

CLAVES CEEYPP — PANORAMA PARA LA DECISIÓN · N° 8

Crimen organizado e inteligencia artificial: la brecha entre la guerra territorial y la soberanía cognitiva

Dr. Norberto Emmerich

Centro de Estudios en Estrategia y Políticas Públicas — Septiembre de 2026

Resumen

La convergencia entre crimen organizado e inteligencia artificial ha abierto una brecha profunda entre dos formas de comprender y disputar el territorio en América Latina. Este paper examina cómo las organizaciones criminales, particularmente los cárteles del narcotráfico, han adoptado tecnologías de inteligencia artificial para optimizar sus operaciones, desde la logística del trasiego de drogas hasta la extorsión automatizada mediante deepfakes. A través del análisis de casos documentados en México, Colombia, Ecuador y Bolivia, se evidencia que el crimen organizado ha experimentado una metamorfosis tecnológica que lo posiciona como un actor pionero en la adopción de herramientas digitales avanzadas. El trabajo sostiene que esta transformación no solo incrementa la eficacia de las operaciones criminales, sino que redefine la naturaleza misma del conflicto: mientras el Estado conserva la ventaja en la guerra territorial —fuerza letal, control físico, presencia militar—, el crimen organizado avanza hacia una soberanía cognitiva sobre el territorio, comprendiéndolo y anticipándolo a través de datos que el Estado no procesa. La asimetría resultante no es una simple carrera armamentística, sino una cesión estructural de capacidades de seguridad, agravada por la dependencia algorítmica de los Estados y por la disputa hegemónica global entre China y Estados Unidos. El trabajo concluye que esta brecha entre guerra territorial y soberanía cognitiva constituye uno de los mayores desafíos para la seguridad regional en la próxima década.

Palabras clave: crimen organizado, inteligencia artificial, narcotráfico, América Latina, soberanía cognitiva, drones

1. Introducción

Durante décadas la imagen del narcotráfico latinoamericano estuvo asociada a “monsters trucks”, suburbans todoterreno, radios de corto alcance y hombres armados imponiendo su control territorial mediante el ejercicio aplastante de la violencia. Esta imagen, aunque todavía sigue vigente en el terreno, ha quedado obsoleta. Las organizaciones criminales de alto riesgo han experimentado una transformación profunda que las ha convertido en cuerpos capaces de operar con la sofisticación de las corporaciones multinacionales, incorporando tecnologías de vanguardia que incluyen la inteligencia artificial, los drones armados, las redes de comunicación satelital y los sistemas de análisis predictivo.

Esta adaptación tecnológica no es un fenómeno marginal. Un estudio publicado en septiembre de 2025 por el investigador Juan Manuel Aguilar Antonio del CISAN-UNAM, como parte del programa europeo PACCTO 2.0, documenta que organizaciones mexicanas tales como el Cártel de Sinaloa y el Cártel Jalisco Nueva Generación (CJNG) utilizan algoritmos, bots y sistemas de automatización en sus operaciones cotidianas, que van desde las extorsiones hasta el narcotráfico.

El análisis, divulgado en el repositorio oficial Zenodo de la Comisión Europea y el CERN, clasifica a estas organizaciones como “jerárquicos clásicos” que incorporan la IA para mejorar su logística, aunque ya muestran tendencias hacia modelos más sofisticados como plataformas autónomas de servicios criminales.

La relevancia de este fenómeno radica en la asimetría que genera. Mientras los cárteles capitalizan rápidamente las tecnologías emergentes, las instituciones estatales enfrentan limitaciones presupuestarias, burocráticas y de conocimiento especializado que les impiden seguir el mismo ritmo. Esta brecha tecnológica no solo incrementa la eficacia de las operaciones criminales, sino que erosiona la capacidad del Estado para proteger a la ciudadanía y mantener el monopolio de la fuerza.

La brecha tecnológica entre el crimen organizado y el Estado es tan profunda que permite formular la siguiente hipótesis: no existe un dilema de seguridad entre la utilización de la inteligencia artificial por parte de las organizaciones criminales y el retraso estatal en incorporarla como instrumento de las políticas de seguridad interior. Dicho de otro modo, no se trata de una carrera armamentística simétrica, sino de una

relación asimétrica donde uno de los actores ya ha tomado la delantera.

