معهد فلسطين لأبحاث الأمن القومي
Palestine Institute for National Security Research

الذكاء الاصطناعي والأمن الوطني الفلسطيني: فرص بناء القدرة ومخاطر التبعية الرقمية

ورقة بحثية في إطار موضوع «الذكاء الاصطناعي والتحول في طبيعة الصراع: الأمن والقرار والسيادة الرقمية في العصر الخوارزمي»

د. عامر أبو هنية

مدير وحدة الأمن السيبراني والذكاء الاصطناعي، معهد فلسطين لأبحاث الأمن القومي

الملخص

تسأل هذه الورقة، كيف يستفيد الفاعل الفلسطيني من الذكاء الاصطناعي في بناء قدرة أمنية وطنية من غير أن يزيد اعتماده الرقمي على أطراف لا سلطة له عليها، بعضها طرف في الصراع؟ وتتناول فلسطين بوصفها حالة حدّية؛ فالترددات وإدخال المعدات وربط الشبكات رهن موافقة إسرائيلية منذ عام 1995، ولم يُجَز الجيل الرابع في الضفة الغربية إلا في كانون الثاني/يناير 2026، فيما بقيت غزة على الجيل الثاني. وتعتمد الورقة التحليل الوثائقي، وتقترح إطاراً مزدوج السلسلة يقابل بين سلسلة القدرة وسلسلة التبعية في أربع طبقات (المادية، والبيانات، والخوارزميات، والقواعد)، وتقيس التبعية بخمسة معايير، خامسها «اتجاه التبعية» إضافةً تستدعيها الحالة الفلسطينية. وتخلص إلى أن أجدى الفرص وأقلها تبعية تقع في الأمن السيبراني الدفاعي، وحوكمة البيانات الحكومية المتبادلة عبر منصة «زنّار»، والموارد اللغوية العربية والفلسطينية، وأن عائقها الأول مؤسسي وتشريعي لا تقني. وتميّز بين مخاطر مفروضة من الخارج، كالتبعية المادية والعقوبات العابرة للحدود، ومخاطر داخلية قابلة للمعالجة، أهمها نقص الكفاءات وغياب قانون نافذ لحماية البيانات، وتنتهي بمصفوفة للفرص والمخاطر وخمس أولويات لا تحتاج إلى موافقة خارجية.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن الوطني، التبعية الرقمية، التبعية المُدارة، السيادة الرقمية، الأمن السيبراني، فلسطين.

معهد فلسطين لأبحاث الأمن القومي
Palestine Institute for National Security Research

Abstract

This paper asks how a Palestinian actor can use artificial intelligence to build national security capacity without deepening its digital dependency on parties it does not control, some of them parties to the conflict. Palestine is treated as an extreme case: spectrum, equipment entry and network interconnection have required Israeli approval since 1995; the West Bank was approved for 4G only in January 2026, while Gaza remains on 2G. Using documentary analysis, the paper develops a dual-chain framework that sets a capability chain against a dependency chain across four layers (physical, data, algorithms, rules) and assesses dependencies against five managed-dependency criteria, the fifth of which, direction of dependency, is added by the Palestinian case. The most feasible and least dependent opportunities lie in defensive cybersecurity, the governance of government data exchanged through the Zinnar platform, and Arabic and Palestinian language resources; their obstacles are mainly institutional and legislative. Risks divide into imposed risks (physical dependency and extraterritorial sanctions) and internal ones open to Palestinian action (the skills gap and the absence of a data protection law in force). The paper closes with an opportunity–risk matrix and five priorities that need no external approval.

Keywords: artificial intelligence, national security, digital dependency, managed dependency, digital sovereignty, cybersecurity, Palestine.

1. المقدمة

يغلب على الخطاب الرسمي العربي أن يقدّم الذكاء الاصطناعي فرصةً تنموية: إنتاجية أعلى وخدمات حكومية أسرع. لكنه يُسقط سؤالاً أشد إلحاحاً: من يملك البنية التي تعمل عليها هذه الأدوات، ومن يقدر على إيقافها أو الاطلاع على ما يمر خلالها؟ فقد أوضح Farrell وNewman (2019) أن الدول التي تقع العقد المركزية للشبكات العالمية تحت ولايتها تستطيع تحويل الاعتماد المتبادل إلى أداة إكراه، بالرصد أو بالقطع، ومع انتقال جزء متزايد من الأمن الوطني إلى البيانات ونماذج تحليلها يغدو موقع الفاعل في هذه الشبكات جزءاً من قوته أو من هشاشته.

ويأخذ السؤال في فلسطين طابعاً حاداً. فمنذ الاتفاقية المرحلية لعام 1995 ترتبط الترددات وإدخال المعدات وربط الشبكات بموافقة إسرائيلية (Israeli–Palestinian Interim Agreement, 1995)، ولم تُجَز خدمات الجيل الرابع في الضفة الغربية إلا في كانون الثاني/يناير 2026، فيما بقيت غزة على الجيل الثاني (Reuters, 2026). وفي المقابل صار الفضاء الفلسطيني ميداناً لتطبيقات خوارزمية يوظفها الطرف الآخر، من التعرف على الوجه في الخليل والقدس الشرقية (Amnesty International, 2023) إلى أدوات توليد الأهداف في غزة (Abraham, 2024؛ Human Rights Watch, 2024)، وهو ما نفاه الجيش الإسرائيلي (Israel Defense Forces, 2024). وفي أيلول/سبتمبر 2025 أقرت Microsoft بأن مراجعتها وجدت أدلة تدعم عناصر من التقارير عن استخدام وحدة في وزارة الدفاع الإسرائيلية لخدماتها السحابية، فأوقفت خدمات محددة لها (Smith, 2025).

على أن الفلسطينيين ليسوا متلقين فقط: فقد صدرت استراتيجية وطنية للذكاء الاصطناعي عام 2023 (Ministry of Telecommunications and Digital Economy, 2023؛ Demaidi, 2025a)، وأعلن رئيس الوزراء خطة حكومية للذكاء الاصطناعي والاقتصاد الرقمي في نيسان/أبريل 2026 (Al-Quds, 2026)، وعقد معهد فلسطين لأبحاث الأمن القومي مؤتمره الأول للأمن السيبراني والذكاء الاصطناعي في أيار/مايو 2026 (جامعة بيرزيت، 2026). فالسؤال لم يعد هل سيدخل الذكاء الاصطناعي في الأمن الوطني الفلسطيني، بل كيف، وبأي كلفة من التبعية.

