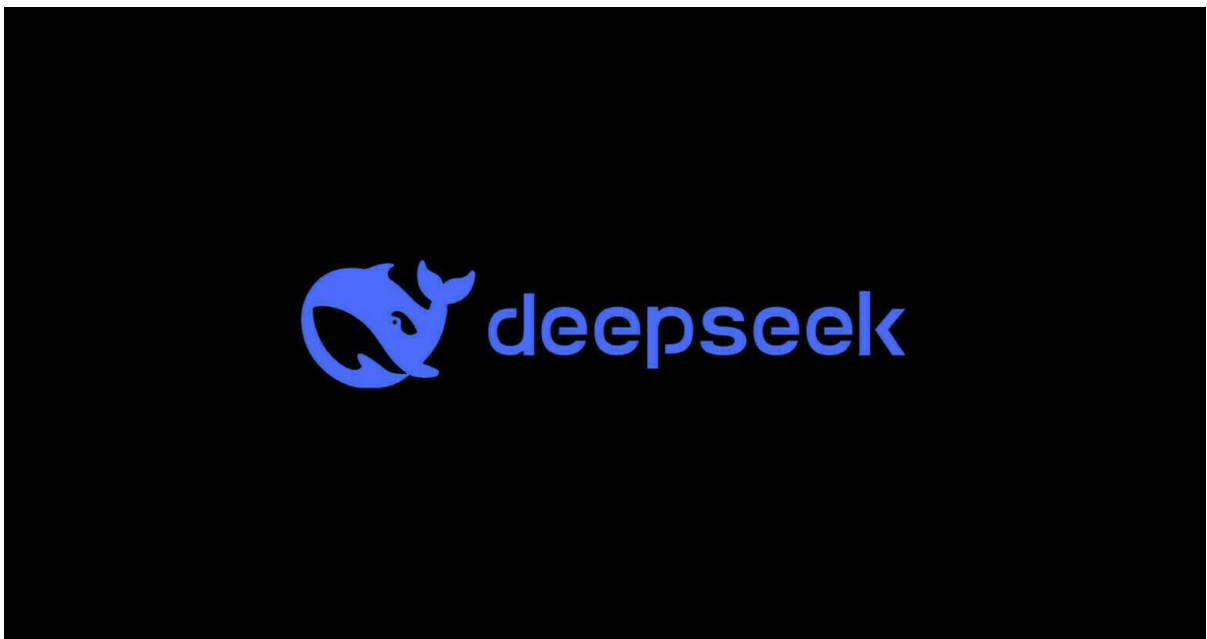


La IA en tiempos de guerra

Javier Borràs Arumí, CIDOB



Las tecnologías de doble uso civil-militar

- Las tecnologías de doble uso toman más relevancia
- Dos en concreto están cambiando la guerra: los **drones** y la **inteligencia artificial**
- Debate abierto y politizado sobre **qué es una tecnología de doble uso**: ¿un vehículo eléctrico o un drone agrícola lo son, porque recaban datos?



Tecnologías “democratizadoras” de la guerra

- Tanto la IA como los drones son **tecnologías que “democratizan” la guerra**, ya que son baratas y accesibles (Scharre, 2026): tanto estados ricos como pobres, actores estatales como no estatales, pueden acceder a ellas
- Son tecnologías que benefician el **poder asimétrico**: el lado débil gana ventaja
- Crean una asimetría de recursos:
 - Drone iraní de 35.000\$ interceptado por misil estadounidense de 4.000.000\$;
 - Tener un equipo de analistas de datos con una suscripción de 20 euros a un modelo de IA
- **China tiene una posición central como proveedor** de ambas tecnologías “democratizadoras” de la guerra

