Miguel Borrajo

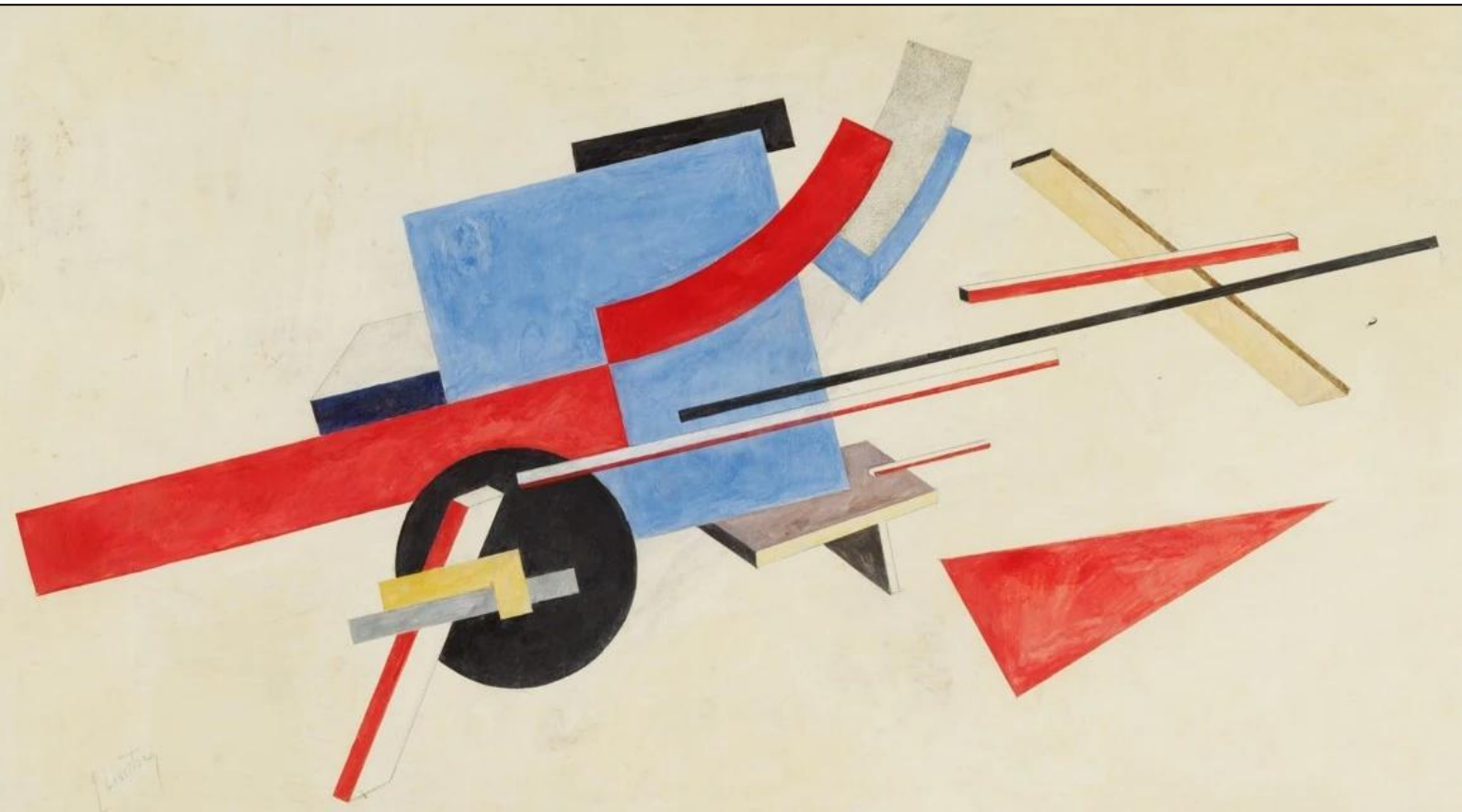
Veinte segundos para matar. La IA y la guerra automatizada

29/06/2026

Veinte segundos. Ese es el tiempo que tiene un analista militar para aprobar o rechazar un ataque. Sobre su pantalla, cuadros de vídeo seleccionados por un algoritmo ofrecen un abanico de probabilidades: 0,92 de que el punto brillante sea un lanzacohetes; 0,87 de que el edificio contiguo actúe como puesto de mando, 0,10 que se [...]

HISTORIA
POLÍTICA

12 min.