2. مشكلة الدراسة وموقعها من الأدبيات

يتيح الذكاء الاصطناعي للفاعل محدود الموارد أن يردم جزءاً من فجوته الأمنية بكلفة معقولة، لأن كثيراً من النماذج والأدوات بات مفتوح المصدر، لكن الطريق إلى ذلك يمر عادةً ببنى يملكها غيره: سحابة أجنبية، ونماذج مغلقة عبر واجهات برمجية، ومعدات لا تدخل إلا بإذن. ونسمي هذا التوتر «مفارقة القدرة والتبعية».

ولا تحل الأدبيات المتاحة هذه المفارقة. فأغلب ما كُتب في الذكاء الاصطناعي والأمن الوطني يدور حول تنافس القوى الكبرى (Horowitz, 2018؛ Scharre, 2023)، وأدبيات السيادة الرقمية تفترض دولة تبسط سلطتها على إقليمها (Couture & Toupin, 2019؛ Pohle & Thiel, 2020)، وأدبيات «الاستعمار الرقمي» تشرح علاقات الهيمنة التقنية (Kwet, 2019) دون أن تقدم أداة لتقييم قرار شراء أو تشغيل بعينه. وقد وثّقت الأدبيات الفلسطينية القيود على البنية التحتية (Tawil-Souri, 2012؛ Tawil-Souri & Aouragh, 2014؛ World Bank, 2021)، وبيّن Cristiano (2019) أن

فكرة الفضاء السيبراني الوطني المطابق للإقليم لا تصمد في الفضاء الفلسطيني المجزأ. لكننا لم نجد دراسة تقيّم الفرص الأمنية للذكاء الاصطناعي في فلسطين ومخاطر التبعية الناتجة عنها بمعايير موحدة.

ومن هنا السؤال الرئيسي: ما الفرص التي يتيحها الذكاء الاصطناعي لبناء القدرة الأمنية الفلسطينية، وما مخاطر التبعية المترتبة عليها، وكيف يُوازَن بينهما؟ وتتفرع عنه ثلاثة أسئلة: أي الاستخدامات أجدى وأقل إنتاجاً للتبعية؟ وأي المخاطر مفروض من الخارج وأيها قابل للتأثير من الداخل؟ وبأي معايير تُقبل تبعية ما أو تُرفض؟ وتختبر الورقة افتراضين: أن أجدى الفرص هي الدفاعية منخفضة التبعية بشرط أن تستند إلى مؤسسة قائمة وإطار قانوني يحمي الحقوق، وأن التبعية في الطبقات العليا اختيارية في الأصل لكنها تصير مفروضة فعلياً متى تعذّر الخروج منها.

3. المنهجية وحدود الدراسة

تتبع الورقة تصميم دراسة الحالة المفردة (Yin, 2018)، وتختار فلسطين بمنطق الحالة الحدّية التي يبلغ فيها متغير ما حداً غير مألوف فتنكشف آليات تظل مستترة في الحالات العادية (Seawright & Gerring, 2008)؛ والتعميم المقصود تحليلي لا إحصائي. وتقوم البيانات على التحليل الوثائقي وحده (Bowen, 2009): نصوص تشريعية واتفاقيات، ووثائق حكومية، وتقارير مؤسسات دولية ومنظمات حقوقية، ودراسات محكّمة، وتصريحات منشورة للشركات. ولأن بعض الوقائع الأمنية لا يمكن التحقق منه من مصادر مفتوحة، صُنّفت الأدلة في خمسة مستويات يُشار إليها عند الادعاءات الحساسة: (أ) وثيقة رسمية أو إقرار من الجهة المعنية، و(ب) تقرير حقوقي أو تحقيق صحفي ذو منهجية معلنة، و(ج) دراسة محكّمة أو تقرير بحثي مؤسسي، و(د) تقدير ثانوي غير مؤكد، و(هـ) حكم تحليلي للباحث.

وللمنهجية حدوده: فما لا يُنشر عن المؤسسات الأمنية يبقى خارج التحليل، وقد تكون بعض القدرات القائمة أكبر مما يظهر هنا، أما أحكام الجدوى والتبعية في مصفوفة الفرص والمخاطر فتقوم على سلّم تصنيف معلن في (القسم 8)، وتبقى تقدير الباحث إلى أن تُحكَّم وفق بروتوكول دلفي المبيَّن هناك، ويشمل النطاق الضفة الغربية بما فيها القدس وقطاع غزة، مع أن الفوارق بينهما تجعل بعض الأحكام صالحاً لإحداهما دون الأخرى.

4. الإطار المفاهيمي: سلسلتان وأربع طبقات

تنطلق التعريفات التقليدية للأمن الوطني من دولة تحمي إقليمها ومؤسساتها، وهذا لا يكفي في فلسطين، فبعض أوضح التهديدات الموثقة استهدف المجتمع لا الدولة. فحين اختُرقت هواتف ستة مدافعين فلسطينيين عن حقوق الإنسان ببرنامج «بيغاسوس» بين 2020 و2021، وهو ما كشفته منظمة Front Line Defenders وأكده مختبرا Citizen Lab والعفو الدولية (Citizen Lab & Amnesty International Security Lab, 2021)، كان المستهدف جزءاً من القدرة الوطنية بمعناها الواسع. لذلك نأخذ بمفهوم موسّع للأمن الوطني يضم المؤسسات والمجتمع المدني والأفراد (Buzan et al., 1998).

يخفض الذكاء الاصطناعي كلفة التنبؤ فترتفع قيمة ما يكمّله من بيانات وحكم بشري (Agrawal et al., 2018؛ Goldfarb & Lindsay, 2022). فالقدرة الأمنية القائمة عليه سلسلة: بنية اتصال وحوسبة، فبيانات، فنماذج، فكفاءات تفهمها، فمؤسسة تحوّل المخرجات إلى قرار، فقواعد تحكم ذلك كله. ولكل حلقة مورّد، فإذا كان خارجياً نشأت إلى جانب سلسلة القدرة سلسلة

تبعية موازية. وتمتد السلسلتان عبر أربع طبقات: المادية (الشبكات والطيف والمعدات والحوسبة)، والبيانات، والخوارزميات، والقواعد (القوانين والعقود وضوابط التصدير). وتقترب هذه القسمة من النماذج الطبقية المعروفة للفضاء السيبراني، كنموذج Choucri وClark (2019) الذي يتدرج من التقنية المادية إلى المعلومات والمستخدمين، غير أن إطارنا يضيف طبقة القواعد ويقرأ كل طبقة موضعاً محتملاً للتبعية، وهو أقرب بذلك إلى ما يسميه المؤلفان «تحليل نقاط التحكم».