El presente trabajo tiene como objetivo analizar el uso que el crimen organizado, con especial énfasis en las organizaciones dedicadas al narcotráfico en América Latina, hace de la inteligencia artificial. Se examinarán casos documentados en México, Colombia, Ecuador y Bolivia, así como las implicaciones para la seguridad regional y las respuestas estatales frente a esta nueva realidad.

2. Marco conceptual: la cuarta revolución criminal

2.1. Del crimen tradicional al crimen 4.0

La evolución del crimen organizado en América Latina puede entenderse como una serie de saltos cualitativos:

- El "crimen 1.0" correspondería a las organizaciones tradicionales basadas en el control territorial y la violencia física directa.
- El "crimen 2.0" incorporó capacidades de comunicación cifrada y logística sofisticada.
- El "crimen 3.0" representa la expansión transnacional con redes diversificadas de negocios ilícitos.
- El "crimen 4.0", objeto de este análisis, se caracteriza por la integración sistémica de tecnologías emergentes, particularmente la inteligencia artificial, en todas las fases de la operación criminal.

Esta cuarta generación no se limita a la adopción de gadgets tecnológicos aislados. Como señala Aguilar, la IA "no funciona como gadget, sino como sistema", integrando desde los bots conversacionales que inducen al pago bajo amenaza hasta los algoritmos que seleccionan víctimas por su perfil psicológico. La orden criminal ya no solo desciende a lo largo de la cadena de mando, se programa.

2.2. Tipologías de adopción tecnológica

El estudio del PACCTO 2.0 establece cuatro tipologías de grupos criminales según su nivel de adopción tecnológica:

- Jerárquicos clásicos: organizaciones con estructuras verticales tradicionales que incorporan la IA para optimizar la logística y las comunicaciones. El CJNG y el Cártel de Sinaloa se ubican dentro de esta categoría.
- Cibercolectivos: grupos que operan principalmente en entornos digitales, sin una presencia territorial significativa.
- Plataformas autónomas: estructuras que venden servicios criminales basados en la IA bajo el modelo Crime-as-a-Service (CAAS), incluyendo herramientas como FraudGPT, DarkBARD y Xanthorox AI.
- Actores paraestatales: organizaciones que emplean la IA para el control territorial y político, con capacidades cuasi-estatales.

La evolución de los cárteles mexicanos a lo largo de las categorías descritas evidencia una tendencia preocupante: la incorporación tecnológica en el crimen organizado no sigue una lógica escalonada ni secuencial, sino que avanza "a saltos". Las organizaciones no transitan de un estadio al siguiente en orden progresivo: combinan capacidades heterogéneas, de modo que un grupo con comunicaciones rudimentarias puede acceder simultáneamente a información sofisticada, y uno que apenas se tecnifica hoy puede diseñar mañana mapas territoriales anticipatorios.

2.3. Desarrollo desigual y combinado: la heterogeneidad tecnológica del crimen organizado

La incorporación tecnológica en el crimen organizado no sigue una lógica escalonada ni secuencial. Las organizaciones no transitan de un estadio al siguiente en orden progresivo, sino que combinan capacidades heterogéneas, de modo que un grupo con comunicaciones rudimentarias puede acceder simultáneamente a

información sofisticada y uno que apenas se tecnifica hoy puede diseñar mañana mapas territoriales anticipatorios. Este comportamiento responde a una doble dinámica: por un lado, una desigualdad entre las capacidades disponibles dentro de una misma organización y entre organizaciones comparables; por otro, una combinación funcional de lo técnicamente avanzado con lo socialmente atrasado.

Desigualdad interna y entre organizaciones

El primer rasgo se observa en el interior de los propios cárteles mexicanos. Aunque el CJNG y el Cártel de Sinaloa se ubican en la categoría de "jerárquicos clásicos", ya muestran tendencias hacia tipologías más sofisticadas. Esto significa que operan simultáneamente en distintos estadios de desarrollo tecnológico: mientras algunas células siguen utilizando métodos tradicionales de extorsión, otras emplean algoritmos de segmentación de víctimas por perfil psicológico.

