

# Ver el mundo como una Palestina

Luchas interseccionales contra  
las Big Tech y el apartheid de Israel



*Apoorva PG*

TRADUCCIÓN AL ESPAÑOL POR NURIA DEL VISO PABÓN  
ILUSTRACIÓN DE ANĐELA JANKOVIĆ



En mayo de 2021, mientras las fuerzas israelíes lanzaban una intensa oleada de ataques aéreos sobre la asediada Franja de Gaza –con el resultado de 256 víctimas palestinas y decenas de miles de heridos–, Google y Amazon Web Services (AWS) firmaron el Proyecto Nimbus, un contrato de 1.200 millones de dólares para proporcionar servicios en la nube al gobierno y al ejército israelíes. Las dos corporaciones proporcionarían de hecho la columna vertebral tecnológica de la ocupación israelí de los territorios palestinos. Ya están en marcha tres centros de datos para este proyecto. Amazon Web Services también proporcionó la plataforma en la nube para el programa espía Pegasus hasta que saltó la noticia sobre el Proyecto Pegasus, y sigue haciéndolo para la aplicación Blue Wolf, que permite a los soldados israelíes capturar imágenes de palestinos en toda la Cisjordania ocupada y luego cotejarlas con bases de datos militares y de inteligencia.

Este contrato, de un alcance y unas repercusiones sin precedentes, es solo una manifestación de los profundos vínculos entre Israel y las grandes empresas tecnológicas. Hewlett Packard Enterprise, por ejemplo, tenía un contrato exclusivo de 2017 a 2020 para suministrar servidores para la base de datos de población de Israel, que también se utilizó para determinar diversas formas de exclusión de los ciudadanos palestinos de Israel y los residentes de la Jerusalén Oriental ocupada. Las grandes tecnológicas han contribuido a sostener una ocupación basada en el control militar y la vigilancia perpetua, que los palestinos llevan décadas denunciando como una forma de *apartheid* y de *colonialismo de colonos*. Amnistía Internacional y otras organizaciones internacionales, el Relator Especial de la ONU sobre los derechos humanos en los Territorios Palestinos Ocupados (TPO) y un número creciente de gobiernos consideran que Israel está cometiendo el delito de *apartheid*.

La ubicuidad de la tecnología y el control digitales, junto con la monetización de los datos personales, han llevado a que los datos se conviertan en la nueva frontera del colonialismo. Comprender el papel de las grandes empresas tecnológicas en la consolidación de la violación de los derechos humanos de los palestinos por parte de Israel pone de relieve la urgente necesidad de hacer frente a este colonialismo global de los datos. Esto se debe tanto a que los métodos de represión probados contra los palestinos se están adoptando en todo el mundo como a que cuestionar a las grandes empresas tecnológicas, su connivencia con las agencias militares y de vigilancia y su robo de nuestros datos nos permite construir luchas interseccionales contra la matriz de opresión –militarización, capitalismo neoliberal y *apartheid* israelí– que las grandes empresas tecnológicas refuerzan y de la que se benefician.

Los profundos vínculos entre Israel y las grandes empresas tecnológicas han permitido un flujo bidireccional de beneficios, delitos y complicidad. Esto permite a Israel desplegar tecnología de rápida innovación desarrollada por empresas transnacionales e integrarla en su vigilancia, control y represión de la población palestina. Al mismo tiempo, la tecnología israelí desarrollada para controlar al pueblo palestino se pone a disposición de las empresas tecnológicas israelíes e internacionales para que la amplíen y exporten a otros países con fines represivos. Consideremos algunas de estas estadísticas recopiladas por la campaña palestina Stop the Wall en su informe *Digital Walls*:

- Durante las últimas décadas, más de 300 empresas multinacionales tecnológicas líderes establecieron centros de I+D en Israel, lo que representa alrededor del 50 % del gasto en I+D [investigación y desarrollo] de las empresas.
- Estas multinacionales han adquirido un total de 100 empresas israelíes. Algunas de ellas, como Intel, Microsoft, Broadcom, Cisco, IBM y EMC, han adquirido más de diez empresas locales durante el tiempo que llevan operando en Israel.