وليست التبعية خطراً في ذاتها، بل قد تكون مصدر مرونة: فنقل أوكرانيا بياناتها الحكومية إلى سحابة خارج حدودها في الأيام الأولى للحرب عام 2022 هو ما أبقى مؤسساتها عاملة (Amazon, 2022). تصير التبعية خطراً حين يملك المورّد، أو من له سلطة عليه، قدرة على قطع الخدمة أو الاطلاع على ما يمر عبرها أو التلاعب بمخرجاتها أو جعل الخروج منها مكلفاً إلى حد الارتهان (Opara-Martins et al., 2016). ولقياس ذلك نعتمد خمسة معايير للتبعية المُدارة (الجدول 1). والأربعة الأولى ليست جديدة؛ فهي حاضرة في أدبيات الارتهان للمورّد وقريبة مما اعتمدته المفوضية الأوروبية في إطارها لتقييم سيادة الخدمات السحابية (European Commission, 2025). أما الخامس، اتجاه التبعية، فهو ما تضيفه الحالة الفلسطينية، وفيه المساهمة المفاهيمية للورقة.

جدول 1: معايير التبعية المُدارة

الرمز	المعيار	السؤال العملي	تبعية مُدارة	تبعية غير مُدارة
R1	قابلية الاستبدال	هل يوجد بديل يمكن الانتقال إليه خلال مدة معقولة؟	عدة مزودين وصيغ بيانات قياسية	مزود وحيد وصيغ خاصة
R2	قابلية التدقيق	هل يمكن فحص طريقة عمل النظام واختباره محلياً؟	نموذج مفتوح الأوزان وتقارير اختبار مستقلة	صندوق أسود عبر واجهة برمجية فقط
R3	كلفة الخروج	كم يكلف الانتقال إلى بديل مالياً وزمنياً؟	كلفة منخفضة وخطة خروج موثقة	كلفة مرتفعة ولا خطة
R4	الولاية القانونية	لأي قانون تخضع البيانات، ومن يستطيع إلزام المزود بكشفها؟	ولاية الفاعل أو ولاية صديقة بضمانات مكتوبة	ولاية قد تكون معادية أو بلا ضمانة
R5	اتجاه التبعية	هل المورّد طرف محايد أم طرف في الصراع؟	مورّد محايد أو متعدد الجنسيات	طرف في الصراع أو خاضع لسلطته

فاعتماد دولة على مزود سحابي تحكمه قوانين دولة حليفة شيء، ومرور الاتصالات عبر طبقة مادية يتحكم فيها طرف في الصراع شيء آخر؛ ففي الحالة الثانية لا يحتاج أثرا المراقبة ونقطة الاختناق اللذان وصفهما Farrell وNewman (2019) إلى قرار استثنائي، لأنهما قائمان في بنية العلاقة نفسها.

5. السياق الفلسطيني: بنية رقمية تحت القيد

يلخص الجدول 2 أبرز المؤشرات، ويتضح منه أن جزءاً معتبراً من الضعف يقع خارج الطبقة المادية. ويبيّن العمود الأخير «مستوى الدليل» درجة موثوقية المصدر وفق السلّم المعرَّف في القسم 3، من (أ) للوثيقة الرسمية إلى (هـ) لحكم الباحث، ويُذكر مستويان حين يستند المؤشر إلى مصدرين مختلفين.

جدول 2: مؤشرات مختارة عن البيئة الرقمية والأمنية الفلسطينية (حتى تشرين الأول/أكتوبر 2026)

الطبقة	المؤشر والوضع	المصدر	مستوى الدليل
المادية	الترددات وإدخال المعدات وربط الشبكات مرهونة بموافقة إسرائيلية؛ الجيل الرابع في الضفة بموافقة صدرت في كانون الثاني/يناير 2026، وغزة على الجيل الثاني	Interim Agreement (1995)؛ Reuters (2026)	أ، ب
المادية	غزة (أيلول–تشرين الأول 2025): 11% فقط ممن أعمارهم 10 سنوات فأكثر وصلوا إلى الإنترنت بصورة دائمة، و29% لم يصلوا إليه إطلاقاً	الجهاز المركزي للإحصاء الفلسطيني وآخرون (2026)	أ
البيانات	منصة «زنّار» المبنية على X-Road لتبادل البيانات بين الجهات الحكومية؛ 71 من 100 في مؤشر جرد البيانات المفتوحة	e-Governance Academy (n.d.)؛ Demaidi (2025b)	أ، ج
الخوارزميات	1,867 منشوراً في الذكاء الاصطناعي حتى 2023؛ خمسة مراكز بيانات؛ مدونة «كُرّاس» المشروحة للهجة الفلسطينية	Demaidi (2025b)؛ Jarrar et al. (2017)	ج
القواعد	لا قانون شاملاً نافذاً لحماية البيانات؛ مسودة قرار بقانون بلغت القراءة الثالثة عام 2022 وما تزال قيد النقاش؛ قرار لمجلس الوزراء عام 2019 بشأن البيانات الشخصية للمواطنين	7amleh (2023)؛ قرار مجلس الوزراء رقم (3) لسنة 2019	ب، أ
القواعد	الفئة الرابعة في مؤشر الأمن السيبراني العالمي 2024؛ استراتيجية وطنية للذكاء الاصطناعي (2023)	International Telecommunication Union (2024)؛ Ministry of Telecommunications and Digital Economy (2023)	أ

ونقف عند ملاحظتين. الأولى أن أرقام غزة تصف بيئة لا يصح فيها افتراض الاتصال أصلاً، فقد أفاد 97% ممن واجهوا صعوبات في استخدام الإنترنت بانقطاعات مستمرة (الجهاز المركزي للإحصاء الفلسطيني وآخرون، 2026). والثانية أن جانباً كبيراً من الفجوة يقع في طبقة القواعد التي تملك المؤسسات الفلسطينية أن تتحرك فيها: فقد رصدت دراسة حديثة فجوات قانونية وتنظيمية وضعفاً في التحقيق الجنائي الرقمي، وأوصت بإنشاء هيئة وطنية للأمن السيبراني (Atrash et al., 2025). أما القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية فقد انتقدت منظمات حقوقية مسودته قبل إقرارها لاتساع الصلاحيات وغموض التعريفات (Amnesty International et al., 2017).