Veinte segundos. Ese es el tiempo que tiene un analista militar para aprobar o rechazar un ataque. Sobre su pantalla, cuadros de vídeo seleccionados por un algoritmo ofrecen un abanico de probabilidades: 0,92 de que el punto brillante sea un lanzacohetes; 0,87 de que el edificio contiguo actúe como puesto de mando, 0,10 que se trate de una familia con sus hijos. Si el cronómetro llega a cero, el misil parte a su destino. Si no, la oportunidad se esfuma. La escena no forma parte de la ciencia ficción, sino que se constituye como una forma de guerra ya en funcionamiento: una *cadena letal* acelerada por la inteligencia artificial, donde el juicio humano se ha reducido a una simple confirmación al final del proceso.

¿Cómo se ha llegado hasta aquí? ¿Qué tipo de historia, de organización social y de inversión técnica permite que una red neuronal, alojada en la nube, filtre objetivos militares como si se tratara de un sistema de recomendación? Para entenderlo tenemos que fijarnos en el lugar que ocupa la tecnología en el sistema de producción, y cómo fuerzas históricas —económicas, militares, estatales— la moldean desde su nacimiento.

A lo largo de las próximas secciones, se mostrará que la inteligencia artificial no surge como un proyecto motivado por la comprensión de la naturaleza del conocimiento, sino como la formalización de necesidades logísticas, militares e industriales contingentes. Para ello trazaremos un pequeño recorrido histórico por la consolidación de la inteligencia artificial como tecnología de mando: desde su origen militar, pasando por su implementación industrial, hasta su despliegue actual en infraestructuras privadas conectadas a la guerra. Esta historia no solo permite entender qué hace la IA, sino también qué se entiende por «inteligencia» dentro de las mismas fuerzas productivas que la impulsan: detectar-seleccionar-ejecutar.

I. La Guerra en el nacimiento del Estado moderno

En *Coercion, Capital and European States* (1992), Charles Tilly sostiene que los Estados europeos no surgieron de una evolución natural de las instituciones políticas, sino del entrelazamiento histórico entre tres fuerzas materiales: la guerra, el capital y la coerción organizada. Su tesis es que las transformaciones políticas y tecnológicas no

se explican por ideas ni valores, sino por la necesidad de financiar, sostener y coordinar la violencia armada. La forma estatal moderna no precede a la guerra, todo lo contrario, es su producto.

Durante la Edad Media tardía, la guerra era una actividad descentralizada. Los señores feudales movilizaban campesinos y mercenarios de forma temporal; la financiación dependía del saqueo o del tributo inmediato. Pero a medida que las armas de fuego y la artillería pesada transformaron el campo de batalla, el conflicto necesitó de una forma de inversión intensiva de capital. Los cañones, las fortificaciones de piedra, la pólvora y las flotas navales exigían un gasto continuo en materias primas, transporte y personal especializado. Tilly muestra que este cambio técnico y militar hizo inviable la guerra sin una base fiscal estable. «La guerra hizo al Estado moderno, y el Estado hizo la guerra», dirá Tilly. La fórmula resume una dialéctica en la que cada avance en coerción generaba nuevas necesidades de capital y nuevas instituciones para recaudar.

Más adelante, entre los siglos XIV y XVII, esa presión condujo a una reestructuración completa del poder político. Las ciudades comerciales del norte de Italia y los Países Bajos desarrollaron mecanismos de crédito público, letras de cambio y deuda soberana para financiar guerras prolongadas. Inglaterra y Francia, por su parte, consolidaron sistemas impositivos permanentes y aparatos administrativos capaces de sostener ejércitos profesionales. Las innovaciones técnicas —cañones fundidos, artillería móvil, cartografía precisa— se difundían solo cuando podían integrarse en esa nueva infraestructura fiscal. Tilly insiste en que la tecnología bélica no fue motor autónomo del cambio, sino un instrumento dependiente de la organización del capital; un medio subordinado a la capacidad de los gobernantes para recaudar, endeudarse y centralizar recursos.

Esa dinámica generó un proceso de selección histórica. Las unidades políticas que lograron institucionalizar un circuito estable entre coerción y capital sobrevivieron; las que no, desaparecieron o fueron absorbidas. Las pequeñas señorías y repúblicas comunales se vieron incapaces de sostener ejércitos permanentes frente a monarquías centralizadas con haciendas y tesorerías en expansión. La competencia bélica actuó como mecanismo evolutivo: solo los sistemas capaces de convertir

recursos económicos en poder militar —y viceversa— se consolidaron como Estados. A la inversa, la concentración del poder fiscal alimentó la capacidad de coerción: cuanto mayor el control tributario, mayor el ejército; cuanto mayor el ejército, mayor la capacidad de recaudar. El resultado fue la creación de lo que Tilly denomina «máquinas fiscales□militares».