InSight Crime documentó la existencia de los "Operadores Droneros", una unidad especializada del CJNG dedicada exclusivamente al manejo de drones y artefactos explosivos, que utiliza equipos comerciales adaptados —no fabricados internamente— para lanzar bombas contra fuerzas de seguridad y grupos rivales. Mientras tanto, otras células de la misma organización dependen de métodos de extorsión telefónica tradicionales o incluso de vigilancia humana básica. La coexistencia de una unidad tecnológicamente avanzada con estructuras operativas convencionales dentro del mismo cártel ilustra la desigualdad interna de capacidades.

La desigualdad también se manifiesta entre organizaciones de escala comparable. El estudio del PACCTO 2.0 señala que, mientras el CJNG ha centralizado el desarrollo de esquemas de extorsión automatizada con IA generativa, el Cártel de Sinaloa ha adoptado una lógica de replicación descentralizada: diversas células operan de manera autónoma en la ejecución de campañas de smishing, lo que facilita una rápida adopción de herramientas como deepfakes o geolocalización automatizada, muchas veces sin necesidad de una estructura de mando centralizada. Dos organizaciones de peso similar desarrollan, así, capacidades tecnológicas dispares, con arquitecturas organizativas distintas para integrar la misma tecnología.

Combinación de lo avanzado y lo rudimentario

El segundo rasgo es la articulación funcional de capacidades que, en una lógica secuencial, serían incompatibles. En las fronteras de Bolivia, los grupos de contrabando combinan drones de última tecnología —uno de ellos recibió disparos y "las balas no le hicieron nada"— con personas ancianas apostadas en la frontera, dotadas de teléfonos celulares básicos, para reportar los movimientos de las patrullas. Modifican sus vehículos para que las llantas soporten "colas de lagarto" (alfombras de clavos) y utilizan equipos sofisticados de comunicación por radiofrecuencia. Lo técnicamente avanzado y lo socialmente atrasado coexisten y se articulan funcionalmente. La vigilancia humana precarizada no es un residuo del pasado, sino un componente activo del dispositivo.

Un patrón análogo se observa en el plano financiero. El Cártel de Sinaloa ha integrado modelos de inteligencia artificial con criptomonedas y tecnología blockchain para triangular las ganancias del tráfico de fentanilo, convirtiéndolas en yuanes con la complicidad de casas de cambio chinas. Esta capacidad financiera sofisticada coexiste con métodos tradicionales de lavado de dinero en sectores como ganadería, minería y construcción. La organización combina lo más avanzado de las finanzas digitales con lo más arcaico de la economía informal.

La combinación también opera en el plano del reclutamiento. Una investigación del Civic AI Lab de la Northeastern University y El Colegio de México reveló que TikTok se ha convertido en herramienta de reclutamiento para los cárteles mexicanos: se identificaron 100 cuentas activas vinculadas a organizaciones ilícitas, de las cuales el 47% promovía el reclutamiento de nuevos miembros y el 31% difundía propaganda, con el CJNG representando el 54.3% de las cuentas detectadas. Al mismo tiempo, esas mismas

organizaciones utilizan IA para clonar voces de familiares en extorsiones telefónicas. La manipulación emocional más primitiva se articula con la tecnología de síntesis de voz más avanzada.

El salto como forma del avance

Los expertos describen el uso de drones explosivos como un "salto tecnológico" y un "salto táctico". David Saucedo, analista de seguridad, explica que "al principio solo eran herramientas de vigilancia y con el tiempo les añadieron bombas de contacto y un mecanismo para programar su detonación gracias al conocimiento de algunos ingenieros contratados". Este salto no siguió una progresión lineal: las organizaciones pasaron directamente de la vigilancia básica al ataque con explosivos, sin desarrollar capacidades intermedias. La investigadora Dulce Torres, del Colmex, señala que "lo que más me preocupa es la intimidación de la población. Literalmente usan los drones para causar un desplazamiento forzado de las comunidades".

2.4. Síntesis

Estos ejemplos demuestran que el crimen organizado no tecnifica sus operaciones siguiendo una secuencia ordenada ni lineal. Sigue, en cambio, un proceso contradictorio —complejo y necesariamente adaptativo— que responde a las circunstancias propias de la expansión y la urgencia:

- Coexisten capacidades de distinto nivel dentro de una misma organización (unidades especializadas en drones junto a células que operan con métodos tradicionales).
- Se combinan tecnologías avanzadas con métodos rudimentarios de forma funcional (drones de última generación con espías ancianos; IA generativa con explotación de vulnerabilidades humanas básicas).
- Se saltan etapas de desarrollo tecnológico (de la vigilancia básica al ataque con explosivos sin pasos intermedios).
- Diferentes organizaciones desarrollan capacidades desiguales para integrar la misma tecnología (CJNG centralizado vs. Sinaloa descentralizado).