6. فرص بناء القدرة

6.1 الأمن السيبراني الدفاعي: المؤسسة قبل الأداة

هذا من أنضج المجالات، وكثير من أدواته مفتوح المصدر يعمل محلياً. لكن النموذج يعمل داخل مؤسسة ولا يصنعها، ولذلك فالفرصة الأولى ليست تقنية، بل إنشاء مركز وطني للاستجابة للحوادث وعمليات الأمن، أو تفعيله إن كان قائماً بصورة غير معلنة، يبدأ بالجهات المرتبطة بمنصة «زنّار» ثم يتسع إلى المصارف ومشغلي الاتصالات والكهرباء والمياه. ودور الذكاء الاصطناعي فيه أكثر تواضعاً مما توحي به المواد الترويجية: فمحللو مراكز العمليات يشكون من كثرة الإنذارات الكاذبة لا من قلة ما يُكتشف (Alahmadi et al., 2022)، فتكون القيمة الأولى للنماذج فرز التنبيهات وربطها.

أما كشف الشذوذ فيحتاج إلى حذر، لأن أخطاء منهجية كتسرب بيانات الاختبار إلى التدريب شائعة في هذا الحقل (Arp et al., 2022)، فلا يُعتمد نظام قبل تقييمه على بيانات فلسطينية.

وثمة أدوات منخفضة الكلفة والتبعية معاً: منصة MISP لتبادل مؤشرات التهديد مفتوحة المصدر وتعمل على خوادم محلية ويحدد أعضاؤها مستويات المشاركة (Wagner et al., 2016)، ونظام EPSS يقدّر احتمال استغلال الثغرات ونتائجه متاحة مجاناً (Jacobs et al., 2021)، فترتب المؤسسة معالجة ثغراتها دون إرسال أي بيانات عن أنظمتها. في المقابل، تبقى القرارات واسعة الأثر، كعزل نظام حكومي، بيد الإنسان، لأن الأنظمة القائمة على التعلم الآلي قابلة للخداع بمدخلات مصممة أو بتسميم بيانات تدريبها (Vassilev et al., 2024)، والمهاجم الذي يعرف أن النظام يعزل الأجهزة تلقائياً قد يعطّل المؤسسة بيدها.

6.2 البيانات الحكومية واستمرارية المؤسسات ودعم القرار

يقوم تصميم X-Road الذي بُنيت عليه منصة «زنّار» على توقيع الرسائل وختمها زمنياً وحفظ سجل بها (Nordic Institute for Interoperability Solutions, 2021)، فهو ينتج بطبيعته بيانات عمّن طلب ماذا ومتى. ورصد الأنماط غير المعتادة فيها يكشف الاختراق الخارجي وإساءة الاستخدام من الداخل معاً، فيحمي المؤسسةَ ويحمي المواطن منها (المستوى هـ). أما استمرارية المؤسسات فمعضلتها أصعب: حفظ نسخ من سجلات الأحوال المدنية والأراضي خارج الإقليم يحميها من التدمير لكنه يضعها تحت ولاية أجنبية. ولا نرى حلاً كاملاً، لكن المخاطر تقل بتشفير النسخ بمفاتيح فلسطينية وتوزيعها على أكثر من ولاية، وباتفاقيات بين الدول بدل عقد مع مورّد واحد. أي أن بعض أهم الفرص لا يمكن أن يكون منخفض التبعية أصلاً، والمعيار المناسب له إدارة التبعية لا خفضها.

وفي دعم القرار، ما يُسوَّق تنبؤاً بالسلوك البشري هو غالباً استقراء لأنماط ماضية يحمل تحيزات بياناتها (Lum & Isaac, 2016). لذلك نقترح هدفاً أكثر تواضعاً: معرفة ما يجري الآن بسرعة أكبر، كمؤشرات مجمّعة من البيانات الإدارية، أو تقدير الأضرار من صور الأقمار الصناعية. ونحذّر من شراء أنظمة تنبؤ أمني مغلقة تدّعي تحديد الأفراد «الخطرين»: جدواها مشكوك فيها، وهي لا تقبل التدقيق، وتُطبَّق على السكان أنفسهم.

6.3 الموارد اللغوية والنماذج المفتوحة: ميزة نسبية

لو اخترنا فرصة واحدة تجمع الجدوى وانخفاض التبعية لكانت الموارد اللغوية العربية والفلسطينية؛ فالشركات الكبرى لا تملك حافزاً قوياً للاستثمار في لهجة يتكلمها بضعة ملايين، وبناء هذه الموارد يحتاج إلى معرفة باللغة والسياق أكثر مما يحتاج إلى حوسبة ضخمة. وثمة أساس قائم: مدونة «كُرّاس» المشروحة للهجة الفلسطينية (Jarrar et al., 2017)، ونماذج عربية مفتوحة مثل AraBERT (Antoun et al., 2020) وJais (Sengupta et al., 2023)، يمكن تكييفها وتشغيلها محلياً لتصنيف الوثائق الحكومية وكشف رسائل التصيد المكتوبة بلهجة محلية. ولهذه القدرة وظيفة أهم هي تدقيق الأنظمة المستوردة، بعد أن ثبت إفراط أنظمة Meta في الإشراف على المحتوى العربي والفلسطيني (BSR, 2022؛ Human Rights Watch, 2023).

6.4 الكفاءات وحماية المجتمع المدني

يتوقف كل ما سبق على الكفاءات، والمشكلة ليست غياب الخريجين بل ندرة من يجمع الذكاء الاصطناعي بالأمن وهجرة من يتخصص فعلاً. غير أن كل قدرة دفاعية هي أيضاً قدرة على الرؤية؛ فمركز العمليات يرى حركة الشبكات، ونماذج تحليل النصوص قد تُوجَّه إلى التضليل الخارجي أو إلى مراقبة التعبير الداخلي. لذلك تُبنى الضمانات مع القدرة لا بعدها: أداة قانونية منشورة تحدد الصلاحيات، وحصر العمل في أمن الأنظمة دون المحتوى، وتسجيل وصول المركز نفسه إلى البيانات، ومراجعة مستقلة يشارك فيها المجتمع المدني (Necessary and Proportionate Coalition, 2014).