El papel de la tecnología en este proceso fue doble. En primer lugar, amplió el radio de acción y el coste de la guerra. En segundo lugar, impulsó transformaciones administrativas destinadas a absorber esos costos: contabilidad pública, censos, catastros, archivos, estandarización de monedas y medidas. La tecnología de la coerción generó, indirectamente, la tecnología de la administración. A lo largo de los siglos XVII y XVIII, la generalización de la imprenta burocrática, los sistemas postales y los primeros telégrafos permitieron coordinar territorios cada vez más amplios bajo un mismo aparato estatal. Como subraya Tilly, la centralización política fue inseparable del desarrollo de las técnicas de registro y comunicación. La racionalidad burocrática —más tarde identificada por Weber como esencia del Estado moderno— emergió como consecuencia práctica de la necesidad de mantener la guerra a gran escala. En el siglo XIX, esta tendencia se consolidó con la industrialización. La expansión ferroviaria, el telégrafo y las nuevas armas de retrocarga transformaron la logística militar y la administración civil. El Estado se convirtió en gestor de infraestructuras, productor de estadísticas y regulador de flujos materiales y humanos. Tilly identifica aquí un punto crucial: la guerra moderna ya no dependía únicamente del ejército, sino de la capacidad de movilizar economías enteras. La frontera entre producción civil y militar se volvió porosa. La industria armamentística, las fábricas de acero y los bancos nacionales formaron un mismo ecosistema de poder. El Estado□Nación fue la forma política que mejor respondió a esa integración entre coerción y capital: suficientemente centralizado para imponer impuestos y conscripciones, pero lo bastante permeable para incorporar el crédito privado y la innovación técnica.

Así, lo que Tilly llama «máquinas fiscales-militares» designa una forma recurrente, muy actual, de articulación entre violencia, infraestructura y mando. A lo largo de la historia, las innovaciones técnicas más decisivas —desde la artillería hasta el telégrafo, desde el catastro hasta el cálculo estadístico— no fueron herramientas

elaboradas por el puro deseo de conocer, sino organizadas por necesidades concretas de control, extracción y ejecución. Esta dinámica continúa vigente bajo nuevas formas. Si el Estado moderno surgió para sostener la guerra industrial, las plataformas digitales actuales reconfiguran ese mismo mandato en clave algorítmica y transnacional.

II. El complejo digital-militar-industrial en la producción de la inteligencia

La dinámica que Tilly describe no ha desaparecido: se ha digitalizado. Si antes el Estado necesitaba arsenales y haciendas para sostener la guerra, hoy necesita centros de datos, contratos con plataformas tecnológicas y algoritmos de decisión. La inteligencia artificial no es ajena a esta historia, sino su continuación. Para comprenderlo, es necesario rastrear su nacimiento militar y su función actual como tecnología de mando letal.

1.1. Los ejes de la producción de la inteligencia militar

La inteligencia artificial no se conformó en torno a una gran pregunta filosófica (algo como «¿cuál es la naturaleza del conocimiento?»), sino alrededor de un encargo muy específico: organizar información y automatizar decisiones para la guerra. Desde el inicio se articularon tres ejes: primero, la capacidad de integrar señales y operar en tiempo real, como mostraron Whirlwind y SAGE; segundo, la formalización de la decisión en problemas bien definidos, impulsada por RAND y los programas de Simon y Newell; y tercero, la clasificación automática de datos ruidosos, inaugurada con el perceptrón de Rosenblatt. Ese conjunto —tiempo real, decisión formalizada y clasificación automática— estableció la gramática de lo que más tarde se llamaría «inteligencia artificial».

En los años cincuenta, el sistema SAGE (Semi-Automatic Ground Environment) supuso una infraestructura sin precedentes: costó unos 10 mil millones de dólares en 1954 —equivalente a 67 mil millones actuales, tres veces más que el Proyecto Manhattan— y conectó una red de radares distribuidos por toda Norteamérica con

ordenadores centrales y consolas de operador. Su propósito era acortar al máximo el tiempo entre detectar un avión enemigo y lanzar la respuesta: un circuito cerrado que integraba transmisión de datos, cálculo automático, autorización de mando y ejecución del ataque. Funcionó entre 1963 y 1984, consumía megavatios de energía y requería miles de operadores, pero estableció los fundamentos de tecnologías que luego derivarían en el tráfico aéreo civil, la informática en red y, en última instancia, en internet.

