

La guerra algorítmica: cómo los drones, la IA y los deepfakes cambiaron el rumbo de los conflictos bélicos

09/03/2026



Las **guerras actuales** ya no se definen solo por la potencia de fuego o el tamaño de los ejércitos, sino por la **capacidad de procesar datos, controlar redes** y operar sistemas tecnológicos complejos: la **inteligencia artificial**, la **vigilancia satelital**, los **drones de bajo costo** y los **ataques cibernéticos** ya transformaron la forma en que se desarrollan, y ganan, los conflictos bélicos.

Así lo afirmó a **TN Tecno** Eduardo Laens, especialista en IA, docente universitario: “La imagen clásica que tenemos de la guerra, con trincheras, soldados con fusiles y generales moviendo fichas en un mapa de papel, quedó obsoleta”, explicó. “Hoy **la guerra se libra en servidores en la nube** de algún proveedor de TI, en el espectro electromagnético y **a través de**

algoritmos de IA”.

Según el especialista, el escenario actual recuerda a otros momentos en los que una innovación tecnológica alteró de forma radical el equilibrio militar global. “Estamos atravesando lo que diplomáticos y analistas ya bautizaron como el ‘**momento Oppenheimer de nuestra generación**’”, afirmó.



La guerra algorítmica: los drones, IA y deepfakes cambiaron el rumbo de los conflictos bélicos. (Imagen generada por IA/ADobeStock)

La diferencia es que ahora el cambio no se limita a una nueva arma, sino que **afecta a toda la infraestructura tecnológica** que sostiene las operaciones militares, y la guerra se volvió tan tecnológica que un simple fallo de software, un centro de datos comprometido o un algoritmo sesgado pueden alterar el destino de naciones enteras.

Drones baratos y guerra electrónica

Uno de los factores más visibles de esta transformación es la expansión del **uso de drones en el campo de batalla**. Los vehículos aéreos no tripulados, especialmente los modelos de visión en primera persona, **modificaron la relación entre costo y capacidad de destrucción**. En conflictos recientes, **drones** relativamente baratos lograron destruir equipamiento militar extremadamente costoso.

“Hoy un drone de visión en primera persona que cuesta unos **400 dólares** puede destruir tanques de combate principales valorados en **2 millones de dólares**”, explicó Laens, que además de autor del libro *Humanware*, es el CEO de la empresa Varegos, empresa especializada en Hiperautomatización.

El impacto es particularmente evidente en la guerra entre Ucrania y Rusia, donde el especialista afirma que los drones generan entre el 70% y el 80% de las bajas en el frente.

Pero la operación de estos sistemas depende de otro elemento clave: la conectividad. En ese punto **aparece la guerra electrónica**, un frente invisible que busca interferir señales, bloquear comunicaciones o inutilizar sistemas enemigos mediante el **control del espectro electromagnético**.

De acuerdo con Laens, algunas fuerzas militares desplegaron sistemas diseñados específicamente para **interferir radares, satélites y comunicaciones** en grandes áreas, lo que convierte a las redes de comunicación en un objetivo estratégico central.

A esto se suma la **integración entre inteligencia artificial**, sensores y constelaciones de satélites capaces de detectar movimientos y procesar enormes volúmenes de información en [tiempo real](#).

“Se generan exabytes de datos en el llamado borde táctico”,

explicó el especialista. “Las corporaciones de defensa están creando ecosistemas de computación en la nube para procesar esos datos sensoriales y alimentar directamente a sistemas de misiles guiados con mínima intervención humana”.

Silicon Valley, el Pentágono y el debate sobre la ética de la IA

La creciente **dependencia militar de la inteligencia artificial** también provocó tensiones entre gobiernos y empresas tecnológicas.

Tradicionalmente, el desarrollo de armamento estaba en manos de compañías del sector defensa. Hoy, buena parte del software que impulsa estos sistemas se desarrolla en empresas tecnológicas.

Ese cambio quedó expuesto en un **conflicto reciente entre el Departamento de Defensa de Estados Unidos y compañías del sector de IA**. Según explicó Laens a **TN Tecno**, el gobierno estadounidense exigió a proveedores tecnológicos aceptar cláusulas que permitieran el uso de sus modelos de inteligencia artificial para “cualquier uso legal”.

Una de las compañías involucradas fue [Anthropic](#), dirigida por Dario Amodei, que rechazó esas condiciones: “La empresa se negó a permitir que su tecnología se utilizara para diseñar armas totalmente autónomas o para vigilancia masiva nacional”, señaló. La respuesta del gobierno fue **excluir a la compañía de contratos federales bajo argumentos vinculados con la seguridad nacional**.

Poco después, **OpenAI firmó un acuerdo con el Pentágono** y eliminó sus restricciones anteriores sobre uso militar para asegurar el contrato.

La decisión generó reacciones entre los usuarios de sus productos. La tasa de [desinstalaciones de la aplicación](#)

[ChatGPT](#) se disparó un 295% el 28 de febrero de 2026. Al mismo tiempo, la base de usuarios del modelo Claude creció más de un 60%.

Centros de datos y redes como objetivos militares

En el contexto actual, la infraestructura tecnológica se convirtió en un objetivo estratégico dentro de los conflictos.

Centros de datos, cables de telecomunicaciones, redes de internet y plataformas digitales pasaron a ser piezas clave para el funcionamiento de gobiernos, economías y operaciones militares. “La **ciberseguridad** ya no es una función de soporte en la retaguardia”, afirmó Laens. “Se transformó en un **dominio principal del conflicto bélico**”.

El especialista mencionó episodios recientes en Medio Oriente, donde ataques físicos y cibernéticos se combinaron contra infraestructuras tecnológicas. Entre ellos se registró un incendio en un centro de datos operado por la división de nube de Amazon en Emiratos Árabes Unidos después de que las instalaciones fueran alcanzadas durante intercambios de ataques.

En paralelo, grupos hacktivistas realizaron **ofensivas de denegación de servicio contra bancos, aerolíneas y organismos gubernamentales** en distintos países de la región.

Deepfakes y la guerra psicológica

Otro frente clave es el de la información. Las herramientas de **inteligencia artificial generativa** permiten producir audios, imágenes y videos hiperrealistas que pueden utilizarse para propaganda o **manipulación informativa**.

Durante la guerra en Ucrania circuló un **video falsificado** del

presidente Volodymyr Zelensky anunciando la rendición de su país. En paralelo también aparecieron contenidos falsos atribuidos al presidente ruso Vladimir Putin.

Sin embargo, Laens sostuvo que el impacto más profundo no siempre está en el engaño directo: “El daño más insidioso de los *deepfakes* no es necesariamente que la gente crea la mentira. El problema es que **generan lo que se conoce como el ‘dividendo del mentiroso’**: cuando todo puede ser falso, entonces cualquier evidencia real puede descartarse como generada por IA”.

Ese fenómeno puede afectar incluso investigaciones sobre crímenes de guerra o abusos documentados en video. En ese contexto, el especialista advirtió que **la dimensión tecnológica de los conflictos seguirá creciendo en los próximos años**.

“La carrera armamentista ya no se libra únicamente en fábricas de municiones”, concluyó. “Se libra en salas de servidores, donde la ciberseguridad, los datos y la inteligencia artificial determinan quién gana la guerra y cómo se redefine el valor de la vida humana”.

Fuente: TN