7. مخاطر التبعية الرقمية

7.1 الطبقة المادية: تبعية لطرف في الصراع

هذه أخطر التبعيات بمقياس المعيار الخامس، لأن تأخير ترقية الشبكات أو منع إدخال المعدات أو قطع الاتصال يجري ضمن ترتيبات قائمة دون حاجة إلى عقوبات دولية. وقد شهدت غزة خلال الحرب انقطاعات بلغ بعضها حد الانقطاع الشامل. وتُخفَّف آثارها بأنظمة حكومية تعمل محلياً عند الانقطاع ونسخ احتياطية موزعة جغرافياً.

7.2 الحوسبة والبرمجيات: حين تتغير سياسة دولة المورّد

لا أحد يُلزم المؤسسات الفلسطينية بمزود سحابي بعينه، لكن الاختيار الحر قد يصير قيداً. ففي أيار/مايو 2025 أفادت وكالة أسوشيتد برس بأن المدعي العام للمحكمة الجنائية الدولية فقد الوصول إلى بريده لدى Microsoft بعد العقوبات الأمريكية عليه (Quell, 2025؛ المستوى ب)، ونفت الشركة إيقاف خدماتها عن المحكمة لكنها أقرت بتواصلها معها طوال العملية التي انتهت بفصله عن خدماتها (Krempl, 2025؛ المستوى أ)، ثم أكدت المحكمة في تشرين الأول/أكتوبر 2025 انتقالها إلى حزمة مكتبية أوروبية مفتوحة المصدر (Jennings-Trace, 2025). والحالة قريبة من فلسطين: ففي أيلول/سبتمبر 2025 فرضت الولايات المتحدة عقوبات على مؤسسة الحق ومركز الميزان والمركز الفلسطيني لحقوق الإنسان بسبب تعاونها مع المحكمة (Kane, 2025)، والحظر يشمل من حيث المبدأ الشركات الأمريكية التي تقدم البريد والتخزين السحابي (المستوى هـ).

وتتراكم هذه المخاطر بهدوء فيما يُسمى الارتهان للمورّد (Opara-Martins et al., 2016). وهنا يتأكد الافتراض الثاني: التبعية المختارة تبقى اختيارية ما دام الخروج ممكناً، وما لا خروج منه يصير مفروضاً.

7.3 الخوارزميات والبيانات

تجتمع في الحالة الفلسطينية مصادر الغموض الثلاثة التي ميّزتها Burrell (2016): السرية التجارية، ونقص المعرفة التقنية، والغموض الناتج عن طبيعة التعلم الآلي. والتحيز ليس احتمالاً نظرياً؛ ففي تشرين الأول/أكتوبر 2023 اعتذرت Meta بعد أن أدرجت الترجمة الآلية في Instagram كلمة «إرهابيين» في ملفات مستخدمين فلسطينيين تضمنت عبارة دينية شائعة (Arab News, 2023)، ووجد Naous وزملاؤه (2024) أن النماذج اللغوية الكبيرة تميل إلى المرجعيات الغربية حتى حين تُسأل بالعربية. فالنموذج المستورد الذي يُستعمل دون اختبار محلي يأتي معه منظور لا يفهم السياق،

ولأن النماذج المتاحة عبر الواجهات الخارجية تتغير دون إشعار يصبح التدقيق عملاً مستمراً، ومن هنا قيمة النماذج مفتوحة الأوزان.

وفي البيانات ثلاث مسائل: بيانات عن الفلسطينيين لا يملكونها ولا يعلمون بوجودها (Smith, 2025)؛ والتسرب عبر الأدوات اليومية، كما حين منعت Samsung موظفيها من أدوات الذكاء الاصطناعي التوليدي بعد إدخال بعضهم شيفرة حساسة فيها (Gurman, 2023)، ففي غياب سياسة حكومية معلنة يصبح كل موظف يلخص مذكرة رسمية بأداة مجانية نقطة تسرب محتملة (المستوى هـ)؛ وغياب قانون نافذ لحماية البيانات يحرم المواطن من معرفة ما تحتفظ به المؤسسات عنه وإلى أين يُنقل (7amleh, 2022)، ويتضاعف الخطر مع كل ربط جديد للبيانات قبل صدوره.

7.4 الفجوة في الكفاءات بوصفها تبعية

النظام الذي لا يوجد من يفهمه محلياً صندوق أسود ولو كانت شيفرته مفتوحة، والمؤسسة التي لا تملك مهندسين قادرين على نقل أنظمتها إلى بديل مرتهنة لمورّدها مهما كانت شروط عقدها. فالفجوة في الكفاءات تبعية قائمة بذاتها، لكنها داخلية في معظمها، فهي من أخطر التبعيات وأكثرها قابلية للعلاج في آن.

8. مصفوفة الفرص والمخاطر

ولكي لا يبقى التصنيف حكماً عاماً، اتبعنا منطق التقييم شبه الكمي المعتمد في المعيار الدولي ISO 31000، الذي يعرّف الخطر بأنه أثر عدم اليقين في الأهداف سلبياً كان أو إيجابياً (International Organization for Standardization, 2018)، وفي دليل NIST لتقييم المخاطر (Joint Task Force Transformation Initiative, 2012). فأعطينا كل استخدام درجتين: درجة الفرصة (O) من ثلاثة معايير، ودرجة الخطر والتبعية (R) من معايير الجدول 1 الخمسة مضافاً إليها الأثر على الحقوق (H)، مع قاعدة قيد تعامل كل استخدام يبلغ الدرجة القصوى في H معاملة الخطر المرتفع أياً كان مجموعه. ويعرض الجدول 3 الدرجات التفصيلية والموقع الناتج لكل استخدام.