El precedente inmediato fue Whirlwind, un proyecto iniciado en el MIT en 1944 con financiación de la Marina estadounidense. Concebido originalmente como un simulador de vuelo, pronto se convirtió en el primer ordenador capaz de operar en tiempo real. A diferencia de las máquinas de cálculo por lotes de la época, que procesaban problemas matemáticos como extensas hojas de cálculo electrónicas, Whirlwind podía recibir señales de sensores, procesarlas en milisegundos y devolver resultados al operador casi instantáneamente.

De Whirlwind a SAGE se fijó un patrón que se volvería estructural en la era digital: integrar múltiples fuentes de señal, transportar datos sin interrupciones, computar con suficiente velocidad y situar al humano en un puesto de validación, cerrando así un circuito de «detectar-decidir-actuar». *Este fue el primer eje: la informática en tiempo real como herramienta para cerrar un ciclo de detección y respuesta*.

Al mismo tiempo, la RAND Corporation, creada en 1946 como brazo analítico de la Fuerza Aérea de EE. UU., se convirtió en el espacio donde los dilemas de la guerra nuclear y la administración militar se tradujeron en problemas de cálculo sistemático. Como documenta Paul Edwards en *The Closed World* (1996), lo que urgía era fijar protocolos operativos: decidir qué señales contaban como amenaza, cómo combinar fuentes de información ruidosa, en qué punto una probabilidad debía activar una alerta y con qué reglas debe actuarse al detectar una anomalía.

En ese entorno trabajaron Herbert Simon y Allen Newell, que disponían en RAND del JOHNNIAC, uno de los pocos ordenadores de gran escala de la época. Su acceso privilegiado a tiempo de máquina y financiación militar les permitió experimentar con algo que excede el cálculo numérico: la posibilidad de formalizar el propio

proceso de decisión. De ahí surgieron programas como *Logic Theorist* (1956), concebido para reproducir demostraciones de los axiomas del *Principia Mathematica*, y el *General Problem Solver* (1957), pensado para aplicar ese mismo procedimiento a cualquier dominio representable. Ambos partían de la teoría de la decisión que Simon había formulado en *Administrative Behavior* (1947): la idea de que la acción racional consiste en recorrer un «espacio de problemas» delimitado, identificar alternativas, evaluar costes y justificar elecciones. Su aportación fue decisiva: redefinieron la inteligencia como la capacidad de resolver problemas bien formulados en espacios cerrados, donde cada paso podía justificarse y rastrearse. Esto los hacía perfectamente funcionales en el marco que RAND y proyectos como SAGE necesitaban: procedimientos previsibles, trazabilidad de cada decisión y ejecución en tiempos controlados. *Aquí se consolidaba el segundo eje: la formalización de la decisión en protocolos claros y problemas bien definidos*.

En esa misma trayectoria se inscribe el perceptrón de Frank Rosenblatt, desarrollado en 1957 con financiación de la Oficina de Investigación Naval. Aunque a menudo se lo presenta como un intento de imitar el cerebro, su diseño era mucho más pragmático: una máquina de clasificación capaz de procesar entradas sensoriales (como una cámara rudimentaria de 20×20 píxeles), ajustar sus parámetros y distinguir patrones elementales entre datos ruidosos. Su interés militar era evidente: automatizar la detección de blancos, filtrar señales útiles y reducir la incertidumbre en los sistemas de vigilancia.

En paralelo, figuras como Marvin Minsky impulsaban desde el plano conceptual una definición de la inteligencia entendida como un repertorio de técnicas aplicables al control y la resolución de problemas. Su obra Steps Toward Artificial Intelligence (1961), elaborada con John McCarthy y financiada por los servicios conjuntos de las Fuerzas Armadas, funcionó como catálogo de métodos y como hoja de ruta para orientar la investigación. Ese mismo ecosistema cristalizó en el *MIT Artificial Intelligence Laboratory*, fundado en 1959, que desde su inicio se sostuvo mediante contratos del Pentágono y de *DARPA*. El laboratorio operaba como nodo estratégico en una red de defensa y gestión de infraestructuras, donde universidad, Estado e industria trabajaban de manera conjunta. *Ese fue el tercer eje: la clasificación automática*

de señales y la capacidad de extraer patrones fiables en condiciones de ruido e incertidumbre.