No se trata de una escalera que asciende peldaño a peldaño, sino de una combinación heterogénea de capacidades que se articulan según las necesidades operativas y las oportunidades tecnológicas disponibles en el mercado.

3. Aplicaciones de la Inteligencia Artificial por el narcotráfico

3.1. Extorsión automatizada y Deepfakes

Una de las aplicaciones más documentadas del uso de la IA por las organizaciones criminales es la extorsión mediante deepfakes y clonación de voz. El Cártel Jalisco Nueva Generación y el Cártel de Sinaloa han utilizado inteligencia artificial generativa para replicar voces de familiares o figuras de autoridad con alto nivel de fidelidad acústica, montando escenarios de secuestro, emergencia médica o coerción judicial.

La capacidad de simular interacciones conversacionales verosímiles a través de modelos de lenguaje entrenados para sostener diálogos prolongados ha sido esencial para el éxito de los esquemas de fraude afectivo y emocional. Los bots conversacionales programados con IA permiten escalar la extorsión sin recurrir a la interlocución humana directa, detectando patrones emocionales en las respuestas de la víctima y ajustando su tono o contenido en tiempo real para maximizar la presión psicológica.

En Bolivia, el Clan San Roque ha experimentado con videos falsos de secuestros para extorsionar a familiares de víctimas a cambio de criptomonedas. Esta modalidad, conocida como "secuestro virtual", reduce drásticamente el riesgo para los perpetradores mientras mantiene altos niveles de efectividad en la presión sobre las víctimas.

3.2. Optimización logística y análisis predictivo

Los cárteles utilizan algoritmos de inteligencia artificial para analizar datos masivos que informan sobre las rutas marítimas, el movimiento de las fuerzas de seguridad, los patrones de consumo local y los territorios de control de los grupos rivales. Mediante un análisis predictivo se pueden anticipar los operativos de las fuerzas de seguridad y planificar emboscadas o eficientizar las rutas de traslado sin depender exclusivamente de los informantes humanos, más lentos y proclives al error.

La conectividad satelital de baja órbita ha permitido a los cárteles mantener una comunicación estable en medio del océano, la sierra o la selva. Los narco-submarinos y los semisumergibles han evolucionado hasta convertirse en vehículos controlados remotamente, siguiendo determinadas rutas calculadas por software y reportando su posición a través de sistemas de rastreo avanzados. Se ha documentado el desarrollo de submarinos semiautónomos capaces de transportar hasta 10 toneladas de droga.

3.3. Drones armados y vigilancia aérea

El uso de drones por organizaciones criminales representa una de las problemáticas más significativas. El CJNG creó una unidad especializada en aeronaves no tripuladas conocida como "Operadores de Drones", integrada por expertos que utilizan estos dispositivos para inteligencia, vigilancia, reconocimiento, propaganda intimidatoria y ataques.

Las cifras son elocuentes: de cinco ataques con drones atribuidos al narcotráfico en el año 2020, el CJNG pasó a 107 en 2021, 233 en 2022 y 260 solo en el primer semestre de 2023. Los criminales utilizan modelos comerciales como el DJI Mini 3, modificados con tubos galvanizados que contienen pólvora, perdigones o fragmentos metálicos. El CJNG emplea drones agrícolas DJI Agras T40, capaces de transportar sustancias tóxicas o explosivos líquidos para causar mayor daño.

En Ecuador, los atentados con drones cargados de explosivos contra ciertos pabellones carcelarios en Machala y la utilización de drones agrícolas modificados para transportar armamento hacia los centros penitenciarios evidencian una nueva dimensión de la eficiencia criminal. La disputa entre el Estado ecuatoriano y las organizaciones como Los Lobos y Los Choneros ya no se libra únicamente en las calles, sino también en el espacio aéreo de baja altura.

Colombia ha documentado más de 350 ataques con drones en el pasado año 2025, con un saldo de 15 muertos y 170 heridos, atribuidos principalmente al accionar de las disidencias de las FARC que no adhirieron al acuerdo de paz del año 2016.