جدول 3: مصفوفة الفرص والمخاطر وفق سلّم شبه كمي (O: درجة الفرصة من 9؛ R: درجة الخطر والتبعية من 12)

الرمز	الاستخدام	O1	O2	O3	O	R1	R2	R3	R4	R5	H	R	الموقع
U01	مركز وطني للاستجابة بأدوات مفتوحة المصدر	3	3	3	9	0	0	0	0	1	1	2	ابدأ الآن
U02	منصة وطنية لتبادل مؤشرات التهديد (MISP)	3	3	2	8	0	0	0	0	1	0	1	ابدأ الآن
U03	ترتيب معالجة الثغرات بتقديرات EPSS	3	3	2	8	0	0	0	0	0	0	0	ابدأ الآن
U04	رصد أنماط الوصول في سجلات «زنّار»	3	2	3	8	0	0	0	0	1	1	2	ابدأ الآن
U05	مسار جامعي يجمع الذكاء الاصطناعي بالأمن السيبراني	2	3	3	8	0	0	0	0	0	0	0	ابدأ الآن
U06	حلول أمنية سحابية تجارية	3	3	3	9	1	2	2	2	1	1	9	أدِر بشروط
U07	نماذج لغوية تجارية عبر واجهات خارجية	3	3	2	8	1	2	1	2	1	1	8	أدِر بشروط

الرمز	الاستخدام	O1	O2	O3	O	R1	R2	R3	R4	R5	H	R	الموقع
U08	نسخ البيانات السيادية خارج الإقليم	2	3	3	**8**	1	1	1	2	1	1	**7**	**أدِر بشروط**
U09	تقدير الأضرار من صور الأقمار الصناعية	2	2	3	**7**	1	1	1	2	1	0	**6**	**أدِر بشروط**
U10	ربط البيانات الإدارية لأغراض التحليل	2	2	3	**7**	0	0	1	0	0	2	**3**	**أدِر بشروط**
U11	نماذج عربية مفتوحة الأوزان تعمل محلياً	2	2	2	**6**	0	0	1	0	0	0	**1**	**استثمر تدريجياً**
U12	عنقود حوسبي وطني مشترك	1	3	2	**6**	1	0	1	0	2	0	**4**	**استثمر تدريجياً**
U13	أنظمة تنبؤ أمني مغلقة جاهزة	1	1	2	**4**	2	2	2	1	1	2	**10**	**تجنّب**

المفتاح: O1 الجدوى بالموارد المتاحة، وO2 النضج التقني، وO3 الأثر الأمني (من 1 إلى 3 لكل منها)؛ R1–R5 معايير الجدول 1، وH الأثر على الحقوق (من 0 إلى 2 لكل منها). الحدود: O ≤ 7 فرصة مرتفعة، وR ≤ 6 أو H = 2 خطر مرتفع. الألوان وفق اصطلاح خرائط الحرارة (أخضر، أصفر، أحمر) في ISO 31000 و.NIST SP 800-30

وتُظهر المصفوفة أن ما يمكن البدء به الآن يتركز في أدوات متواضعة (U01–U05)، وأن موقع «أدِر بشروط» هو الأكثر عدداً والأصعب لأن شروطه تحتاج إلى مؤسسات وتشريعات ومفاوضات. وبهذا يجد الافتراض الأول دعماً مع تعديلين: الفرصة الدفاعية تبقى نظرية ما لم تستند إلى مؤسسة عاملة وقانون للبيانات، وبعض أهم الفرص لا يمكن خفض تبعيته فيكون المعيار إدارتها.

وتبقى هذه الدرجات تقدير الباحث (المستوى هـ) إلى أن تُحكَّم ببروتوكول دلفي من جولتين وفق إرشادات Okoli وPawlowski (2004): لجنة من 10 إلى 15 خبيراً من القطاعات الحكومية والأكاديمية والخاصة والمجتمع المدني، يقدّر كلٌّ منهم باستقلال، ثم يُطلَعون على الوسيط والمدى الربيعي لكل بند فيعيدون التقدير. ويتحقق الإجماع إذا لم يتجاوز المدى الربيعي درجة واحدة، وتُعرض البنود التي لا إجماع فيها بوصفها مواضع خلاف لا أحكاماً.

9. التوصيات

الأولويات الخمس الأولى في الجدول 4 قصيرة الأجل وضمن الصلاحيات الفلسطينية، وتنفيذها ينقل عدداً من الاستخدامات من «أدِر بشروط» إلى «ابدأ الآن». ويضاف إليها ألا تتعاقد مؤسسة حكومية على خدمة حيوية قبل أن تجيب كتابةً عن أسئلة الجدول 1.

جدول 4: الأولويات المقترحة

الأولوية	الجهة المعنية أساساً	الأفق	موافقة خارجية؟
قانون لحماية البيانات الشخصية بعد تشاور عام، مع جهة رقابة مستقلة	مجلس الوزراء ووزارة الاتصالات والاقتصاد الرقمي	قصير	لا
فريق أولي لمركز وطني للاستجابة، بأداة قانونية منشورة تحصر عمله في أمن الأنظمة	وزارة الاتصالات والاقتصاد الرقمي وجهات «زنّار»	قصير	لا
سجل وطني لمخاطر التبعية يقيّم كل خدمة حيوية بالمعايير الخمسة ويُلزم بخطة خروج	مجلس الوزراء والمؤسسات الحكومية	قصير	لا

الأولوية	الجهة المعنية أساساً	الأفق	موافقة خارجية؟
سياسة معلنة لاستخدام الذكاء الاصطناعي في القطاع العام تقوم على تصنيف البيانات: عامة، وداخلية، وشخصية حساسة، وسيادية	وزارة الاتصالات والاقتصاد الرقمي	قصير	لا
مسار جامعي يجمع الذكاء الاصطناعي بالأمن السيبراني، مرتبط بالمركز الوطني	الجامعات ووزارة التعليم العالي	قصير إلى متوسط	لا
مختبر لتقييم الأنظمة المستوردة على بيانات محلية، وموارد لغوية فلسطينية لأغراض الأمن	الجامعات ومراكز البحث	متوسط	لا
نسخ مشفرة من البيانات السيادية في أكثر من ولاية، باتفاقيات بين الدول	الحكومة بالتعاون مع دول صديقة	متوسط	نعم
عنقود حوسبي وطني مشترك للجامعات والمؤسسات العامة	الحكومة والجامعات والمانحون	متوسط	نعم
السيطرة على الطيف وإدخال المعدات وإعادة بناء شبكات غزة	القيادة السياسية في المحافل الدولية	طويل	نعم

10. الخاتمة

انتهت الورقة إلى أن فرص الذكاء الاصطناعي في بناء القدرة الأمنية الفلسطينية حقيقية، لكنها أضيق مما يوحي به الخطاب العام وأشد ارتباطاً بالمؤسسات مما يوحي به الحديث عن التقنية؛ فأجداها يحتاج إلى قرارات أكثر مما يحتاج إلى حوسبة: مركز يُنشأ، وقانون يصدر، وسياسة تُعلن. أما المخاطر فصنفان: مفروضة، كالتبعية المادية لطرف في الصراع والعقوبات التي بدأت تطال مؤسسات فلسطينية؛ وقابلة للتأثير، كنقص الكفاءات وغياب قانون البيانات والتسرب عبر الأدوات اليومية.