- Más de 30 unicornios tecnológicos –empresas emergentes valoradas en más de 1.000 millones de dólares– tienen su sede en Israel. Esto supone alrededor del 10 % de los unicornios del mundo.

Esta relación simbiótica impulsa la inversión de las grandes empresas tecnológicas en Israel y refuerza el crecimiento de la vigilancia y la tecnología digital militarizada, de la que Israel ha sido pionero, aunque no es el único.

### **‘Big Tech’ y guerras imperiales globales**

El contexto específico de las grandes corporaciones tecnológicas y el *apartheid* de Israel forma parte de una estructura de poder global de dominación, racismo y estados coercitivos. La tecnología digital incluye sistemas de vigilancia utilizados por primera vez por los militares, como sostiene el informe Digital Walls:

Ambos procesos –la digitalización y la militarización– no son solo desarrollos parcialmente paralelos en el tiempo. Están profundamente entrelazados: los primeros ordenadores surgieron de la Segunda Guerra Mundial e Internet fue desarrollado en la Guerra Fría por el ejército estadounidense. No es de extrañar que la tecnología, la investigación y la industria militares estén obteniendo enormes beneficios del inicio de la economía digital.

El Proyecto Maven del Pentágono ilustra cómo estos procesos y sus interrelaciones siguen creciendo a la par que las guerras globales e imperiales. Desde principios de 2000, el ejército estadounidense ha utilizado aviones no tripulados para atacar objetivos en otros países, causando también víctimas civiles. El Proyecto Maven está orientado a fomentar los ataques con aviones no tripulados mediante el análisis de imágenes de vigilancia con el uso de Inteligencia Artificial (IA). Google fue contratado inicialmente para este proyecto, pero se retiró a raíz de las objeciones de sus propios empleados. El contrato pasó entonces

a AWS y Microsoft, y desde entonces se ha transferido a la Agencia Nacional de Inteligencia Geoespacial de Estados Unidos (NGA).

El proyecto Big Tech Sells War, que ha seguido la senda de connivencia entre las empresas tecnológicas estadounidenses y la violencia antimusulmana y la islamofobia, señaló que “la Ley [Patriota] autoriza amplios poderes al Gobierno para vigilar a los estadounidenses e incluso detener indefinidamente a inmigrantes que no están acusados de delitos. Su aprobación abrió las puertas para que las grandes tecnológicas se convirtieran, ante todo, en intermediarias de nuestros datos personales, vendiéndolos a agencias gubernamentales y empresas privadas dentro y fuera del país y desencadenando la era de la economía de datos”. La Agencia de Seguridad Nacional de Estados Unidos (NSA), cuyo programa de vigilancia masiva sacó a la luz el ex contratista Edward Snowden, tuvo acceso a los servidores de Microsoft en septiembre de 2007; a los de Google en enero de 2009; a los de Facebook en junio de 2009; a los de YouTube en 2010; y a los de Apple en octubre de 2012, por mandato de las enmiendas a la Ley de Vigilancia de Inteligencia Extranjera, que desde entonces han sido reformadas.

Décadas de normalización de la vigilancia masiva, la introducción de ataques remotos con drones por parte del ejército estadounidense, y la construcción de muros y otros mecanismos de control fronterizo para impedir la entrada de inmigrantes han dependido de una tecnología en constante avance para clasificar, vigilar y atacar a las personas. Esta dinámica ha corrido paralela a la transformación de la gran tecnología en la industria multimillonaria que es hoy. Una cronología de ambas trayectorias –la evolución de las tecnologías de represión y el crecimiento de las grandes tecnológicas– puede encontrarse en la campaña Big Tech Sells War. En 2013, AWS consiguió su primer contrato en la nube en Estados Unidos con la CIA, la Agencia de Seguridad Nacional (NSA) y otras agencias de inteligencia estadounidenses. En abril de 2022, la NSA volvió a adjudicar a AWS un contrato (independiente) de 10.000 millones de dólares para servicios de computación en la nube. Microsoft protestó contra la obtención de este contrato por parte de AWS, sucesor del contrato Joint Enterprise

Defense Infrastructure (JEDI) IT, que Microsoft tenía en 2019. En marzo de 2021, Microsoft firmó para proporcionar gafas de realidad aumentada HoloLens al ejército estadounidense en un contrato por valor de unos 21.880 millones de dólares en 10 años.