De estos tres ejes podemos lanzar una hipótesis: cuando las infraestructuras, los recursos y los incentivos están alineados en torno a la optimización del mando, el control y la automatización, es inevitable que el concepto mismo de inteligencia que se va consolidando en estos entornos termine siendo definido en términos de funcionalidad organizativa. Inteligencia, entonces, pasa a significar la capacidad de una máquina para ejecutar operaciones que permiten decidir más rápido, con mayor precisión y menor incertidumbre, dentro de sistemas jerárquicos y altamente estructurados. Esa es la inteligencia que interesa —y que se financia— en este marco. Bajo esta lógica, el proyecto de la Inteligencia Artificial se define, convirtiéndose en una ingeniería de la decisión operativa. Con el tiempo, esa deriva del concepto se convierte, a su vez, en una narrativa de progreso: más datos procesados, menor latencia, mayor acierto empiezan a parecer sinónimos de «más inteligente». El relato se constituye así de tal manera que parece que la tecnología avanza hacia una «inteligencia superior». Algunas grandes empresas como *OpenAI* o *Microsoft* incluso tienen acuerdos sobre la AGI (Inteligencia Artificial General), la inteligencia general, una inteligencia que «superará a la humana», (signifique lo que signifique eso). En realidad es la inercia de un aparato diseñado para acortar ciclos de decisión instrumentales y estandarizar procesos a gran escala, una idea de inteligencia que encaja a la perfección con los objetivos de las industrias militar y civil precisamente porque nace en los laboratorios de ambas.

1.2. La consolidación de la IA en la industria

El recorrido histórico que aquí desarrollo se apoya en el trabajo de Jonnie Penn, cuya tesis *Inventing Intelligence* (2020) documenta con detalle cómo la IA se configuró, desde mediados del siglo XX, como una tecnología orientada a resolver los problemas de mando y control propios de la guerra y de la administración estatal. A partir de archivos, contratos y discursos técnicos, Penn muestra que los laboratorios que prosperaron fueron aquellos capaces de alinear sus investigaciones con esta lógica operativa.

Sin embargo, aunque los orígenes de la inteligencia artificial están indisolublemente ligados a la planificación militar y la gestión estatal, fue en el sector industrial donde la IA se consolidó como fuerza productiva. A partir de los años 50, corporaciones como *IBM, General Motors y General Electric* identificaron en la computación simbólica y el control automático una solución directa a los límites de la gestión tradicional: el tiempo muerto en la producción, la dependencia del conocimiento tácito de los operarios y la autonomía relativa de los trabajadores cualificados. Penn documenta cómo IBM, a través de su División de Investigación, estandarizó lenguajes como FORTRAN para facilitar la programación científica al mismo tiempo que invertía activamente en centros universitarios (*Stanford, Carnegie Mellon, MIT*) para alinear la investigación académica con sus objetivos comerciales y operativos. En este proceso, pensar se convirtió, una vez más, en una operación formalizable: seleccionar información relevante, procesarla según reglas explícitas y ejecutar un resultado. Este desplazamiento conceptual tuvo efectos materiales precisos. En 1956, *General Motors* financió junto al *MIT* el desarrollo del sistema *APT* (*Automatically Programmed Tool*), una infraestructura de programación para el control numérico. Su objetivo era recentralizar la autoridad técnica y eliminar la necesidad de operarios expertos. Como señala Penn, este movimiento fue percibido como una forma de «disipar la capacidad de acción» de los maquinistas veteranos, históricamente ligados al sindicalismo. En palabras de Harry Braverman, citado por Penn, se trataba de una «transferencia sistemática del saber hacia el capital» o, más bien, un traslado de la información desde el trabajo vivo (capital variable) hacia el trabajo muerto (capital constante). La IA no solo automatizaba tareas, además, definía quién tenía derecho a intervenir.

El patrón se repite en distintos niveles. A medida que la informática se expandía, IBM priorizó modelos de interacción que facilitaran el control remoto de grandes volúmenes de datos, mientras que el Pentágono financiaba redes de tiempo compartido (como ARPANET) para conectar centros de mando. Penn detalla cómo esta racionalidad técnica fue impulsada por los mismos actores que promovieron la automatización industrial, eliminando sistemáticamente la variabilidad humana del núcleo operativo. El resultado fue una convergencia estratégica: los laboratorios más financiados eran aquellos que ofrecían soluciones al problema del control, no

aquellos que exploraban la complejidad de la cognición.

La historia industrial de la IA muestra un interés persistente en redefinir el trabajo, la autonomía y la inteligencia desde una lógica de instrumentalización. Los sistemas diseñados para sustituir al operador humano en el taller migraron al espacio digital, al análisis financiero, a la logística militar. El principio técnico era el mismo: reducción de incertidumbre, maximización del control, exclusión de la subjetividad.