China: líder en drones

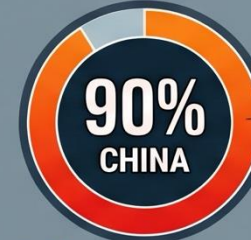
▶ UCRANIA: DRONES EN COMBATE



+70%
DE BAJAS
EN UCRANIA
SON CAUSADAS
POR DRONES



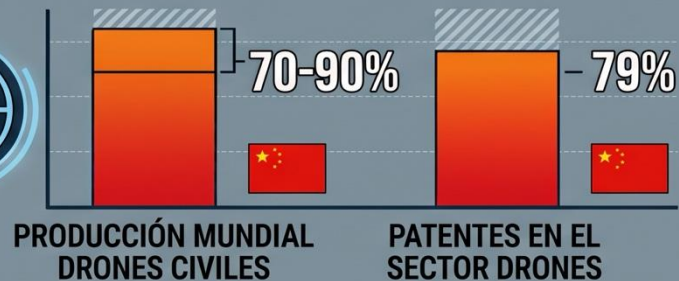
▶ ORIGEN DE LOS DRONES EN UCRANIA



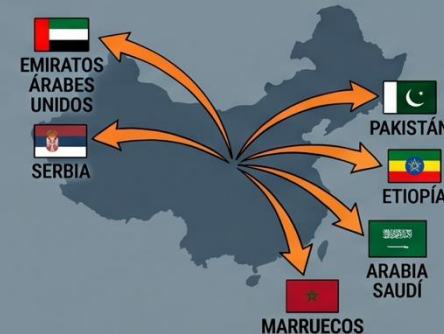
+90% DE DRONES UTILIZADOS EN
UCRANIA USAN COMPONENTES CHINOS



▶ PRODUCCIÓN Y PATENTES GLOBALES DE DRONES



▶ EXPORTACIONES MILITAR DE PEKÍN



PEKÍN ES EL MAYOR
EXPORTADOR DE DRONES
MILITARES



EVOLUCIÓN Y TIPOS DE OPERACIONES CON DRONES

PETRAEUS & FLANAGAN, 2026

1) DRONES AUTÓNOMOS (Presente)



Llegan al objetivo sin GPS y con la conexión rota.

2) ENJAMBRES DE DRONES COORDINADOS POR IA



Coordinación, comunicación y reacción en tiempo real dirigidos a nivel de enjambre.

3) FORMACIONES AUTÓNOMAS



Coordinación de drones autónomos de diferentes entornos.

4) EL FUTURO: OPERACIONES TOTALMENTE AUTÓNOMAS



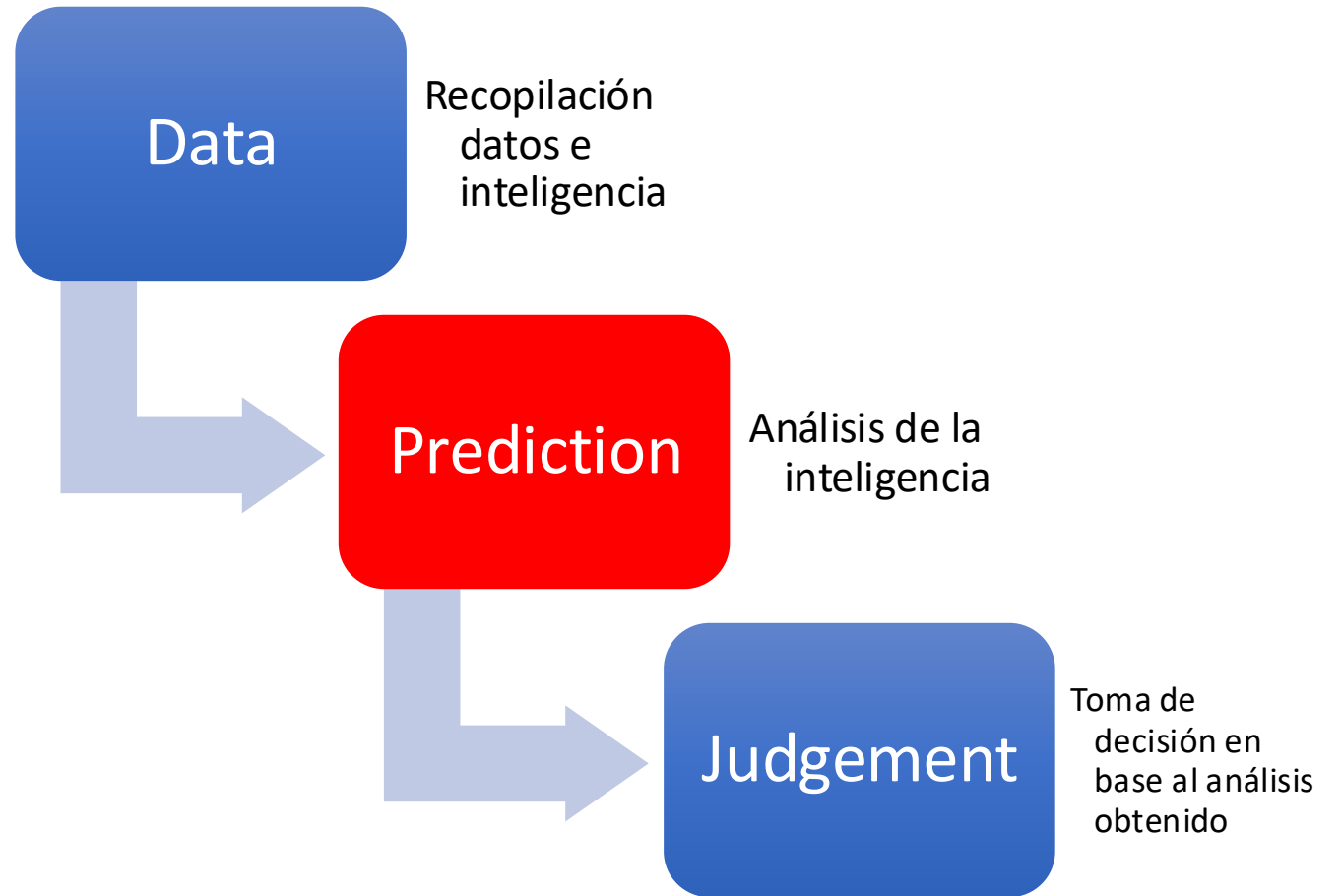
Toda la operación es autónoma, adaptándose y tomando decisiones para lograr objetivos.

