IA, CRIMEN ORGANIZADO Y SEGURIDAD EN MÉXICO: ¿QUIÉN CONTROLA LA TECNOLOGÍA?

CREATED BY
GARCIA
RODRIGUEZ USIEL

INTRODUCCIÓN: MÉXICO ANTE LA VIOLENCIA MODERNA

- México enfrenta una crisis de seguridad: homicidios, narcotráfico, desapariciones, ciberextorsión.
- La tecnología (IA incluida) ya forma parte de este conflicto, tanto del lado del Estado como del crimen organizado.
- Pregunta central: ¿Quién está aprovechando la IA? ¿Para proteger o para controlar?

CRIMEN ORGANIZADO Y TECNOLOGÍA EN MÉXICO

Lo que ya ocurre:

- Drones con explosivos: Usados por el CJNG (Cártel Jalisco Nueva Generación) para atacar a rivales o fuerzas de seguridad en Michoacán, Zacatecas, Jalisco.
- Intervención de comunicaciones: Uso de software avanzado para rastrear o intervenir dispositivos.
- Ciberextorsión y phishing: Ataques cibernéticos a personas, empresas y gobiernos locales.
- Narcomensajes deepfake: Uso potencial de IA para crear audios/videos falsos que intimiden o difundan desinformación.

GOBIERNO Y FUERZAS DE SEGURIDAD

¿Cómo usan la IA o tecnologías avanzadas?

- Reconocimiento facial: Implementado en CDMX para vigilancia urbana y estaciones del Metro.
- Plataformas de análisis criminal predictivo: Algunas policías usan software para identificar zonas de riesgo (aún poco público).
- Drones de vigilancia y cámaras con IA: Proyecto de seguridad urbana con empresas privadas (como Hikvision, Dahua).

Problemas:

- Corrupción e infiltración del crimen organizado en cuerpos policiales.
- Riesgo de abuso de estas tecnologías (vigilancia masiva sin control legal).
- México carece de regulación específica sobre el uso ético de IA en seguridad.

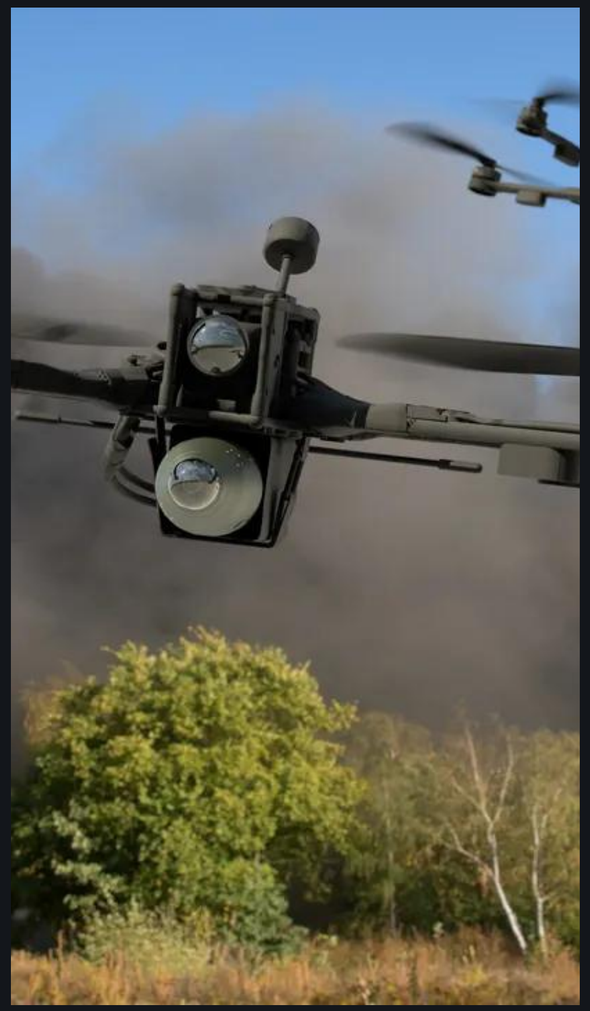
CIBERSEGURIDAD NACIONAL

Amenazas actuales:

- Hackeo a instituciones públicas: Ejemplo: Guacamaya Leaks (2022), revelaron información del Ejército.
- Ataques a PEMEX y bancos: Ransomware que paralizó operaciones.
- Poca preparación del gobierno en ciberdefensa basada en IA.

Falta de protección:

- Solo existen iniciativas fragmentadas del gobierno para ciberseguridad.
- INE, SEDENA, IMSS y universidades han sido víctimas de ataques, muchas veces sin seguimiento público.



EL LADO OSCURO: POSIBLE USO FUTURO DE IA POR CÁRTELES

¿Qué podría pasar si acceden a modelos avanzados?

- Generar miles de mensajes falsos para manipular la opinión pública.
- Ubicar blancos mediante reconocimiento facial desde drones.
- Crear deepfakes de políticos, amenazas o confesiones falsas.

CONCLUSIÓN

- México está en una zona gris tecnológica: El Estado usa herramientas con IA, pero el crimen también está modernizándose.
- Sin regulación ni estrategia nacional de ciberdefensa con IA, México queda vulnerable.
- Reflexión final: ¿Quién debe controlar esta tecnología? ¿Y qué riesgos hay si no se hace nada?

REFERENCIAS

- Newton, C. (2024, agosto 26). Cuatro formas en que la IA está transformando el crimen organizado en América Latina. InSight Crime. https://insightcrime.org/es/noticias/cuatro-formas-inteligencia-artificial-transformando-crimen-organizado-america-latina/
- Orgaz, C. J. (2024, octubre 4). Inteligencia artificial: 6 maneras en que grupos criminales de América Latina usan la IA para delinquir. BBC. https://www.bbc.com/mundo/articles/crej5gwllvlo
- Redactores, R. (2025, abril 16). México emplea inteligencia artificial y combate al crimen organizado. Reseller. https://reseller.com.mx/mexico-emplea-inteligencia-artificial/
- (S/f). Com.mx. Recuperado el 21 de mayo de 2025, de https://prevenet.com.mx/la-delincuencia-organizada-en-mexico-aliada-de-la-tecnologia-y-las-criptomonedas/

GARCIA RODRIGUEZ USIEL

GRACIAS

GARCIA RODRIGUEZ USIEL