III. Corporaciones, guerra y automatización

Los tres ejes que fundaron la IA en los cincuenta —tiempo real, decisión formalizada y clasificación automática— no quedaron en el MIT ni en RAND: hoy son la gramática de las arquitecturas digitales. Lo que antes cerraba un bucle radar-misil ahora articula nube, sensores planetarios y algoritmos de selección de objetivos. La línea es continua: de SAGE a Project Maven, de RAND a Azure, del perceptrón a las redes que criban imágenes satelitales. No estamos ante una novedad, sino ante la actualización de un mismo dispositivo. Y mientras los titulares fantasean con una «inteligencia general», las herramientas ya cumplen su función: reducir incertidumbre, acortar la decisión, estandarizar la ejecución. Dos escenas lo muestran con nitidez: el monopolio transnacional del *cloud* y la introducción de la IA en la selección de objetivos militares.

3.1 El monopolio transnacional del cloud

El despliegue contemporáneo de la inteligencia artificial no puede entenderse sin mirar quién controla los medios de producción sobre los que se ejecutan. Lo que en los años cincuenta eran sótanos llenos de válvulas y cables —los radares de SAGE, los simuladores de RAND— hoy son granjas de servidores distribuidas por todo el globo. Pero la lógica es la misma: centralizar la información, reducir la latencia, asegurar el mando. La diferencia es que esa centralización ya no se organiza desde un único laboratorio estatal, sino desde un monopolio transnacional corporativo que concentra la capacidad de cómputo global. Tres empresas —Amazon, Microsoft, Google— dominan el mercado del cloud en Occidente y han convertido sus centros

de datos en nodos estratégicos del complejo digital-militar-industrial. OpenAI opera sobre Microsoft Azure y Oracle Cloud (proyecto Stargate); Anthropic entrena sus modelos sobre AWS (Project Rainier) y Google Cloud; xAI construye sus propios centros (Colossus, en Memphis) pero todos dependen de la misma arquitectura de GPU Nvidia y de contratos con el Pentágono.

Amazon Web Services (AWS), pionera en este terreno, aloja desde 2013 la infraestructura de la comunidad de inteligencia estadounidense (contrato C2S, Cloud Commercial Services), renovada en 2020 como C2E por 10.000 millones de dólares. AWS es el sistema circulatorio de la CIA y la NSA. *Microsoft Azure*, a través de su división *Government*, maneja entornos clasificados para el Pentágono. Fue la gran competidora en el contrato JEDI (Joint Enterprise Defense Infrastructure), pensado para unificar toda la nube del antiguo Departamento de Defensa en un solo entorno operativo; aunque JEDI se disolvió en 2021, el nuevo contrato multicloud (JWCC) volvió a recaer en los mismos actores. *Google Cloud Plataform*, tras la protesta masiva de sus empleados en 2018 contra *Project Maven* (del que hablaremos en un momento), prometió no renovar su participación en ese proyecto. Pero siguió vinculada a contratos de ciberseguridad y análisis de datos para aliados estratégicos, desde el Reino Unido hasta Israel, y hoy forma parte también del JWCC.

A este reparto se sumó *Oracle*, incorporada tras haber denunciado el contrato JEDI por favorecer un monopolio tecnológico. Aunque su cuota de mercado es marginal, su inclusión en el JWCC respondió a la necesidad institucional de diversificar el proveedor y contener futuras impugnaciones legales. *Oracle* opera hoy como actor funcional en ciertos nichos militares donde la latencia y la trazabilidad son críticas, pero su peso estructural es muy inferior al de los tres gigantes.

El caso de *OpenAI* muestra cómo esta infraestructura dual se ha normalizado. Hasta enero de 2024, sus términos de uso prohibían aplicaciones militares. En ese mismo mes, la compañía modificó la política: ya no prohíbe «military and warfare», sino solo el desarrollo o uso de armas y el daño directo a personas. En junio de 2025, el Departamento de Defensa adjudicó a *OpenAI Public Sector LLC* —la filial de *OpenAI* dedicada a relaciones institucionales— un contrato de 200 millones de dólares mediante un *other transaction agreement*, un mecanismo legal del Pentágono que evita

