

La militarización de las Big Tech: el auge de la industria de defensa digital de Silicon Valley

Por: ROBERTO J. GONZÁLEZ. 19/07/2023

En Estados Unidos, las grandes tecnológicas y las fuerzas armadas están cada vez más fusionadas. Deshacer el nudo será clave para evitar guerras interminables en el extranjero y una policía militarizada en casa.

En septiembre de 2011, la CIA y el ejército estadounidense lanzaron conjuntamente un ataque con drones **autorizado por el presidente Barack Obama**. El ataque se saldó con **el asesinato en Yemen de Anwar al Awlaki**, un ferviente clérigo musulmán nacido en Estados Unidos. Los organizadores del ataque se basaron en los datos de geolocalización de Awlaki, controlados por la [Agencia de Seguridad Nacional](#) en el marco de un programa de vigilancia. Dos semanas después, un ataque de aviones no tripulados de la CIA mató a otro ciudadano estadounidense utilizando el mismo tipo de datos: el hijo de 16 años de al Awlaki, [Abdulrahman al Awlaki](#).

Aunque al Awlaki fue asesinado deliberadamente por las fuerzas estadounidenses, otros ciudadanos estadounidenses -y miles de civiles en Afganistán y otras partes de Asia Central y Oriente Próximo- han sido asesinados inadvertidamente por [aviones no tripulados](#). Estos casos presagian un fallo importante en la última iteración de la guerra automatizada: la **imprecisión de las tecnologías y los grandes márgenes de error** que acompañan incluso a los nuevos sistemas de armamento más sofisticados. En su forma más avanzada, las herramientas informatizadas hacen uso de la inteligencia artificial y el aprendizaje automático, y pronto **podrían tener capacidades totalmente autónomas**.

Los dispositivos digitales portátiles con conexión a Internet han transformado a miles de millones de personas en todo el mundo en máquinas atomizadas de producción de datos, que introducen información en cientos, si no miles, de algoritmos cada día. Aunque hemos integrado rápidamente los teléfonos inteligentes y las tabletas en nuestras vidas, **pocas veces reflexionamos sobre cómo los datos almacenados y transmitidos por estos aparatos pueden militarizarse fácilmente**. Por ejemplo, [informes recientes](#) describen cómo la Agencia de Inteligencia de Defensa de

EE.UU., afiliada al Departamento de Defensa (DoD), utiliza habitualmente datos de geolocalización disponibles comercialmente recogidos de teléfonos móviles individuales, a veces sin orden judicial. Las agencias militares y de inteligencia pueden utilizar esos datos no sólo para espiar, sino también para **reconstruir redes sociales e incluso para dirigir ataques letales contra individuos.**

Drones, software de geolocalización, programas espía y otras herramientas de este tipo son emblemáticos de una nueva serie de colaboraciones entre la Gran Tecnología y la Gran Defensa. **Durante las dos últimas décadas, el Departamento de Defensa y 17 agencias gubernamentales estadounidenses conocidas colectivamente como la Comunidad de Inteligencia de Estados Unidos han intentado captar la innovación tecnológica en su origen: Silicon Valley.** Las agencias militares y de espionaje lo han hecho creando puestos avanzados a lo largo de la Costa Oeste; organizando un consejo asesor de alto nivel que vincula al Pentágono con las grandes empresas tecnológicas; coordinando cumbres, foros y reuniones privadas con inversores influyentes y ejecutivos de empresas; y apelando directamente a los corazones y las mentes de empresarios, ingenieros, informáticos e investigadores que a veces se muestran escépticos ante los burócratas gubernamentales, especialmente los del DoD.

En muchos sentidos, es imposible comprender plenamente al ejército estadounidense hoy en día sin un análisis de sus profundas **conexiones con la industria tecnológica.**

“Los dispositivos digitales portátiles con conexión a Internet han transformado a miles de millones de personas en todo el mundo en máquinas atomizadas de producción de datos, que introducen información en cientos, si no miles, de algoritmos cada día”

Las interconexiones entre los mundos de la tecnología de redes y la defensa se remontan a hace más de 50 años. Por ejemplo, desde principios de la década de 1960, la Agencia de Proyectos de Investigación Avanzada (ARPA) del Departamento de Defensa desempeñó un papel crucial en la financiación de la investigación informática que dio lugar a la ARPANET, **precursora de la actual Internet**. El desarrollo inicial de Silicon Valley fue financiado en gran parte por **agencias de defensa e inteligencia**, y el Pentágono invirtió mucho en empresas tecnológicas (enlace externo) durante toda la Guerra Fría.

¿Qué es la guerra virtual?