Big Tech Sells War calcula que, en los últimos 20 años, los contratos de las grandes tecnológicas con el Pentágono y el Departamento de Seguridad Nacional (DHS) han ascendido aproximadamente a 44.000 millones de dólares. En el momento de escribir este artículo, Steve Pandelides, Director de Seguridad de AWS, había trabajado para el FBI durante más de 20 años, entre otras cosas en el Centro Nacional de Lucha contra el Terrorismo y en la División de Tecnología Operativa. Jared Cohen trabajó en Google, donde fundó Jigsaw, encargada de desarrollar herramientas antiterroristas para plataformas de medios sociales, entre otras cosas. Anteriormente fue personal de planificación de políticas del Departamento de Estado de Estados Unidos y ahora trabaja en Goldman Sachs.

En muchos sentidos, las grandes empresas tecnológicas se basan en el modelo del complejo militar-industrial para crear un nuevo complejo tecnológico-militar. Pero a diferencia de la naturaleza descarada de la industria armamentística tradicional, en la que las armas están obviamente diseñadas para matar y reprimir, la ‘Big Tech’ es más insidiosa porque pretende ser democrática y accesible al mismo tiempo. La difusa distinción entre uso militar y civil contribuye a normalizar su ubicuidad y embota nuestra respuesta a los urgentes desafíos que plantea.

## **La tecnología del apartheid israelí**

Ver la situación desde la perspectiva de la ciudadanía palestina ayuda a despejar la niebla, dada la complicidad de las grandes tecnológicas en el sistema de *apartheid* de Israel. Desde antes de su establecimiento en 1948, mediante la limpieza étnica de cientos de miles de palestinos, Israel ha desplegado su aparato militar y de vigilancia para

desposeerlos, fragmentarlos y restarles aún más poder. El Cuerpo de Inteligencia de las Fuerzas de Ocupación Israelíes, Unidad 8200, se fundó en 1952. Desde entonces, se encarga de recopilar información y descifrar códigos. El espionaje y la vigilancia masiva de los palestinos es la fuerza motriz de gran parte del rápido desarrollo de nuevas tecnologías por parte de Israel. He aquí cómo la Autoridad de Innovación de Israel habla de la ciberguerra:

La ciberguerra siempre ha estado a la vanguardia de la industria israelí de alta tecnología. [...] La combinación ganadora de graduados de las unidades tecnológicas de las FDI [Fuerzas de Defensa de Israel] y un entorno de innovación apoyado por la Autoridad de Innovación permite que la tecnología israelí de vanguardia dé forma al futuro a partir de hoy (Israel Innovation, s/f).

Israel exporta este paradigma de seguridad –de miedos fabricados que justifican respuestas autoritarias por parte de los estados para garantizar su *seguridad* y *supervivencia*– junto con sus armas y tecnologías. En el caso del régimen de apartheid de Israel, esta necesidad de seguridad se extiende solo a la población judía, mientras que los palestinos viven en diversos grados de privación de derechos, despojados de seguridad por las políticas de Israel.

La Unidad 8200 puede intervenir cualquier conversación telefónica en los Territorios Palestinos Ocupados. Hay cámaras de reconocimiento facial instaladas –una por cada 100 palestinos– en el Jerusalén Este ocupado. La información privada se utiliza para chantajear a los palestinos para que se conviertan en informantes (Mondoweiss, 2014). Las cámaras Hawk Eye, diseñadas para leer las matrículas, permiten a las fuerzas policiales israelíes obtener información y la ubicación de los vehículos en tiempo real. Los puestos de control israelíes tienen instalada tecnología de reconocimiento facial, inicialmente proporcionada por HP. La aplicación *Lobo azul*, apodada el *Facebook para palestinos* secreto del ejército israelí, capta imágenes de palestinos de toda Cisjordania ocupada y las coteja con la base de datos gestionada por los servicios militares y de inteligencia israelíes. Los soldados



israelíes son recompensados por capturar un gran número de fotografías de palestinos bajo ocupación (Abukhater, 2022).