las cargas administrativas de los contratos públicos tradicionales y favorece la agilidad en proyectos tecnológicos. El contrato, gestionado por la *Chief Digital* and *Artificial Intelligence Office* (CDAO), establece el desarrollo de «capacidades de IA de frontera para abordar desafíos críticos de seguridad nacional en dominios de combate y empresariales», con plazo de finalización en julio de 2026. Los casos de uso incluyen ciberdefensa, procesamiento automatizado de datos, apoyo a misiones, optimización administrativa y acceso a servicios de salud para el personal militar. En julio de 2025, *OpenAI* recibió un segundo contrato por el mismo monto, esta vez junto a *Anthropic*, *Google* y *xAI*, para desarrollar flujos de trabajo de agentes digitales destinados a misiones de seguridad nacional. Ambos contratos forman parte de la iniciativa *OpenAI for Government*, que consolida proyectos con los laboratorios nacionales de Los Alamos, Livermore y Sandia, la NASA, el NIH y el Departamento del Tesoro. La misma infraestructura de nube (Azure), las mismas arquitecturas de modelo (transformers) y los mismos métodos de entrenamiento sirven tanto para aplicaciones civiles como para contratos de defensa. La frontera entre uno y otro uso no es técnica, sino contractual y administrativa.

El resultado es una paradoja: la misma infraestructura que se presenta como civil —chatbots, almacenamiento de correos electrónicos, procesamiento de pagos, catálogos de fotos personales— aloja también sistemas de defensa y procesamiento de inteligencia militar. AWS gestiona datos clasificados de la CIA y la NSA; Azure opera entornos del Pentágono; *Google Cloud* mantiene contratos de ciberseguridad con aliados estratégicos. Los centros de datos, los métodos de optimización y las arquitecturas de modelo no distinguen entre usos: la diferencia la establece el contrato, no la tecnología. De este modo, la genealogía se cierra sobre sí misma: lo que RAND imaginó como cálculo sistemático y lo que SAGE ejecutó como cadena de detección y respuesta reaparece en 2025 en forma de clusters de AWS, *Azure* y *Oracle*, con contratos de defensa firmados en salas de juntas privadas.

3.2 Selección automática de objetivos militares

Lanzado en 2017 por el antiguo Departamento de Defensa de EE. UU., *Project Maven* fue diseñado para traducir las promesas del aprendizaje automático en ventajas operativas inmediatas. Su lógica era directa: emplear visión por computador y fusión

de sensores para acelerar la *cadena letal*, la secuencia que va de detectar a disparar. Donde antes hacían falta miles de analistas revisando horas de vídeo de drones, Maven prometía reemplazarlos con redes neuronales alojadas en *GovCloud*, la nube gubernamental operada por Amazon y Google. En ejercicios como *Scarlet Dragon*, imágenes satelitales entraban en el sistema, un algoritmo marcaba posibles blancos, y un operador humano debía validar rápidamente el objetivo antes de que un lanzacohetes HIMARS ejecutase el ataque.

Según el Pentágono, el sistema automatiza cuatro de los seis pasos tradicionales de la cadena letal, permitiendo a un equipo reducido tomar hasta 80 decisiones de ataque por hora. Si antes el proceso implicaba descubrir, fijar, rastrear, apuntar, atacar, evaluar, ahora se limita, en la práctica, a Atacar y Evaluar. Tras los ataques del 7 de octubre de 2023, Israel adoptó y radicalizó esta lógica. Dos sistemas, *Gospel* (Habsora) y *Lavender*, operaron como fábricas algorítmicas de objetivos. *Gospel* generaba coordenadas a partir de inteligencia multifuente —viviendas, antenas, edificios civiles convertidos en blancos—, mientras que *Lavender* cruzaba decenas de miles de nombres gazatíes con indicadores de afiliación a milicias. En ambos casos, el operador humano aparecía solo al final de la cadena, con apenas unos segundos para aprobar cada ataque. Según testimonios recogidos por *+972 Magazine* y *Local Call*, ese tiempo de validación era tan reducido que la intervención humana equivalía a «un sello de aprobación». Aunque estas cifras no provienen de documentos oficiales, múltiples relatos coinciden en señalar un margen operativo de segundos, con umbrales predefinidos de «bajas civiles aceptables».

Parte de esta infraestructura corría sobre *Microsoft Azure*, la misma nube que aloja datos corporativos a escala global. En 2025 se reveló que Azure había almacenado llamadas interceptadas por la *Unity 8200*, una unidad de inteligencia israeli, con el objetivo de almacenar grabaciones de llamadas interceptadas por la población palestina. Microsoft anunció una suspensión parcial, sin romper sus contratos de ciberseguridad con el Estado israelí.