Evidentemente, la guerra virtual significa cosas distintas para cada persona. No existe una definición consensuada, lo que permite interpretar el término de forma amplia, holística y antropológica. Yo adopto una perspectiva amplia, centrándome en cuatro elementos diferentes: los sistemas de armas robóticas y autónomas; una versión de alta tecnología de las operaciones psicológicas o psyops; los programas de modelización y simulación predictiva, que algunos denominan “contrainsurgencia computacional”; y la ciberguerra, es decir, el ataque y la defensa de infraestructuras críticas. Estas tecnologías y técnicas se basan en la producción, disponibilidad y análisis de cantidades masivas de datos -a menudo datos de vigilancia- recogidos de drones, satélites, cámaras, teléfonos móviles, transacciones electrónicas, redes sociales, mensajes de correo electrónico y otras fuentes de Internet.

Podemos considerar esto como **una guerra de algoritmos**. Cada vez más, las tecnologías hacen uso de la inteligencia artificial o IA para automatizar los procesos de toma de decisiones. El desarrollo de armas virtuales depende de los esfuerzos combinados de una amplia gama de científicos y expertos técnicos: no sólo químicos, físicos, ingenieros, programadores informáticos y analistas de datos, sino también investigadores en biotecnología, politólogos, psicólogos y antropólogos. Gran parte del trabajo es **bastante banal** y tiene lugar en edificios anodinos de parques de oficinas suburbanos, campus tecnológicos o laboratorios universitarios. **Silicon Valley se ha convertido en uno de los principales centros de este tipo de trabajo de defensa e inteligencia.**

En cierto modo, la guerra virtual es una continuación de la llamada **Revolución en Asuntos Militares** o RMA, una doctrina articulada por la **Oficina de Evaluación de Redes del Pentágono**

en los años ochenta y noventa. Se inclinaba fuertemente hacia soluciones basadas en la tecnología. Después del 11-S, cuando Estados Unidos emprendió su llamada Guerra Global contra el Terror, y entró en guerra contra redes globales de insurgentes armados con tecnologías relativamente sencillas como bombas improvisadas, rifles y lanzagranadas, la RMA perdió fuelle, y la contrainsurgencia se puso de moda tras un largo paréntesis. Pero ahora, en un periodo marcado por la rápida innovación, **los modos algorítmicos de gobernanza y el ascenso al poder de naciones rivales como China y Rusia** -cada una de las cuales persigue sus propias tecnologías virtuales de lucha bélica-, el combate informatizado ha vuelto a ocupar un lugar central entre las élites del establishment militar estadounidense.

La intersección entre la gran defensa y la gran tecnología: Creación de DIUx

Mountain View descansa cómodamente entre las boscosas montañas de Santa Cruz y la costa sur de la bahía de San Francisco. Durante la primera mitad del siglo XX fue una ciudad tranquila con granjas de ganado, huertos frutales y pintorescas calles céntricas. Pero después de que un equipo de científicos dirigido por **William Shockley inventara allí el semiconductor en 1956**, creció rápidamente, junto con el resto de Silicon Valley. Hoy es un bullicioso suburbio con más de 80.000 residentes.

A primera vista, parece un lugar extraño para que se establezcan agencias militares y de inteligencia. Mountain View está a casi 4.024 km del Pentágono. Los vuelos directos de San Francisco a Honolulu tardan menos que los vuelos a Washington, DC.

El Pentágono y Silicon Valley no sólo están alejados geográficamente, sino que también hay otras diferencias. **El Departamento de Defensa suele considerarse una burocracia notoriamente hinchada**, estirada y derrochadora, con estructuras organizativas rígidamente jerarquizadas y normas laborales inflexibles. En cambio, el mayor empleador de Mountain View es Alphabet, la empresa matriz de Google, una de las corporaciones más valiosas del mundo. Su campus de 26 acres, conocido como Googleplex, incluye más de 30 cafeterías, comida y bebida gratis para sus empleados, gimnasios y piscinas. Un esqueleto de tiranosaurio rex de hierro a tamaño real, al que los empleados de Google llaman cariñosamente Stan,

ocupa un lugar destacado en el exterior de un edificio principal.

A pesar de estas diferencias -de hecho, debido a ellas-, **el secretario de Defensa Ash Carter estableció muy públicamente un puesto avanzado del Pentágono a menos de tres kilómetros del Googleplex.** La [Unidad de Innovación de Defensa Experimental](#), o DIUx, se creó en agosto de 2015 para identificar e invertir rápidamente en empresas que desarrollaran tecnologías punteras que pudieran ser útiles para el ejército. Con DIUx, el Pentágono creó su propio acelerador de start-ups dedicado a financiar empresas especializadas en IA, sistemas robóticos, análisis de big data, ciberseguridad y biotecnología.

El nuevo hogar de DIUx no estaba tan fuera de lugar. Su sede se encontraba en un edificio ocupado en su día por la Guardia Nacional del Ejército, en los terrenos del Centro de Investigación Ames, el mayor de los diez centros de campo de la NASA, y Moffett Field, antaño sede del 130º Escuadrón de Rescate de la Guardia Nacional Aérea de California. Los gigantes de la defensa Lockheed Martin y Northrop Grumman tienen oficinas a menos de 3 km. **En 2008, la propia Google invadió territorio gubernamental: firmó un contrato de arrendamiento de 40 años con la NASA Ames para un nuevo campus de investigación.** Luego firmó un acuerdo de sesenta años con la NASA para arrendar 1.000 acres de Moffett Field, incluidos tres enormes hangares para dirigibles. En la actualidad, Google utiliza los hangares para construir [globos estratosféricos](#) que algún día podrían proporcionar servicios de Internet a los habitantes de zonas rurales, o quizá llevar a cabo misiones militares de vigilancia a gran altitud.