Ni siquiera el panóptico de Jeremy Bentham capta esta situación, ya que solo pretendía vigilar para controlar, mientras que Israel y su aparato tecnológico pretenden vigilar, coaccionar, chantajear y violar, todo ello en el marco de su régimen de *apartheid*.

Al igual que la industria armamentística, la esfera de la tecnología digital israelí se despliega dentro de un sistema de *apartheid*, por el que las herramientas y aplicaciones se *prueban sobre el terreno* en palestinos antes de exportarlas. Jalal Abukhater, en el artículo citado anteriormente, señala:

Para las empresas israelíes dedicadas al desarrollo de tecnologías de vigilancia y programas espía, los territorios ocupados no son más que un laboratorio donde probar sus productos antes de comercializarlos y exportarlos a todo el mundo con fines lucrativos. Para el Gobierno israelí, este régimen de vigilancia es tanto una herramienta de control como un negocio para hacer dinero (Abukhater, 2022).

De hecho, como reveló el Proyecto Pegasus, el programa espía Pegasus del Grupo NSO israelí se ha utilizado en todo el mundo para espiar a periodistas y activistas, así como a dirigentes gubernamentales y de la oposición. En India, por ejemplo, la lista de objetivos del programa espía Pegasus incluye a cualquiera que plantee un desafío serio al Gobierno derechista de Modi. Es bien sabido que las armas y tecnologías militares israelíes se utilizan como medio de represión en todo el mundo. Sin embargo, sigue estando oculto el papel de las grandes empresas tecnológicas en la producción y exportación de tecnologías represivas por parte de Israel.

## **Las grandes tecnológicas, beneficiarias del apartheid**

Mientras que su régimen colonial de *apartheid* y de colonos es el *laboratorio* para la producción de armas y tecnología represivas, son las

grandes empresas tecnológicas las que proporcionan la inversión necesaria y apoyan la proliferación de la industria israelí de TI y ciberseguridad, de la que se beneficia ampliamente.

Los principales gigantes tecnológicos, desde Microsoft hasta Google y AWS, participan activamente en la industria tecnológica israelí. Microsoft habría adquirido dos empresas israelíes de ciberseguridad entre 2015 y 2017. Adallom, fundada por un veterano de la unidad especial de Inteligencia israelí, fue comprada en 2015 por 320 millones de dólares, y Hexadite por 100 millones en 2017.

En 2019, AWS, contratada junto con Google para construir la plataforma en la nube de Israel junto con Google, trabajó con centros de datos locales para establecer la infraestructura en la nube. Como parte del proyecto Nimbus, Google ha creado recientemente una región local de nube en Israel. Según el contrato, las dos empresas se han “comprometido a realizar compras recíprocas y a poner en marcha una cooperación industrial en Israel equivalente al 20% del valor del contrato” (Scheer, 2022). El segundo mayor centro de I+D de Facebook también tiene su sede en Israel.

Los estados que compran programas espía y tecnología digital israelíes para reprimir a sus ciudadanos están afianzando el régimen de *apartheid* de Israel, y, como tal, deben ser cuestionados, junto con la denuncia de la complicidad y la especulación de las grandes empresas tecnológicas con sede en Estados Unidos.

## **Praxis de la interseccionalidad: la campaña No Tech for Apartheid**

La expansión del control y la complicidad de las grandes empresas tecnológicas en la represión militar se ha visto contrarrestada por diversos retos y por la resistencia popular. Desde la primera fase de denuncias de irregularidades hasta las campañas actuales que exponen cómo las grandes empresas tecnológicas se benefician de la guerra existe una demanda creciente para poner fin a la militarización de la tecnología.

