا تبيع للصين أو روسيا أو ميانمار بسبب حقوق الإنسان والأخلاقيات»، مقدّماً تقنيتها بوصفها «قوة للخير» من أجل إنفاذ القانون.[130] وتضع مثل هذه الادعاءات الشركة ضمن إطار أخلاقي انتقائي، حيث لا تُساءَل شرعية المراقبة في ذاتها، بل يُعاد تأطيرها من خلال اختيار العملاء، بما يسمح بتسويق التكنولوجيا بوصفها مسؤولة وواعية بالحقوق، حتى وهي تظل مدمجة في بُنى تحتية للسيطرة ذات طابع عسكري.

الخلاصات الرئيسة

لا تكمن أهمية هذه النتائج فيما تفعله هذه الشركات فحسب، بل في البنية التحتية التي تجعل عملياتها ممكنة. وتُظهر نتائج هذه الورقة أن توكا وكورسايت إيه آي لا يمكن فهمهما على نحو أدق بوصفهما شركتين تكنولوجيتين خاصتين ومعزولتين، بل بوصفهما أدوات على مستوى الشركة بالمعنى الاقتصادي، تُغسل، بالمعنى الحرفي، من خلالها السياسة الصناعية الإسرائيلية ذات الطابع العسكري.[131] ويتوافق ذلك مع مجموعة متنامية من الأدبيات التي تفهم المراقبة بوصفها ناشئة من تقاطع سلطة الدولة،[132] والفاعلين المؤسسيين،[133] والأسواق العابرة للحدود،[134] لا من مجالات مؤسسية منفصلة.

وعلى الرغم من أن توكا وكورسايت تعملان في مجالين تكنولوجيين مختلفين، فإنهما تؤديان أدواراً متكاملة داخل بنية السياسة الصناعية نفسها. فتجسّد توكا كيفية دمج القدرات السيبرانية الهجومية في الحوكمة من خلال لغة الاستخبارات القانونية والمرونة، في حين تُظهر كورسايت كيفية تطبيع المراقبة البيومترية من خلال خطابات الذكاء الاصطناعي الأخلاقي والامتثال. واستناداً إلى الأعمال الحديثة لمعهد «AI Now» حول «قوميات الذكاء الاصطناعي»، التي تبرز كيف تعبّئ الدول السياسة الصناعية لتشكيل أنظمة الذكاء الاصطناعي بما يتماشى مع الأولويات

129 Liberty. "Liberty Responds to Essex Police Pausing Use of Facial Recognition Cameras Due to Racial Bias." Liberty Human Rights, March 20, 2026. https://www.libertyhumanrights.org.uk/issue/liberty-responds-to-essex-police-pausing-use-of-facial-recognition-cameras-due-to-racial-bias/

130 Cheslow, Daniella. "Israeli Firm Develops Body Cams with Facial Recognition Technology." The Times of Israel, January 23, 2022. Updated January 25, 2022. https://www.timesofisrael.com/israeli-firm-develops-body-cams-with-facial-recognition-technology/.

131 Yaron Salman, "Light unto the Nations Through Arms Sales: Israel's Arms Diplomacy Goals, Achievements, and Limitations," Contemporary Review of the Middle East 12, no. 2 (2025), https://doi.org/10.1177/23477989251318874.

132 Feldstein, Steven. "Front Matter." In The Global Expansion of AI Surveillance. Washington, DC: Carnegie Endowment for International Peace, 2019. http://www.jstor.org/stable/resrep20995.1.

133 7amleh – The Arab Center for the Advancement of Social Media. Israel's Surveillance Industry and Human Rights: Impact on Palestinians and Worldwide. December 2023. https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf

134 Ahmad H. Sa'di, "Israel's Settler-Colonialism as a Global Security Paradigm," Race & Class 63, no. 2 (2021): 21–37, https://doi.org/10.1177/0306396821996231.

الجيوسياسية والاقتصادية،[135] يمكن فهم السياسة الصناعية الإسرائيلية للذكاء الاصطناعي كتشكيل مكثّف يُنظَّم فيه تطوير الذكاء الاصطناعي صراحةً حول العسكرة والضرورات الأمنية. [136]

وتُظهر النتائج أيضاً تطبيع المراقبة، وهو ما وصفه بعض الباحثين بأنه خطاب تكنوقراطي. [137] وتستخدم الشركتان مصطلحات السلامة العامة، والصمود السيبراني، والاستخبارات القانونية، والذكاء الاصطناعي الأخلاقي كأطر لإضفاء الشرعية، لا كأوصاف محايدة. وعلى المستوى المادي، تُظهر النتائج أن شكل الشركة بالمعنى الاقتصادي مركزي في عولمة التقنيات ذات الطابع العسكري. [138] فشركات مثل توكا وكورسايت لا تكتفي بتسويق ابتكارات الدولة تجارياً؛ بل تنظّمها، وتتوسطها، وتنشرها عبر ترتيبات تعاقدية وتنظيمية معقدة. ويدعم ذلك ويوسّع الحجج المتعلقة بنشوء «مجمع استخباراتي–صناعي»، تُدمج فيه الفاعلون من الشركات الكبرى بنيوياً في البنى التحتية الأمنية للدولة. [139]

وانسجاماً مع الانتقادات الموجهة إلى «الذكاء الاصطناعي الأخلاقي» بوصفه شكلاً من أشكال الحوكمة بلا قيود،[140] تشير النتائج إلى أن الادعاءات الأخلاقية تعمل كآليات للتمايز السوقي أكثر من كونها قيوداً جوهرية. وأخيراً، تعزز النتائج الانتقادات القديمة لتآكل الحدود بين الدولة والسوق في إنتاج الأمن. [141]