“Con DIUx, el Pentágono creó su propio acelerador de start-ups dedicado a financiar empresas especializadas en IA, sistemas robóticos, análisis de big data, ciberseguridad y biotecnología”

La oficina de DIUx estaba muy cerca de otras empresas tecnológicas: El Lab126 de Amazon (donde se gestaron el lector Kindle, Amazon Echo y otros dispositivos digitales); la sede corporativa de LinkedIn; y el campus de Microsoft en Silicon Valley. Las oficinas corporativas de Apple se encontraban a 8 km, en la cercana Cupertino. **Las nuevas instalaciones del Pentágono se encontraban literalmente en la intersección de la Gran Tecnología y la Gran Defensa.** La oficina de DIUx, situada en un edificio de ladrillo, abarcaba las contradicciones del Pentágono Oeste: “Los pasillos son monótonos, las puertas tienen cerraduras de combinación. Pero en

el interior, los recién llegados han renovado los espacios con pizarras, pizarras blancas y escritorios dispuestos en diagonales aleatorias, a juego con el ambiente no jerárquico de una startup del Valle”, [informó un observador](#).

El plan de Ash Carter era ambicioso: aprovechar las mejores y más brillantes mentes de la industria tecnológica para uso del Pentágono. Este nativo de Pensilvania había pasado varios años en la Universidad de Stanford antes de su nombramiento como Secretario de Defensa, y quedó impresionado con el espíritu innovador y los magnates millonarios del Área de la Bahía: Están inventando nuevas tecnologías, creando prosperidad, conectividad y libertad”, [dijo Carter](#). “Sienten que ellos también son servidores públicos y les gustaría tener a alguien en Washington con quien poder conectar”. Sorprendentemente, Carter fue el primer Secretario de Defensa en ejercicio que visitó Silicon Valley en más de 20 años.

El Pentágono tiene su propia agencia de investigación y desarrollo (I+D), DARPA, pero persigue proyectos para los que faltan décadas, no meses. Carter quería una oficina ágil y racionalizada que pudiera actuar como una especie de intermediario, **canalizando decenas o cientos de millones de dólares del enorme presupuesto del Departamento de Defensa hacia empresas prometedoras que desarrollaran tecnologías a punto de completarse.** Lo ideal sería que DIUx sirviera de enlace, negociando las necesidades de los generales de cuatro estrellas, los dirigentes civiles del Pentágono y los ingenieros y empresarios con capucha. Pronto, DIUx abrió sucursales en otras dos ciudades con sectores tecnológicos florecientes: Boston y Austin.

A corto plazo, Carter esperaba que DIUx estableciera relaciones con las nuevas empresas locales, reclutara a los mejores talentos, involucrara a los reservistas militares en los proyectos y agilizará los procesos de adquisición del Pentágono, notoriamente engorrosos. Sus objetivos [a largo plazo](#) eran aún más ambiciosos: tomar oficiales militares de carrera y asignarlos a trabajar en proyectos futuristas en Silicon Valley durante meses, para “exponerlos a nuevas culturas e ideas que puedan llevar de vuelta al Pentágono. . .[e] invitar a los técnicos a pasar tiempo en Defensa”.

En marzo de 2016, Carter organizó el [Consejo de Innovación de Defensa](#) (DIB), un grupo de expertos civiles de élite encargado de asesorar y hacer recomendaciones a

los dirigentes del Pentágono. Nombró al ex CEO de Google y miembro del consejo de Alphabet Eric Schmidt para presidir el DIB, que incluía ejecutivos actuales y anteriores de Facebook, Google e Instagram, entre otros.

Tres años después de que Carter pusiera en marcha DIUx, pasó a llamarse **Unidad de Innovación de Defensa** (DIU), lo que indicaba que ya no era experimental. A pesar de las dificultades iniciales, el Subsecretario de Defensa Patrick Shanahan describió DIUx como [“un activo valioso y probado”](#). ‘La organización en sí ya no es un experimento’, dijo en 2018. ‘DIU sigue siendo vital para fomentar la innovación en todo el Departamento y transformar la forma en que el DoD construye una fuerza más letal.’ A principios de 2018, la administración **Trump** solicitó [un fuerte aumento](#) en el presupuesto de DIU para el año fiscal 2019, de \$ 30 millones a \$ 71 millones. Para 2020, la administración solicitó [164 millones de dólares](#), más del doble de la solicitud del año anterior.