4. Casos documentados en América Latina

4.1. México: el CJNG y el Cártel de Sinaloa

México constituye el caso paradigmático de la transformación tecnológica del crimen organizado. El CJNG, descrito por la DEA como "una organización terrorista en todos los niveles", opera en más de 40 países y ha demostrado una capacidad de adaptación tecnológica sin precedentes.

Además del uso de drones armados, el CJNG ha sido vinculado a hackeos de sistemas de videovigilancia en la Ciudad de México y al robo de datos de un teléfono de un agente del FBI, según manifestó el Departamento de Justicia de Estados Unidos. La organización ha diversificado sus ingresos mediante esquemas de lavado de dinero en sectores como ganadería, minería, agricultura y construcción, utilizando criptomonedas como Bitcoin, Tether y Monero.

Un estudio de El Colegio de México en colaboración con el Civic AI Lab de Northeastern University reveló que TikTok se ha convertido en una herramienta de reclutamiento apta para los cárteles mexicanos. Se identificaron 100 cuentas activas vinculadas a organizaciones ilícitas, de las cuales el 47% promovía el reclutamiento de nuevos miembros y el 31% difundía propaganda. El CJNG representaba el 54.3% de esas

cuentas detectadas.

4.2. Colombia: escenarios multictipos y dependencia algorítmica

Colombia enfrenta un escenario de "multictipos" donde las organizaciones ya no dependen de una sola actividad ilegal, sino que participan simultáneamente en narcotráfico, minería ilegal, extorsión y tráfico de migrantes. El Clan del Golfo, el ELN y las disidencias de las FARC han incorporado tecnologías avanzadas en sus operaciones.

Según el libro "Seguridad en Colombia en tiempos de inteligencia artificial" de la exvicepresidenta Marta Lucía Ramírez, las problemáticas actuales son "profundamente diferentes" a las de comienzos de siglo, y en consecuencia requiere respuestas estatales igualmente modernas y coordinadas. En el año 2025 Colombia superó las 253,000 hectáreas sembradas de coca, con una producción potencial de más de 2,650 toneladas métricas de cocaína. El porcentaje de participación de Colombia en el mercado mundial de cocaína crece año tras año, llegan en este momento al 70% del porcentaje global.

Un desafío adicional que no puede obviarse es la dependencia algorítmica. Los expertos advierten que Colombia carece de la infraestructura tecnológica para desarrollar sistemas avanzados de IA para seguridad y defensa, lo que la obliga a depender de tecnologías desarrolladas por empresas privadas extranjeras como OpenAI, Anthropic o Google DeepMind. Esto plantea interrogantes sobre la soberanía algorítmica y la capacidad de auditar y gobernar sistemas críticos de seguridad.

4.3. Ecuador: guerra de drones, crimen transnacional y dependencia algorítmica

El caso ecuatoriano adopta una forma aún más aguda. En enero de 2026, el gobierno anunció una alianza con Palantir Technologies para establecer en el país el primer nodo regional de la empresa en Sudamérica, destinado al control fronterizo, la vigilancia de actividades ilegales en minería y pesca, y el análisis integrado de datos de seguridad social. El acuerdo generó cuestionamientos sobre la soberanía de los datos y la gobernanza algorítmica. Aunque el gobierno sostiene que la información se almacenará en servidores locales, el funcionamiento del software exige que técnicos de Palantir tengan acceso completo a los datos y los especialistas advierten que el país podría convertirse en un "campo de pruebas" cuyos patrones de datos serían luego exportados a las naciones vecinas. A esto se suma que Ecuador carece todavía de una ley integral de regulación de la inteligencia artificial. En agosto de 2026, la Comisión de Educación de la Asamblea Nacional recomendó archivar un proyecto que llevaba dos años de discusión, alegando deficiencias técnicas, riesgo de sobre-regulación del ecosistema digital y problemas de constitucionalidad.