لقد موّل البنك الدولي وبنك التنمية للبلدان الأمريكية، خلال العقد الماضي، برامج للأمن السيبراني والحوكمة الرقمية مكّنت من دمج شركات مراقبة إسرائيلية في بُنى الدولة التحتية عبر الجنوب العالمي وما بعده. وبين عامي 2020 و2023، مُنحت عقود في نيجيريا ومولدوفا وغانا وتشيلي إلى توكا غروب. وبالتوازي مع ذلك، دمجت كورسايت إيه آي أنظمتها في بُنى الشرطة، ومراقبة الحدود، والمراقبة الحضرية في أكثر من خمسين دولة.

أولاً، ليست شركات مثل توكا وكورسايت فاعلين تقليديين من القطاع الخاص يعملون على هوامش الدولة. بل هي امتدادات تنظيمية لسياسة صناعية أوسع ذات طابع عسكري، تترجم القدرات العسكرية والاستخباراتية إلى منتجات قابلة للتوسّع في الأسواق العالمية. وتعمل كورسايت إيه آي وفق منطق موازٍ. فهي تنشأ من شبكة من المهندسين المدرَّبين عسكرياً وهياكل حوكمة مرتبطة بالاستخبارات،

135 Amba Kak, AI Nationalism(s): Global Industrial Policy Approaches to AI—Executive Summary (New York: AI Now Institute, 2024), https://ainowinstitute.org/publications/ai-nationalisms-executive-summary.

136 Anthony King, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence," Journal of Global Security Studies 9, no. 2 (June 2024): ogae009, https://doi.org/10.1093/jogss/ogae009.

137 David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies," in Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination, ed. David Lyon (London: Routledge, 2003), 13–30.

138 Rita Abrahamsen and Michael C. Williams, "Securing the City: Private Security Companies and Non-State Authority in Global Governance," International Relations 21, no. 2 (2007): 237–253, https://doi.org/10.1177/0047117807077006.

139 This paper has drawn on and referenced multiple works by Sophia Goodfriend, building on them to develop its argument. See: Sophia Goodfriend, "New Tech, Old War," London Review of Books (blog), July 2023, https://www.lrb.co.uk/blog/2023/july/new-tech-old-war

140 Jacob Metcalf, Emanuel Moss, and danah boyd, "Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics," Social Research: An International Quarterly 82, no. 2 (Summer 2019): 449–476 (New York: Data & Society Research Institute), https://datasociety.net/wp-content/uploads/2019/09/Owning-Ethics-PDF-version-2.pdf.

141 Linda Weiss and Elizabeth Thurbon, "Power Paradox: How the Extension of US Infrastructural Power Abroad Diminishes State Capacity at Home," Review of International Political Economy 25, no. 6 (2018): 779–810, https://doi.org/10.1080/09692290.2018.1486875.

وتطوّر أنظمة تعرف على الوجوه قادرة على تحديد هوية الأفراد في ظروف الحجب، والحركة، وضعف الرؤية.

ثانياً، إن التوسع العالمي لهذه التقنيات يُتاح من خلال شكل الشركة بالمعنى الاقتصادي نفسه، الذي يعمل كأداة مركزية من أدوات السياسة الصناعية. فمن خلال الشركات التابعة، والمشاريع المشتركة، واتفاقيات الترخيص، والوسطاء المحليين، يتحرك هؤلاء الفاعلون عبر ولايات قضائية متعددة، مع تجزئة المساءلة. وهذه المرونة التنظيمية ليست عرضية؛ بل تعكس نمطاً من التنظيم الصناعي تُنشَر فيه أولويات الدولة عبر شركات تستطيع إعادة تشكيل بنيتها القانونية والمالية والعملياتية استجابةً للبيئات التنظيمية. وبهذا المعنى، تصبح الشركة بالمعنى الاقتصادي الآلية التي تُفعَّل من خلالها السياسة الصناعية ذات الطابع العسكري خارج الحدود الرسمية للدولة. فهي تتيح الوصول إلى الأسواق وتمكّن من الالتفاف على القيود التي كانت ستنطبق خلافاً لذلك على الفعل المباشر للدولة. وما يتبلور هنا ليس نموذج تصدير خطياً، بل بنية تحتية موزعة تُوجَّه من خلالها قدرات المراقبة، ويُعاد تجميعها، وتُدمج داخل أنظمة الحوكمة المدنية.

ثالثاً، تعمل مؤسسات التنمية متعددة الأطراف كواجهات حاسمة في هذه العملية. فمن خلال دمج مثل هذه الشركات في برامج مؤطرة بوصفها بناءً للقدرات الرقمية، أو مرونة سيبرانية، أو تحديثاً مؤسسياً، تسهّل هذه المؤسسات تطبيع تقنيات المراقبة كمكونات من مكونات الحوكمة المشروعة. وهي بذلك لا تموّل تبنّي التكنولوجيا فحسب؛ بل تشارك بصورة فاعلة في بناء أسواق جديدة للتقنيات ذات الطابع العسكري، من خلال إعادة صياغتها بوصفها محايدة وضرورية وتنموية.

تواصلوا معنا:
info@7amleh.org | www.7amleh.org
صفحاتنا على وسائل التواصل الاجتماعيّ: 7amleh