En Estados Unidos, por ejemplo, una campaña popular, No Tech for ICE, destaca el papel clave desempeñado por Palantir y AWS al proporcionar la infraestructura para el Servicio de Inmigración y Control de Aduanas (ICE) junto con otras agencias policiales involucradas en la brutal política de separación familiar de la administración Trump. Palantir recopiló información sobre individuos, lo que permitió a las agencias estatales rastrear y construir perfiles de inmigrantes para ser deportados, mientras que AWS proporcionó servidores para alojar las herramientas de Palantir.

Los organizadores comunitarios están reconociendo y respondiendo rápidamente al modo digital de militarización y represión, que se observa no solo en las exportaciones de los gigantes tecnológicos a estados represivos, sino también en cómo la censura digital y el silenciamiento se utilizan para aplastar las voces de la resistencia y amplificar las ideologías regresivas de derechas. Esto también lo han puesto de relieve grupos de derechos digitales como 7amleh, el Arab Center for Social Media Development y Sada Social, que han demostrado cómo durante el asalto a Gaza de 2021 y en la lucha popular posterior plataformas de medios sociales como Facebook e Instagram censuraron el contenido relacionado con Palestina. Existe un discurso creciente sobre los derechos digitales que reúne a organizadores de base y expertos en tecnología que trabajan para que la esfera digital sea abierta y democrática en lugar de servir como herramienta de sometimiento.

A estas fuerzas se han unido varios empleados actuales (y antiguos) de empresas tecnológicas, en huelga contra el uso de sus productos para violar los derechos de los marginados y con fines militares. Destacaron las profundas implicaciones éticas de involucrarse de la manera que sea en la automatización de la guerra. En 2018, un año antes de su vencimiento, Google anunció que no renovarían su contrato con Project Maven. Como ya se ha dicho, Microsoft y AWS ganaron el contrato.

La campaña contra el Proyecto Nimbus presenta una oportunidad crucial para unir las luchas contra las 'Big Tech' desde varios ángulos: palestinos y activistas solidarios, trabajadores tecnológicos, derechos digitales y activistas sindicales y antimilitaristas.

Meses después de que se anunciara el contrato, noventa empleados de Google y trescientos de Amazon escribieron una carta abierta condenando y oponiéndose a la decisión de sus empleadores de “suministrar al Gobierno y al ejército israelí tecnología que se utiliza para dañar a los palestinos”. Algunos de los manifestantes se enfrentaron a represalias, como Ariel Koren, a quien se le dio un ultimátum para trasladarse de Estados Unidos a Brasil, a pesar de las grandes peticiones públicas en contra de esta acción. Koren abandonó Google en agosto de 2022, señalando en su declaración de dimisión que “Google silencia sistemáticamente las voces palestinas, judías, árabes y musulmanas preocupadas por la complicidad de Google en las violaciones de los derechos humanos de los palestinos, hasta el punto de tomar represalias formales contra los trabajadores y crear un ambiente de miedo”. Otros se unieron a ella para denunciar las represalias tomadas contra quienes apoyaban esta campaña.

Junto con la profunda complicidad de AWS en la industria de TI y ciberseguridad de Israel, y su apoyo a la represión en otros lugares como se ve en el ejemplo de ICE, se ha denunciado ampliamente su historial en el trato inhumano de los trabajadores y la represión sindical (Kantor, 2021). La formación del sindicato Amazon Labor Union en Staten Island fue, por tanto, un momento histórico en el movimiento sindical estadounidense. En conjunto, es probable que las acciones de estos empleados causen cierta preocupación entre los actuales directores ejecutivos de las grandes tecnológicas.

Más allá del apoyo a las agencias militares y de vigilancia, que en esencia contribuye a una militarización cada vez mayor de la vida cotidiana de las personas, también está la cuestión del control de las grandes tecnológicas sobre nuestros datos. Aspectos de nuestras vidas que dejan huellas en el mundo virtual –ahora casi inevitables– se entretejen en algoritmos que influyen profundamente en nuestras elecciones, opiniones políticas y decisiones. Los movimientos por los derechos digitales exigen la defensa de nuestra privacidad y seguridad y contra la comercialización de los datos personales, y en ningún lugar es más evidente que con Google. Existe un creciente desafío al control

de las grandes tecnológicas sobre las vidas individuales y las elecciones codificadas en datos. Las alternativas al colonialismo de los datos también han suscitado animados debates sobre el código abierto, la propiedad pública, etc.