La democratización de la IA

- **Modelos cerrados estadounidenses** (Claude, OpenAI, Gemini...) vs **modelos abiertos chinos** (Deepseek, Moonshot, Qwen...)
- Los modelos de pesos abiertos tienen **mayor capacidad de modificación (fine-tuning)**, gratuitos a nivel de licencias y suelen requerir **menos poder computacional**
- Especialmente beneficiosos para **actores con pocos recursos**: start-ups, países en desarrollo, grupos no estatales
- **Dos tipos de supervisión**: en modelos cerrados la propia compañía vs en modelos abiertos el proveedor de nube

El impacto de la IA en las operaciones militares

- La IA puede sintetizar datos e inteligencia de manera masiva, pero **el humano sigue teniendo un rol central**
- Tres fases claves según Goldfarb & Lindsay: **Data – Prediction – Judgement**
- En este contexto, son más peligrosos los **ciberataques** que puedan corromper los datos o las **operaciones de desinformación** que afecten a la toma de decisiones



Goldfarb & Lindsay, 2022

Despliegue actual de IA en operaciones militares

- Estados Unidos usando modelos de IA de Claude o Open AI en guerra contra Irán
- Israel usando modelos Lavender o Gospel, para identificación de objetivos humanos o de infraestructura
- China tiene doctrina militar de 'intelligentization' (智能化) que se construye sobre 'informatization' (信息化)
- Los centros de datos de IA ya son objetivos militares: ataques UAE y Bahrein en marzo/abril 2026

Impacto “democratización” de IA en ciberseguridad

- Un **ataque contra infraestructura crítica** que antes era cosa de especialistas y demandaba recursos y tiempo, ahora es más accesible
- Al tener conocimiento “especializado” de protocolos y sistemas de control de múltiples infraestructuras, se puede realizar “**disrupción coordinada**” (agua, electricidad, tránsito...) (Sulmeyer, 2026)
- Rol de los **agentes autónomos** de IA – pueden quedar ‘incrustados’ (embedded) y durmientes en infraestructura, y activarse en momento crítico
- Estados y grandes empresas pueden usar IA para mejorar su ciberseguridad, pero hay una **desigualdad asimétrica**

Drones e IA: actores no estatales

- Estas tecnologías “democratizadoras” pueden ser ventajosas para actores no estatales de importancia en Latinoamérica, como el **crimen organizado**
- Uso drones por parte de carteles mexicanos; ataques y contrabando en cárceles Ecuador; vigilancia favelas en Brasil;
- Uso IA para clonación de voz y deepfakes para simulación de secuestros en México y Argentina; falsificación de documentos e identidades en frontera USA-México; facilitación lavado de dinero en México y Brasil;
- En clima geopolítico tenso, **oportunidad de coordinación** entre USA y China, con LATAM y Europa, para prevenir uso por parte de grupos crimen organizado

¡Gracias!

Substack: <https://javierborras.substack.com/>

Linkedin: Javier Borràs Arumí