“En marzo de 2016, Carter organizó el Consejo de Innovación de Defensa (DIB), un grupo de expertos civiles de élite encargado de asesorar y hacer recomendaciones a los dirigentes del Pentágono”

El fondo de capital riesgo de la CIA

Aunque los funcionarios del Pentágono presentaban a DIUx como una organización innovadora, en realidad seguía el modelo de otra empresa creada para prestar un servicio similar a la comunidad de inteligencia estadounidense. A finales de la década de 1990, **la CIA creó una entidad sin ánimo de lucro llamada Peleus para capitalizar las innovaciones que se estaban desarrollando en el sector privado**, con especial atención a Silicon Valley. Poco después, la organización pasó a llamarse **In-Q-Tel**.

El primer Director General, Gilman Louie, describió cómo se creó la organización para resolver [“el problema de los grandes datos”](#):

[Los dirigentes de la CIA] tenían mucho miedo de lo que en aquel momento llamaban la perspectiva de un **‘Pearl Harbor digital’**. Pearl Harbor ocurrió cuando cada parte del gobierno tenía una parte de la información, pero no podían unirla para decir: “Mira, el ataque a Pearl Harbor es inminente”. En 1998, empezaron a darse cuenta de que la información estaba aislada en todas estas agencias de inteligencia

y que nunca podrían unirlos. Intentaban resolver el problema de los grandes datos. ¿Cómo unirlos para obtener información?

Mediante la canalización de fondos de la CIA a empresas nacientes que creaban tecnologías de vigilancia, recopilación de información, análisis de datos y ciberguerra, la agencia esperaba obtener una ventaja sobre sus rivales mundiales cooptando a ingenieros, hackers, científicos y programadores creativos. En 2005, la CIA invirtió aproximadamente 37 millones de dólares en In-Q-Tel. En 2014, la financiación anual de la organización se había disparado a casi **94 millones de dólares** y había realizado [325 inversiones](#) en una asombrosa variedad de empresas tecnológicas.

Si In-Q-Tel parece sacada de una película de James Bond, es porque la organización se inspiró en parte en la rama Q, la oficina ficticia de I+D del servicio secreto británico, popularizada en las novelas de espionaje de **Ian Fleming** y en las superproducciones de Hollywood. **In-Q-Tel y DIUx se crearon aparentemente para transferir tecnologías emergentes del sector privado a los servicios de inteligencia y las agencias militares estadounidenses, respectivamente.** Una interpretación [algo diferente](#) es que estas organizaciones se crearon “para captar innovaciones tecnológicas. [y] para captar nuevas ideas”. Los críticos señalan a In-Q-Tel como ejemplo paradigmático de la militarización de la industria tecnológica.

En términos monetarios y tecnológicos, es probable que la inversión más rentable de In-Q-Tel fuera Keyhole, una empresa con sede en San Francisco que desarrollaba programas informáticos para entrelazar imágenes de satélite y fotos aéreas con el fin de crear modelos tridimensionales de la superficie terrestre. El programa podía crear esencialmente un mapa de alta resolución de todo el planeta. In-Q-Tel aportó financiación en 2003 y, **en pocos meses, el ejército estadounidense utilizó Keyhole para apoyar a las tropas estadounidenses en Irak.**

“Si In-Q-Tel parece sacada de una película de James Bond, es porque la organización se inspiró en parte en la rama Q, la oficina ficticia de I+D del servicio secreto británico, popularizada en las novelas de espionaje de Ian Fleming y en las superproducciones de Hollywood”

Las fuentes oficiales nunca revelaron cuánto invirtió In-Q-Tel en Keyhole, pero **en 2004 Google compró la start-up.** Pasó a llamarse **Google Earth.** La adquisición

fue significativa: el periodista [Yasha Levine escribe](#) que el acuerdo Keyhole-Google “marcó el momento en que la empresa dejó de ser una compañía de Internet puramente orientada al consumidor y **comenzó a integrarse con el gobierno de Estados Unidos**“. En 2007, Google buscaba activamente [contratos gubernamentales](#) repartidos uniformemente entre agencias militares, de inteligencia y civiles.

Además de Google, la cartera de In-Q-Tel incluye empresas con proyectos futuristas como Cyphy, que fabrica drones anclados que pueden volar en misiones de reconocimiento durante largos periodos gracias a una fuente de energía continua; Atlas Wearables, que fabrica rastreadores de actividad física que controlan de cerca los movimientos corporales y las constantes vitales; Fuel3d, que vende un dispositivo portátil que produce escaneados tridimensionales detallados de estructuras u objetos; y Sonitus, que ha desarrollado un sistema de comunicaciones inalámbricas, parte del cual cabe dentro de la boca del usuario. Si DIUx ha apostado por empresas de robótica e inteligencia artificial, In-Q-Tel ha perseguido a las que crean tecnologías de vigilancia: empresas de satélites geoespaciales, sensores avanzados, equipos de biometría, analistas de ADN, dispositivos de traducción de idiomas y sistemas de ciberdefensa.