En el extremo más agudo del colonialismo digital, Palestina es, por tanto, un signo de lo que está por venir y, por tanto, el punto en el que primero debemos resistir. En nombre de la reducción de la brecha digital, las grandes empresas tecnológicas están cada vez más arraigadas, extrayendo datos y lucrándose con ellos. La pandemia de COVID-19 exacerbó esta situación, ya que personas de todo el mundo tuvieron que trabajar y estudiar desde casa, en su mayoría sin acceso a tecnología y equipos digitales.

El creciente interés de estudiantes y académicos por cuestionar el control de las grandes empresas tecnológicas, como Google, en el ámbito de la educación, y su relación directa con la opresión de los palestinos, impulsó a la campaña mundial No Tech for *Apartheid* a elaborar un conjunto de herramientas para organizarse en los campus universitarios.

La campaña contra el Proyecto Nimbus se sitúa en la intersección de la solidaridad palestina y los movimientos contra el *apartheid*, los derechos laborales, los derechos digitales, la descolonización y la desmilitarización. En este movimiento en evolución, ofrece una visión clara de la matriz de opresión de la militarización, el capital neoliberal y el *apartheid* israelí, todo lo cual refuerza la gran tecnología y de lo que obtiene enormes beneficios. Se basa en la comprensión desarrollada por las campañas contra las grandes tecnológicas en la guerra, y reúne a muchas comunidades que luchan contra un contrato que tiene profundas implicaciones para todos. Los sistemas interconectados que nos oprimen exigen que nuestras formas de resistencia también se unan, para desafiar a las fuerzas que pretenden aislarnos. La solidaridad solo existe en la acción, y a través de su propia existencia como fuerza interseccional socava la violencia infligida por el colonialismo, el patriarcado, el racismo y el neoliberalismo. La tecnología no está diseñada para ser neutral, y mientras aspectos de nuestras vidas se adentran cada vez más

en esta esfera, y sus operaciones y mecanismos siguen estando lejos de ser democráticos, con la fuerza de la resistencia global sus herramientas básicas aún pueden democratizarse y hacerse accesibles.

## **Bibliografía**

7amleh, the Arab Center for Social Media Development (2021). #Hashtag Palestine 2021. <https://7amleh.org/storage/Hashtag%202021%20EN.pdf>

Alys Samson Estapé ( mayo de 2021). Israel: the model coercive state and why boycotting it is key to emancipation everywhere. *TNI Longreads*. <https://longreads.tni.org/stateofpower/israel-the-model-coercive-state>.

Abukhater, Jalal (2022). Under Israeli surveillance: Living in dystopia, in Palestine. *Aljazeera*. <https://www.aljazeera.com/opinions/2022/4/13/under-israeli-surveillance-living-in-dystopia-in-palestine>

Amnesty International (2022). Israel's apartheid against Palestinians. <https://www.amnesty.org/en/latest/campaigns/2022/02/israels-system-of-apartheid/>

Big Tech Sells War. Big Tech Sells War - How Big Tech Sells War on our Communities. <https://bigtechsellswar.com/>

Big Tech Sells War. Big Tech Sells War - How Big Tech Sells War on our Communities. <https://bigtechsellswar.com/#timelines-home>

Brewster, Thomas (2021). Project Maven: Amazon And Microsoft Scored \$50 Million In Pentagon Surveillance Contracts After Google Quit. *Forbes*. <https://www.forbes.com/sites/>

thomasbrewster/2021/09/08/ project-maven-amazon-and-microsoft-get-50-million-in-pentagon-drone-surveillance-contracts-after-google/?sh=549483dc6f1e

Fung, Brian (2021). Amazon Web Services disables cloud accounts linked to NSO Group. *CNN Business*. <https://edition.cnn.com/2021/07/19/tech/amazon-nso-group-pegasus-cloud-accounts/index.html>.