Lo que antes eran pasos discretos en una cadena de decisión hoy se condensa en un flujo continuo, donde los algoritmos proponen y los humanos confirman por inercia. La cadena letal se convierte ahora en una interfaz: una máquina de letalidad

estadística en la que la incertidumbre se procesa como probabilidad, y la validación como trámite.

IV. Coerción, capital e infraestructura: una lectura desde Tilly

El enfoque de Tilly permite comprender el presente. Las infraestructuras computacionales actuales cumplen, en parte, funciones que se asemejan a las de los archivos estatales: registrar, clasificar, hacer trazable. Pero van más allá: no solo almacenan información, sino que procesan datos en tiempo real para acelerar la toma de decisiones operativas. Las plataformas de targeting, los sistemas de fusión de sensores y los modelos de clasificación automática no tienen equivalente directo en el arsenal del Estado moderno; son dispositivos nuevos que integran vigilancia, análisis y propuesta de acción en un mismo flujo. La diferencia clave es que estas funciones han sido, en gran medida, externalizadas hacia empresas privadas. Plataformas como *Microsoft Azure, AWS o Google Cloud* alojan procesos decisivos para el ejercicio contemporáneo de la fuerza, bajo contratos financiados con fondos públicos y orientados a optimizar velocidad, cobertura y control. Desde esta perspectiva, la inteligencia artificial no aparece como una disrupción epistemológica, sino como una reconfiguración de los medios materiales del mando. La reducción del juicio humano a una validación de segundos no es consecuencia de una lógica puramente técnica, sino de un marco organizativo que prioriza latencia, escalabilidad y eficiencia por encima de trazabilidad o deliberación. La forma que adopta hoy la inteligencia refleja esas prioridades.

En este sentido, la lección que deja Tilly es que cuando coerción y capital se articulan de forma estable a través de tecnología e infraestructura, producen formas específicas de orden político. La decisión letal computacionalista no puede ser desmantelada desde el plano individual. Requiere una respuesta organizada, estructural y colectiva, que no solo dispute los efectos, sino también las condiciones materiales que los hacen posibles. Esto tiene implicaciones políticas concretas. Si las condiciones necesarias de la decisión letal automatizada dependen de estructuras contractuales, infraestructuras técnicas y flujos financieros, entonces la respuesta no

puede limitarse a una ética del diseño ni a una regulación de dispositivos aislados. Se trata de intervenir sobre los puntos de apoyo del sistema: la financiación pública, las cláusulas de los contratos, la propiedad y localización de los centros de datos, las condiciones laborales del trabajo técnico y los mecanismos de inspección y control.

Estas arquitecturas de decisión son síntomas de una reorganización profunda del mando, la letalidad y la infraestructura digital. Desde *Maven* hasta *Lavender*, pasando por enjambres, drones autónomos y plataformas de tiro asistido por IA, se consolida un modelo donde el vínculo humano se reduce —cuando existe— a un clic. Los sensores alimentan modelos alojados en la nube, los modelos calculan probabilidades, los sistemas actúan. La decisión se descentraliza hacia el perímetro (*edge computing*), pero el poder se concentra más que nunca en infraestructuras privadas. Microsoft Azure, Amazon Web Services, Google Cloud. Estados Unidos, Europa y, cada vez más, China. La guerra contemporánea ya no se sostiene únicamente sobre arsenales físicos, sino sobre clusters de entrenamiento, contratos de hosting y arquitecturas opacas de decisión que los coordinan y activan. Hoy, más que nunca, la centralización que mencionaba Tilly se articula en torno a núcleos empresariales.

Este desplazamiento, a su vez, redefine qué cuenta como inteligencia. Siguiendo a Jonnie Penn, la IA representa una cristalización de formas estadísticas, computables y clasificatorias de saber, que despolitizan la toma de decisiones y neutralizan la deliberación de la misma forma en que lo hace cualquier proceso burocrático. Estamos ante una estructura transnacional donde el desarrollo tecnológico, el diseño computacional y los marcos legales se entrelazan para producir muertes en serie. La responsabilidad se diluye: ¿quién responde cuando la decisión se toma entre sensores, funciones de pérdida y servidores alquilados? Por eso la respuesta no puede limitarse a regular armas autónomas como si fueran objetos aislados. Se trata de confrontar las condiciones materiales que las hacen posibles: las empresas que entrenan, alojan y venden estos sistemas; los Estados que los compran sin rendición de cuentas; las arquitecturas que distribuyen la decisión sin repartir la responsabilidad, y la estructura social que pone el beneficio privado por encima del colectivo.