Más recientemente, In-Q-Tel se ha orientado hacia empresas especializadas en la extracción de [datos de redes sociales](#) y otras plataformas de Internet. Entre ellas figuran Dataminr, que **transmite datos de Twitter para detectar tendencias y posibles amenazas**; Geofeedia, que recopila mensajes de redes sociales indexados geográficamente en relación con noticias de última hora, como **protestas**; y TransVoyant, una empresa que recopila datos de satélites, radares, drones y otros sensores.

Algunos podrían aplaudir el éxito de la contratación de empresas tecnológicas por parte del ejército y las agencias de inteligencia estadounidenses. Dado el rápido desarrollo y despliegue de sistemas de armamento y programas de vigilancia de alta tecnología por parte de naciones [rivales como China](#) –**que ha desplegado tecnologías comparables contra sus propios ciudadanos en la provincia de Xinjiang**-, sus defensores suelen afirmar que el ejército estadounidense no puede permitirse quedarse rezagado en una [carrera armamentística de IA](#). Pero estos argumentos no tienen en cuenta cómo la fusión de la Gran Defensa con otra gran industria vinculará aún más estrechamente la economía estadounidense a guerras interminables en el extranjero y a la militarización de la policía en el país.

Proyecto Maven

Muchas de las empresas financiadas por In-Q-Tel y DIUx han sido pequeñas start-ups muy necesitadas de liquidez. Pero el interés del Pentágono por Silicon Valley también se extiende a las mayores empresas basadas en Internet.

Consideremos el caso del **Proyecto Maven**, conocido formalmente como el **Equipo Interfuncional de Guerra Algorítmica**. El subsecretario de Defensa Robert Work [estableció el programa](#) en abril de 2017, describiéndolo como un esfuerzo “para acelerar la integración del DoD de big data y aprendizaje automático. ... [y] convertir el enorme volumen de datos de que dispone el DoD en inteligencia y conocimientos procesables a gran velocidad...”. El [Bulletin of the Atomic Scientists](#) expone el problema de forma sucinta:

Los aviones espía y los satélites estadounidenses recogen más datos en bruto de los que el Departamento de Defensa podría analizar aunque toda su plantilla se dedicara a ello durante toda su vida. Por desgracia, la mayor parte del análisis de imágenes implica un trabajo tedioso: la gente mira las pantallas para contar coches, personas o actividades. ...la mayoría de los datos de los sensores desaparecen, nunca se analizan, a pesar de que el Departamento lleva años contratando analistas a toda velocidad.

El Pentágono había gastado decenas de miles de millones de dólares en sensores. Crear algoritmos para clasificar y analizar las imágenes tenía sentido desde el punto de vista económico, y con un coste previsto de 70 millones de dólares, el Proyecto

Maven debía de parecer una ganga. El alcance del trabajo era asombroso. En su estado actual, los sistemas de IA requieren conjuntos de datos masivos para el “aprendizaje profundo”, que esencialmente significa aprender con el ejemplo. Durante la segunda mitad de 2017, las personas que trabajaban en el Proyecto Maven etiquetaron más de 150.000 imágenes visuales para crear los primeros conjuntos de datos para entrenar los algoritmos. Las imágenes -fotos de vehículos, personas, objetos, eventos- tenían que tener en cuenta cientos, si no miles, de condiciones variables: diferentes altitudes, ángulos de foto, resolución de imagen, condiciones de iluminación, etc.

¿Qué organización podría encargarse de semejante tarea? Los funcionarios del Pentágono no dijeron nada sobre las empresas implicadas, pero algunos informadores dieron pistas indirectas de la participación de importantes empresas tecnológicas. El coronel del Cuerpo de [Marines Drew Cukor](#) que dirigió el Proyecto Maven, señaló que “estamos en una carrera armamentística de IA. Está ocurriendo en la industria [y] las cinco grandes empresas de Internet lo están persiguiendo con ahínco”. Muchos de ustedes habrán notado que **Eric Schmidt** [entonces consejero delegado de Alphabet Inc, la empresa matriz de Google] llama ahora a Google una empresa de IA, no una empresa de datos”.

Apenas ocho meses después de que el Departamento de Defensa pusiera en marcha el Proyecto Maven, **los militares utilizaban los algoritmos del programa para apoyar las misiones con drones contra el ISIS en Irak y Siria.**

En marzo de 2018, [Gizmodo](#) publicó una [serie de ampollas](#) revelando que el Pentágono había contratado silenciosamente a Google para el trabajo del Proyecto Maven en septiembre de 2017. Según correos electrónicos internos de ejecutivos de Google, el acuerdo estaba valorado en al menos 15 millones de dólares, y se esperaba que aumentara hasta **250 millones.**

Algunos correos electrónicos detallaban reuniones entre ejecutivos de Google y el subsecretario de [Defensa Jack Shanahan](#). Más de diez empleados de Google estaban asignados al proyecto, y la empresa se había asociado con varias otras empresas, entre ellas DigitalGlobe, una empresa de imágenes geoespaciales, y CrowdFlower, una empresa de crowdsourcing. CrowdFlower (que desde entonces ha cambiado su nombre por Figure Eight) pagó a **los llamados “crowd workers”** -

personas que realizan tareas repetitivas en línea, como identificar fotos- para que etiquetaran miles de imágenes para el “aprendizaje profundo” algorítmico. Al parecer, **los trabajadores no sabían lo que estaban construyendo ni quién se beneficiaría de ello.**

Algunos de los correos electrónicos internos de Google daban a entender que la empresa tenía planes ambiciosos que iban más allá de lo sugerido en los anuncios iniciales del Pentágono. Uno de ellos sugería la creación de **un sistema de espionaje** “similar a Google Earth” que permitiera a los usuarios “hacer clic en un edificio y ver todo lo relacionado con él”, incluidas personas y vehículos.