وتتمثل مساهمة الورقة في إضافة معيار اتجاه التبعية إلى معايير التبعية المُدارة، وفي بيان أن الحد بين التبعية المفروضة والاختيارية لا يتبع الطبقات بدقة، ما يجعل الاستثمار في القدرة على الخروج، أي في البدائل المفتوحة والصيغ القياسية والكفاءات المحلية، جزءاً من بناء القدرة نفسه. ونقترح للبحث اللاحق إجراء جولتي دلفي المقترحتين، وتطبيق المعايير الخمسة على عينة من الخدمات الحكومية الفعلية، واختبار الإطار على فاعلين آخرين بلا سيادة إقليمية كاملة.

المراجع

أولاً: المراجع العربية

جامعة بيرزيت. (2026، 20 أيار/مايو). *انطلاق مؤتمر فلسطين الأول للأمن السيبراني والذكاء الاصطناعي*. https://www.birzeit.edu/ar/news/ntlq-mwtmr-flstyn-lwl-llmn-lsybrny-wldhk-lstny

الجهاز المركزي للإحصاء الفلسطيني، ووزارة الاتصالات والاقتصاد الرقمي، وهيئة تنظيم قطاع الاتصالات. (2026، 17 أيار/مايو). *بيان صحفي مشترك بمناسبة اليوم العالمي للاتصالات ومجتمع المعلومات*. https://www.pcbs.gov.ps/media/yilp0kme/wictday2026a.pdf

القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية. (2018). *الوقائع الفلسطينية*.

قرار مجلس الوزراء رقم (3) لسنة 2019 بالبيانات الشخصية الخاصة بالمواطنين. (2019). منصة مقام، جامعة النجاح الوطنية. https://maqam.najah.edu/legislation/247/

ثانياً: المراجع الأجنبية

7amleh. (2022, June 20). *Privacy and personal data protection in Palestine: Double violations and absent legislation*. https://7amleh.org/post/privacy-and-personal-data-protection-in-palestine

7amleh. (2023, October 3). *Position paper: Personal data protection draft law by decree from a human rights–based perspective*. https://7amleh.org/post/1227

Abraham, Y. (2024, April 3). 'Lavender': The AI machine directing Israel's bombing spree in Gaza. *+972 Magazine*.

Agrawal, A., Gans, J., & Goldfarb, A. (2018). *Prediction machines: The simple economics of artificial intelligence*. Harvard Business Review Press.

Alahmadi, B. A., Axon, L., & Martinovic, I. (2022). 99% false positives: A qualitative study of SOC analysts' perspectives on security alarms. In *Proceedings of the 31st USENIX Security Symposium*. USENIX Association. https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi

Al-Quds. (2026, April 28). *Mustafa launches national plan to boost AI and digital economy in Palestine*. https://alquds.com/en/posts/237280

Amazon. (2022, June 9). *Safeguarding Ukraine's data to preserve its present and build its future*. https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

Amnesty International. (2023). *Automated apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT* (MDE 15/6701/2023).

Amnesty International, Avaaz, Human Rights Watch, & 7amleh. (2017, December 20). *Palestine: Reform restrictive cybercrime law. Amended draft better, but still short of international standards* (MDE 15/7632/2017). https://www.amnesty.org/en/documents/mde15/7632/2017/en/

Antoun, W., Baly, F., & Hajj, H. (2020). AraBERT: Transformer-based model for Arabic language understanding. In *Proceedings of the 4th Workshop on Open-Source Arabic Corpora and Processing Tools* (pp. 9–15). European Language Resources Association. https://aclanthology.org/2020.osact-1.2

Arab News. (2023, October 20). *Instagram issue apology for labeling some Palestinian user-profiles as 'terrorist'*. https://www.arabnews.com/node/2394891/media

Arp, D., Quiring, E., Pendlebury, F., Warnecke, A., Pierazzi, F., Wressnegger, C., Cavallaro, L., & Rieck, K. (2022). Dos and don'ts of machine learning in computer security. In *Proceedings of the 31st USENIX Security Symposium* (pp. 3971–3988). USENIX Association.

Atrash, A. J., Farajallah, M., Alsharif, I., & Shanti, N. R. (2025). Strategic gap analysis of Palestine cybersecurity performance in the context of GCI, Kingdom of Saudi Arabia cybersecurity posture and anti-cybercrime law, and Council of Europe convention. In *2025 Engineering for Palestine Conference (ENG4PAL)* (pp. 489–498). Palestine Polytechnic University. https://scholar.ppu.edu/handle/123456789/9387

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40.

BSR. (2022). *Human rights due diligence of Meta's impacts in Israel and Palestine in May 2021*. BSR.

Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1). https://doi.org/10.1177/2053951715622512

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner.

Choucri, N., & Clark, D. D. (2019). *International relations in the cyber age: The co-evolution dilemma*. MIT Press. https://doi.org/10.7551/mitpress/11334.001.0001

Citizen Lab & Amnesty International Security Lab. (2021, November 8). *Devices of Palestinian human rights defenders hacked with NSO Group's Pegasus spyware*. https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society, 21*(10), 2305–2322.