El resultado es una contradicción estructural: por un lado, el Estado externaliza capacidades críticas de seguridad a favor de una empresa privada extranjera mientras al mismo tiempo carece de los instrumentos institucionales para auditarla, supervisarla y exigirle rendición de cuentas. La capacidad técnica se incorpora con rapidez en nombre de la "eficiencia", mientras la capacidad de gobernanza —auditoría, jurisdicción sobre los datos, transparencia algorítmica— queda sistemáticamente rezagada. Es la forma típica de la dependencia algorítmica: no es una simple transferencia de tecnología, sino una cesión estructural de capacidades de seguridad.

Ecuador emerge como el epicentro de la confrontación tecnológica entre el Estado y las organizaciones criminales transnacionales. La disputa entre las fuerzas de seguridad y grupos como Los Lobos y Los Choneros ha trasladado la confrontación al espacio aéreo.

Los operativos que culminaron con las capturas de alias "Sampayo" en Machala y alias "Churrón" en Guayaquil contaron con el apoyo de sistemas de vigilancia aérea que permitieron monitorear los objetivos en tiempo real. Sin embargo, las organizaciones criminales también han incorporado drones para vigilancia de movimientos policiales, monitoreo de rutas ilícitas y, en casos extremos, transporte de explosivos y ataques

dirigidos.

Un estudio de la Universidad de las Fuerzas Armadas del Ecuador señala que, aunque no existe información pública concluyente sobre un uso sistemático de la IA por parte de las organizaciones criminales locales, se identifican indicios de adopción progresiva de herramientas tecnológicas tales como drones modificados, sistemas de comunicación encriptados y análisis de información geoespacial. El país enfrenta "un escenario de alta vulnerabilidad frente a la tecnologización del crimen organizado".

En Ponce Enríquez, cantón de la provincia ecuatoriana de Azuay, incluso bajo el estado de excepción decretado en julio de 2024 por “grave conmoción interna” y “conflicto armado interno”, la respuesta estatal se articuló sobre plataformas convencionales, no sobre sistemas algorítmicos. El Ejército desplegó 200 efectivos con vehículos tácticos e intervino directamente en las minas, mientras la Fuerza Aérea enfrentaba limitaciones para operar por las condiciones del terreno montañoso y nublado. La vigilancia de la zona dependía de tropas especializadas y patrullajes presenciales, no de análisis automatizado de datos. Esta carencia no es casual: la propia Estrategia Nacional de IA (EFIA-EC, enero de 2026) describe el uso estatal de esta tecnología en Ecuador como “experiencias aisladas sin una estrategia coordinada”, y el país figura como “adoptante tardío” con una inversión en I+D equivalente apenas al 0,44% del PIB.

En un territorio donde el crimen organizado disputa el control de una economía minera que genera USD 3,5 millones mensuales, el Estado desplegó una fuerza letal, pero no inteligencia algorítmica. La brecha no es de presencia, sino de capacidad cognitiva: el territorio se vigila con helicópteros, pero no se comprende con algoritmos. El Estado puede estar físicamente presente en Ponce Enríquez y, al mismo tiempo, carecer de los instrumentos inteligentes para procesar la información que esa presencia genera.

4.4. Bolivia: deepfakes y extorsión con criptomonedas

En Bolivia, el caso del Clan San Roque ilustra una modalidad emergente de uso criminal de la inteligencia artificial. El grupo, cuyo nombre proviene del penal de San Roque en Chuquisaca donde se originó su operación, empleó en 2025 herramientas de IA para clonar la voz del exministro de Educación Omar Veliz Ramos. A través de las redes sociales, la organización difundió ofertas de empleo que parecían auténticas —atribuidas a la voz sintetizada del exfuncionario— para captar víctimas y generar ganancias ilícitas que superaron los 720.000 dólares.

Esta modalidad delictiva combina dos elementos que potencian su eficacia: por un lado la credibilidad que otorgan los deepfakes, cuyo realismo dificulta su detección incluso cuando los receptores sospechan que el contenido es artificial; por otro, la utilización de criptomonedas para el cobro de rescates o pagos, que aprovecha la percepción —no siempre exacta— de que las transacciones con activos virtuales son imposibles de rastrear.

Aunque la blockchain de Bitcoin es pública y las transacciones son seudónimas (no anónimas) la conversión a efectivo o el uso de mezcladores y billeteras intermedias dificultan la identificación de los beneficiarios finales. El Clan San Roque encarna una tendencia incipiente pero significativa en la que las organizaciones criminales no requieren infraestructura tecnológica propia para acceder a las capacidades de la IA generativa que están disponibles comercialmente y las combinan con instrumentos financieros digitales para reducir su exposición y maximizar el impacto psicológico sobre las víctimas.