Los responsables de Google se preocupaban en privado por un posible problema de relaciones públicas si se filtraba el proyecto Maven: “Creo que deberíamos hacer buenas relaciones públicas sobre la colaboración del Departamento de Defensa con GCP desde el punto de vista de la tecnología en la nube (almacenamiento, red, seguridad, etc.)”, escribió Fei-Fei Li, científico jefe de IA de Google Cloud, “pero evitar a toda costa cualquier mención o implicación de la IA”.

Pero al final se corrió la voz.

Reuelta de los ingenieros

En febrero de 2018, los correos electrónicos internos sobre el Proyecto Maven circularon ampliamente entre los empleados de Google, muchos de los cuales estaban conmocionados y consternados por lo que habían hecho los altos ejecutivos de la compañía. En cuestión de meses, **más de 4.000 investigadores de Google habían firmado una carta dirigida al CEO Sundar Pichai, exigiendo la cancelación del contrato de Maven.** La carta, firmada por varios ingenieros de alto nivel, comenzaba así: “**Creemos que Google no debería estar en el negocio de la guerra**”. También exigía que Google desarrollara “una política clara que establezca que ni Google ni sus contratistas desarrollarán nunca tecnología bélica”. A finales de año, casi una docena de empleados [dimitieron en protesta por los contratos militares](#) de la empresa y la falta de transparencia de sus directivos.

Sorprendentemente, los empleados tuvieron éxito, al menos momentáneamente. A principios de junio, Google anunció que la empresa pondría fin a su trabajo en el [Proyecto Maven](#) cuando expirara el contrato. Días después, Google publicó una

serie de directrices éticas o “[principios de la IA](#)”, en las que afirmaba que la empresa “no diseñará ni desplegará IA” para sistemas de armamento, para “vigilancia que viole normas internacionalmente aceptadas”, ni para tecnologías utilizadas para contravenir el derecho internacional y los derechos humanos.

El compromiso de Google de cancelar su trabajo en el Proyecto Maven era demasiado bueno para ser cierto. En marzo de 2019, [The Intercept](#) obtuvo un correo electrónico interno de Google en el que se indicaba que **una empresa externa seguiría trabajando en el Proyecto Maven** utilizando “Google Cloud Platform off-the-shelf (servicio básico de computación, en lugar de Cloud AI u otros servicios en la nube) para soportar algunas cargas de trabajo”. Walker añadió que Google estaba trabajando con “el Departamento de Defensa para realizar la transición de forma coherente con nuestros principios de IA y compromisos contractuales”.

Otros informes revelaron que el Departamento de Defensa había adjudicado el contrato del Proyecto Maven a Anduril Industries, más conocida por crear el casco de realidad virtual Oculus Rift. El año anterior, Anduril había puesto a prueba un sistema de vigilancia desarrollado para los agentes de Aduanas y Protección de Fronteras de Estados Unidos. **El sistema utiliza IA para detectar la presencia de personas que intentan cruzar la frontera estadounidense.**

Aunque los medios de comunicación dieron a entender que Google (y más tarde Anduril) eran las únicas empresas que desempeñaban un papel en el Proyecto Maven, la realidad es mucho más compleja y preocupante. Un [minucioso análisis](#) de la organización de investigación sin ánimo de lucro [Tech Inquiry](#) documenta la profunda implicación de otros numerosos contratistas y subcontratistas. El Pentágono concedió “adjudicaciones principales” a ECS Federal y Booz Allen Hamilton, y “subcontrataciones” a una serie de empresas como Microsoft, Clarifai, Rebellion Defense, Cubic Corporation, GATR Technologies, Technical Intelligence Solutions y SAP National Security Services, entre otras. **Estos contratos nunca se hicieron públicos.**

Aunque los empleados de Google que se opusieron al Proyecto Maven representaban sólo una modesta parte de los 70.000 empleados de la empresa, consiguieron desencadenar un debate sobre los contratos militares de la industria tecnológica y un debate más amplio sobre la ética de la IA.