Cristiano, F. (2019). Deterritorializing cyber security and warfare in Palestine: Hackers, sovereignty, and the national cyberspace as normative. *CyberOrient, 13*(1), 28–42. https://doi.org/10.1002/j.cyo2.20191301.0002

Demaidi, M. N. (2025a). Artificial intelligence national strategy in a developing country. *AI & Society, 40*(2), 423–435. https://doi.org/10.1007/s00146-023-01779-x

Demaidi, M. N. (2025b). Palestine: Adapting the science landscape for artificial intelligence. In *Preparing national research ecosystems for AI* (2nd ed., pp. 89–93). International Science Council. https://council.science/wp-content/uploads/2025/02/AI-Paper-Case-Study-Palestine_V2.pdf

e-Governance Academy. (n.d.). *Palestine makes data move*. https://ega.ee/palestine-makes-data-move/

European Commission. (2025). *Cloud sovereignty framework* (Version 1.2.1). Directorate-General for Digital Services. https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44*(1), 42–79.

Goldfarb, A., & Lindsay, J. R. (2022). Prediction and judgment: Why artificial intelligence increases the importance of humans in war. *International Security, 46*(3), 7–50.

Gurman, M. (2023, May 2). Samsung bans staff's AI use after spotting ChatGPT data leak. *Bloomberg*. https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review, 1*(3), 36–57.

Human Rights Watch. (2023, December 21). *Meta's broken promises: Systemic censorship of Palestine content on Instagram and Facebook*. https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and

Human Rights Watch. (2024, September 10). *Questions and answers: Israeli military's use of digital tools in Gaza*. https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza

International Telecommunication Union. (2024). *Global cybersecurity index 2024* (5th ed.). ITU. https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

International Organization for Standardization. (2018). *Risk management: Guidelines* (ISO Standard No. 31000:2018).

Israel Defense Forces. (2024, April 3). Israel Defence Forces' response to claims about use of 'Lavender' AI database in Gaza [Statement]. *The Guardian*.

Israeli–Palestinian Interim Agreement on the West Bank and the Gaza Strip. (1995). Annex III: Protocol concerning civil affairs, Appendix 1, Article 36.

Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I., & Roytman, M. (2021). Exploit prediction scoring system (EPSS). *Digital Threats: Research and Practice, 2*(3), Article 20.

Jarrar, M., Habash, N., Alrimawi, F., Akra, D., & Zalmout, N. (2017). Curras: An annotated corpus for the Palestinian Arabic dialect. *Language Resources and Evaluation, 51*(3), 745–775. https://doi.org/10.1007/s10579-016-9370-7

Jennings-Trace, E. (2025, October 31). The International Criminal Court is ditching Microsoft software for an open source alternative. *TechRadar*. https://www.techradar.com/pro/the-international-criminal-court-is-ditching-microsoft-software-for-an-open-source-alternative

Kane, A. (2025, September 22). The consequences of new US sanctions on Palestinian human rights groups. *Jewish Currents*. https://jewishcurrents.org/the-consequences-of-new-us-sanctions-on-palestinian-human-rights-groups

Krempl, S. (2025, June 5). Microsoft denies mail blockade at the International Criminal Court. *heise online*. https://www.heise.de/en/news/Microsoft-denies-mail-blockade-at-the-International-Criminal-Court-10429628.html

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class, 60*(4), 3–26. https://doi.org/10.1177/0306396818823172

Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19.

Ministry of Telecommunications and Digital Economy. (2023). *Palestinian national strategy for artificial intelligence*. State of Palestine.

Naous, T., Ryan, M. J., Ritter, A., & Xu, W. (2024). Having beer after prayer? Measuring cultural bias in large language models. In *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)* (pp. 16366–16393). Association for Computational Linguistics. https://doi.org/10.18653/v1/2024.acl-long.862

Necessary and Proportionate Coalition. (2014). *International principles on the application of human rights to communications surveillance*. https://necessaryandproportionate.org/principles/

Nordic Institute for Interoperability Solutions. (2021, September 29). *Message logging in X-Road 7*. https://www.niis.org/blog/2021/9/29/message-logging-in-x-road-7

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management, 42*(1), 15–29. https://doi.org/10.1016/j.im.2003.11.002

Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. *Journal of Cloud Computing, 5*, Article 4.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4). https://doi.org/10.14763/2020.4.1532

Quell, M. (2025, May 15). Trump's sanctions on ICC's chief prosecutor have halted tribunal's work, officials and lawyers say. *Associated Press*. https://www.pbs.org/newshour/world/trumps-sanctions-on-iccs-chief-prosecutor-have-halted-tribunals-work-officials-and-lawyers-say

Reuters. (2026, January 6). Israel approves upgrade to 4G mobile services to Palestinians in West Bank. *Al-Monitor*. https://www.al-monitor.com/originals/2026/01/israel-approves-upgrade-4g-mobile-services-palestinians-west-bank

Scharre, P. (2023). *Four battlegrounds: Power in the age of artificial intelligence*. W. W. Norton.

Seawright, J., & Gerring, J. (2008). Case selection techniques in case study research: A menu of qualitative and quantitative options. *Political Research Quarterly, 61*(2), 294–308.

Sengupta, N., Sahu, S. K., Jia, B., Katipomu, S., Li, H., Koto, F., Marshall, W., Gosal, G., Liu, C., Chen, Z., Afzal, O. M., Kamboj, S., Pandit, O., Pal, R., Pradhan, L., Mujahid, Z. M., Baali, M., Han, X., Bsharat, S. M., . . . Xing, E. (2023). *Jais and Jais-chat: Arabic-centric foundation and instruction-tuned open generative large language models* (arXiv:2308.16149). arXiv. https://arxiv.org/abs/2308.16149

Smith, B. (2025, September 25). *Update on ongoing Microsoft review*. Microsoft On the Issues. https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/

Tawil-Souri, H. (2012). Digital occupation: Gaza's high-tech enclosure. *Journal of Palestine Studies, 41*(2), 27–43. https://doi.org/10.1525/jps.2012.XLI.2.27

Tawil-Souri, H., & Aouragh, M. (2014). Intifada 3.0? Cyber colonialism and Palestinian resistance. *Arab Studies Journal, 22*(1), 102–133.

Vassilev, A., Oprea, A., Fordyce, A., & Anderson, H. (2024). *Adversarial machine learning: A taxonomy and terminology of attacks and mitigations* (NIST AI 100-2e2023). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-2e2023

Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). MISP: The design and implementation of a collaborative threat intelligence sharing platform. In *Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security* (pp. 49–56). ACM. https://doi.org/10.1145/2994539.2994542

World Bank. (2021). *Palestinian digital economy assessment*. World Bank.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage.

معهد فلسطين لأبحاث الأمن القومي
Palestine Institute for National Security Research