Investigate & Dismantle Apartheid. (2022). Al Haq issues landmark report 'Israeli Apartheid: Tool of Zionist Settler-Colonialism'. <https://antiapartheidmovement.net/updates/view/al-haq-issues-landmark-report-israeli-apartheid-tool-of-zionist-settler-colonialism/15>

Israel Innovation. Attack is the Best Form of Defense. <https://innovationisrael.org.il/en/reportchapter/attack-best-form-defense>

Kantor, Jodi, Weise, Karen y Ashford, Grace (15 de junio de 2021). The Amazon That Customers Don't See. *The New York Times*. <https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html>

Khan, Azmat (18 de diciembre de 2021). Hidden Pentagon Records Reveal Patterns of Failure in Deadly Airstrikes. *The New York Times*. <https://www.nytimes.com/interactive/2021/12/18/us/airstrikes-pentagon-records-civilian-deaths.html>

Middle East Eye (2021). Meet Blue Wolf, the app Israel uses to spy on Palestinians in the occupied West Bank. <https://www.middleeasteye.net/news/israel-whats-blue-wolf-app-soldiers-use-photograph-palestinians>

Nextgov.com (2021). NSA Awards Secret \$10 Billion Contract to Amazon. <https://www.nextgov.com/it-modernization/2021/08/nsa-awards-secret-10-billion-contract-amazon/184390/>

Notechforice.com. About | #NoTechForICE. <https://notechforice.com/about/>

Novet, Jordan (31 de marzo de 2021). Microsoft wins U.S. Army contract for augmented reality headsets, worth up to \$21.9 billion over 10 years. *CNBC*. <https://www.cnn.com/2021/03/31/microsoft-wins-contract-to-make-modified-hololens-for-us-army.html>

Lunden, Ingrid (2017). Microsoft to buy Israeli security firm Hexadite, sources say for \$100M. *TechCrunch*. <https://techcrunch.com/2017/06/08/microsoft-confirms-its-acquired-hexadite-sources-say-for-100m/?guccounter=2>

Scheer, Steven (24 de mayo de 2021). Israel signs cloud services deal with Amazon, Google. *Reuters*. <https://www.reuters.com/technology/israel-signs-cloud-services-deal-with-amazon-google-2021-05-24/>

Scheer, Steven (20 de octubre de 2022). Google activates Israel's first local cloud region. *Reuters*. <https://www.reuters.com/technology/google-activates-israels-first-local-cloud-region-2022-10-20/>

Shulman, Sophie (8 de enero de 2021). Unit 81: The Elite Military Unit That Caused a Big Bang in the Israeli Tech Scene. *The algemeiner*. <https://www.algemeiner.com/2021/01/08/unit-81-the-elite-military-unit-that-caused-a-big-bang-in-the-israeli-tech-scene/>

Statt, Nick (2018). Google reportedly leaving Project Maven military AI program after 2019. *The Verge*. <https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contract-expire>

Stop The Wall (s/f). Digital Walls. <https://stopthewall.org/digitalwalls/>

Stop The Wall (s/f). Digital Walls. <https://stopthewall.org/digitalwalls/#militarization>



Strout, Nathan (2022). Intelligence agency takes over Project Maven, the Pentagon's signature AI scheme. *C4ISRNet*. <https://www.c4isrnet.com/intel-geoint/2022/04/27/intelligence-agency-takes-over-project-maven-the-pentagons-signature-ai-scheme/>

Theregister.com (2022). \$10b US defense cloud contract re-awarded to AWS. [https://www.theregister.com/2022/04/28/nsa\\_wands\\_aws/](https://www.theregister.com/2022/04/28/nsa_wands_aws/)

VentureBeat (2015). Microsoft confirms it has acquired cloud security platform Adallom. <https://venturebeat.com/business/microsoft-confirms-it-has-acquired-cloud-security-platform-adallom/>

Weiss, Philip (2014). Israel surveils and blackmails gay Palestinians to make them informants. *Mondoweiss*. <https://mondoweiss.net/2014/09/blackmails-palestinian-informants/>

WhoProfits (2021). Hewlett Packard Enterprise (HPE). <https://www.whoprofits.org/company/hewlett-packard-enterprise-hpe/>