La revuelta de Google resonó en toda la Big Tech e inspiró a otros a seguirla. Por ejemplo, en febrero de 2019, más de 200 empleados de Microsoft exigieron que la empresa cancelara un contrato de [480 millones de dólares](#) con el Ejército de Estados Unidos para suministrar a las tropas más de 100.000 auriculares HoloLens de realidad aumentada. La solicitud de propuestas del Pentágono planteaba la necesidad de una pantalla montada en la cabeza capaz de proporcionar a los soldados visión nocturna, apuntar con armas sigilosas y reconocer automáticamente las amenazas. Lo ideal sería que proporcionara a los soldados **“mayor letalidad, movilidad y conocimiento de la situación”**, según el anuncio.

En una [carta abierta](#) al consejero delegado de Microsoft, **Satya Nadella**, los trabajadores expresaron su preocupación por que, en manos de los militares, HoloLens pudiera “diseñarse para ayudar a matar”, “convirtiendo la guerra en un videojuego simulado”. Los empleados añadieron: “No firmamos para desarrollar armas, y exigimos poder opinar sobre cómo se utiliza nuestro trabajo”. Los [ejecutivos de Microsoft](#) se negaron a cancelar el contrato. **Nadella dijo: ‘no vamos a retener la tecnología de las instituciones que hemos elegido en las democracias para proteger las libertades de las que disfrutamos’.**

Durante el verano de 2018, aproximadamente **450 empleados del gigante tecnológico Amazon** firmaron una carta exigiendo que la empresa dejara de vender Rekognition -un programa de software de reconocimiento facial- a las fuerzas de seguridad. La carta de los empleados también pedía que la división de Servicios Web de Amazon dejara de alojar a Palantir, una empresa tecnológica que suministraba software de análisis de datos al Servicio de Inmigración y Control de Aduanas de Estados Unidos, ya que este organismo estaba deportando a menores no acompañados y a sus familias. El consejero delegado de Amazon, **Jeff Bezos**, se encogió de hombros ante la carta de los empleados. ‘Uno de los trabajos del equipo de liderazgo senior es tomar la decisión correcta incluso cuando no es popular’, dijo en octubre de 2018. ‘Si las grandes empresas tecnológicas van a dar la espalda al Departamento de Defensa de Estados Unidos, este país va a tener problemas’.

“Durante el verano de 2018, aproximadamente 450 empleados del gigante tecnológico Amazon firmaron una carta exigiendo que la empresa dejara de vender Rekognition -un programa de software de reconocimiento facial-

a las fuerzas de seguridad”

Mientras los trabajadores tecnológicos expresaban reticencias a involucrarse en proyectos militares, los ejecutivos vendían las mercancías de sus empresas a los funcionarios del Pentágono. Microsoft anunció [Azure Government Secret](#), un servicio en la nube para clientes del Departamento de Defensa y de la comunidad de inteligencia que requieren “cargas de trabajo clasificadas como US Secret”. Los [sitios web de Oracle](#) presumían de cómo sus productos “ayudan a las organizaciones militares a mejorar la eficiencia, la preparación de misiones y la ejecución”. Y Amazon creó un hábil vídeo promocional de [noventa segundos](#) en agosto de 2018, titulado simplemente ‘**Amazon Web Services for the Warfighter**’.

Contra la fusión de la gran tecnología y la gran defensa

Las tecnologías de Silicon Valley ilustran las consecuencias imprevisibles de la liberación de nuevos equipos o programas informáticos. **La idea de que un invento puede utilizarse con fines pacíficos o militares -es decir, la noción de tecnología de doble uso- se generalizó en la sociedad estadounidense durante el siglo pasado.** La historiadora **Margaret O’Mara** nos recuerda que durante la Guerra Fría, “el Valle construyó en pequeño: microondas y radares para comunicaciones de alta frecuencia, transistores y circuitos integrados. Silicon Valley construyó elegantes máquinas miniaturizadas que podían alimentar misiles y cohetes, pero que también tenían posibilidades de uso pacífico: relojes, calculadoras, electrodomésticos y ordenadores”.

Estas tecnologías siguen teniendo aplicaciones de doble uso. Google Earth puede emplearse para cartografía e investigación geográfica, pero también puede ser utilizado por equipos de las Fuerzas Especiales para atacar redes eléctricas, puentes u otras infraestructuras. Microsoft comercializó por primera vez las HoloLens como un dispositivo de realidad aumentada para jugadores, artistas y arquitectos, pero es probable que los consumidores más rentables sean los soldados de infantería. El programa de reconocimiento facial de Amazon podría utilizarse para transacciones bancarias o en cajeros automáticos seguros, pero también pueden emplearse como tecnologías de vigilancia por parte de organismos

militares, **de inteligencia o policiales como el Servicio de Inmigración y Control de Aduanas de Estados Unidos**. Las plataformas en nube que ofrecen Amazon, Oracle, Microsoft y Google pueden almacenar datos para investigadores científicos, funcionarios de salud pública o empresas comerciales. **Pero también pueden aumentar la letalidad de las fuerzas militares.**

Algunos podrían tachar a los ingenieros y científicos disidentes de Google de ingenuos. Al fin y al cabo, ¿no sabían dónde se metían? Si los científicos suelen entender que una vez que producen conocimiento, probablemente no tendrán control sobre cómo se utiliza, entonces seguramente debían entender que los dispositivos y aplicaciones que estaban creando podrían en algún momento convertirse en armas. ¿O no?

Es posible que muchos científicos e ingenieros que ahora se oponen al trabajo militar de Silicon Valley nunca hubieran imaginado que se verían arrastrados **al complejo militar-industrial-tecnológico**. Tal vez incluso decidieron trabajar para empresas tecnológicas porque pensaban que esas empresas no estaban en el negocio de las armas. Después de todo, la carta escrita por los manifestantes de Microsoft afirma: **“No firmamos para desarrollar armas”**.

También es posible que los investigadores depositaran una fe desmesurada en los ejecutivos de su empresa. En Google, los empleados se sintieron traicionados por las decisiones secretas que condujeron al contrato del Proyecto Maven.

La prensa económica reconoce periódicamente que la empresa tiene la mejor “cultura corporativa” de Estados Unidos, no sólo porque los empleados pueden llevar mascotas al trabajo y tienen acceso a comidas ecológicas preparadas por chefs profesionales, sino también porque la organización tiene fama de valorar la colaboración de los empleados.

Una vez que el Proyecto Maven salió a la luz, **la falsa conciencia de los trabajadores tecnológicos empezó a evaporarse**. Ganar seis cifras como ingeniero o programador recién salido de la universidad hace difícil pensar en uno mismo como proletario, especialmente cuando se disfruta de las ventajas que ofrece la industria: almuerzos gourmet gratuitos, gimnasios y guarderías gratuitas, por ejemplo. **Para miles de empleados, ser excluidos de los debates sobre si la empresa debía colaborar en el desarrollo de armas de inteligencia artificial despertó un sentimiento latente de conciencia de clase.**

También había otro problema: los antiguos vínculos de Silicon Valley con el Pentágono. Como se explica en este ensayo y como señala Margaret O'Mara, "Tanto si sus empleados se dan cuenta como si no, todos los gigantes tecnológicos actuales contienen algo de ADN de la industria de defensa...". . Esto implica un reconocimiento mucho más completo de la larga y complicada historia de Silicon Valley y el negocio de la guerra".

"Ganar seis cifras como ingeniero o programador recién salido de la universidad hace difícil pensar en uno mismo como proletario, especialmente cuando se disfruta de las ventajas que ofrece la industria"

* * * * *

La división entre el Pentágono y Silicon Valley es sobre todo un mito: nunca ha existido realmente, al menos de forma significativa. Las diferencias son superficiales y estilísticas. Durante casi un siglo, la economía y la cultura regionales han estado determinadas por lo que podría llamarse el complejo militar-industrial-universitario. Durante la Guerra Fría, el Pentágono ayudó a construir la industria informática concediendo contratos militares en campos como la electrónica de microondas, la producción de misiles y satélites y la investigación de semiconductores.

El historiador **Thomas Heinrich** nos recuerda que las descripciones populares de "ingeniosos inventores-empresarios y capitalistas de riesgo [que] forjaron una economía dinámica de alta tecnología libre de la pesada mano del gobierno" desvían la atención del papel crucial de "la financiación del Pentágono para la investigación y el desarrollo [que] ayudó a sentar las bases tecnológicas para una nueva generación de nuevas empresas" en el siglo XXI. Desde los años 50 hasta finales de los 90, el mayor empleador del sector privado de Silicon Valley no fue Hewlett Packard, Apple, Ampex o Atari. Era el gigante de la defensa Lockheed. Hoy la región se enfrenta a un patrón familiar, aunque el tamaño y la influencia de las empresas tecnológicas actuales empujan a las empresas informáticas de antaño.

Es probable que esto tenga importantes implicaciones en un futuro próximo. Jack Poulson, antiguo investigador científico de Google y cofundador de Tech Inquiry

Es probable que esto tenga importantes implicaciones en un futuro próximo. Jack

Poulson, antiguo investigador científico de Google y cofundador de Tech Inquiry (enlace externo), me lo explicó así: “Creo que estamos siendo testigos de la transición de las principales empresas tecnológicas estadounidenses a los contratos de defensa y me atrevería a pronosticar que en los próximos años comprarán contratistas de defensa, algo así como si Amazon comprara Raytheon”.

La verdadera línea divisoria no está entre el Pentágono y Silicon Valley. **Está dentro de Silicon Valley, donde un modesto contingente de ingenieros y científicos políticamente despiertos se han opuesto a la militarización de su trabajo.** Cuando se enfrenten a un ataque total de mensajes de relaciones públicas, campañas de concienciación, debates “colaborativos”, más compensaciones y prebendas -y quizás la amenaza tácita de perder sus puestos de trabajo o de que los subcontraten-, ¿se rendirán?

En este momento es demasiado pronto para saber el resultado, pero el futuro de la guerra virtual y los campos de batalla digitales puede estar en sus manos.

[LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ](#)

Fotografía: Alai

Fecha de creación

2023/07/19