5. Implicaciones para la seguridad regional

5.1. La asimetría tecnológica

La brecha tecnológica entre las organizaciones criminales y el Estado constituye una de las principales preocupaciones de la seguridad regional. Mientras los cárteles pueden invertir inmediatamente en drones

armados, redes de comunicación privadas y kits de hacking adquiridos en la dark web, las autoridades se ven frenadas por los trámites burocráticos, los presupuestos limitados y la falta de personal especializado.

Esta asimetría se explica en parte por la enorme liquidez del narcotráfico, que genera miles de millones de dólares anuales. A diferencia del gobierno, los cárteles no enfrentan procesos de licitación, auditorías o restricciones legales para adquirir la tecnología que sus operaciones requieren.

5.2. Nuevos modelos de negocio criminal

El modelo Crime-as-a-Service (CaaS) representa un desafío emergente. Ciertas plataformas clandestinas como FraudGPT, DarkBARD y Xanthorox AI ofrecen servicios de clonación de identidad, generación de malware y manipulación de datos, facilitando a los grupos delictivos el acceso a alta tecnología sin necesidad de desarrollarla internamente. El riesgo es que estas plataformas "normalicen" la disponibilidad de la IA criminal, aumentando la capacidad de actores locales y globales para ejecutar con eficiencia delitos sofisticados.

Investigaciones del programa PACCTO 2.0 documentan el crecimiento del modelo Violence-as-a-Service (VaaS), donde las redes criminales subcontratan violencia —desde intimidación hasta asesinatos por encargo— a terceros reclutados a través de redes sociales, videojuegos y aplicaciones cifradas. La Operación GRIMM de Europol identificó más de 1,400 individuos vinculados a las redes de VaaS y realizó aproximadamente 280 arrestos en su primer año de trabajo.

5.3. Reclutamiento automatizado

La inteligencia artificial está transformando los procesos de reclutamiento criminal. El estudio "Hired by the Algorithm" del PACCTO 2.0 Innovation Lab examina cómo las organizaciones criminales utilizan la IA para reclutar niños, adolescentes y adultos en América Latina, el Caribe y la Unión Europea.

La IA no cambia la lógica subyacente del reclutamiento, pero reduce las barreras de costo, habilidad e idioma mientras aumenta la velocidad, la escala y la precisión con que las redes alcanzan, perfilan y engañan a sus objetivos. El resultado es un proceso de reclutamiento más profesional e industrializado. Menores de tan solo 13-14 años son reclutados por diseño, aprovechando su reducida exposición legal.

6. Respuestas estatales y desafíos pendientes

6.1. Modernización de las fuerzas de seguridad

Algunos países han comenzado a modernizar sus capacidades tecnológicas. Colombia estableció en octubre de 2025 el primer Batallón de Aeronaves no Tripuladas (UAVs) de América Latina, compuesto por cuatro compañías especializadas que integran un sistema de vigilancia autónomo con drones equipados con inteligencia artificial.

Ecuador ha recibido un fondo de seis millones de dólares de Estados Unidos para dotar de drones a su Armada, con el objetivo de fortalecer el rastreo de rutas del narcotráfico marítimo. El Ministerio de Defensa ecuatoriano ha impulsado procesos de adquisición orientados a reforzar las capacidades tecnológicas de las Fuerzas Armadas.

6.2. Hacia una soberanía algorítmica

Varios expertos advierten sobre los riesgos de la dependencia algorítmica. Un artículo en Foreign Policy citado por La Silla Vacía señala que la incorporación de IA a la seguridad y defensa está creando una nueva forma de dependencia estratégica, donde las capacidades críticas para la seguridad nacional quedan condicionadas por las decisiones corporativas de empresas privadas extranjeras.

Para Colombia y otros países de la región, el desafío es preservar la "soberanía algorítmica": la capacidad de supervisar, auditar y gobernar sistemas de IA utilizados en seguridad, incluso cuando son desarrollados por terceros. Esto requiere marcos regulatorios claros, mecanismos de control y transparencia en los algoritmos utilizados para vigilancia, análisis de problemáticas y priorización de objetivos.

6.3. La cooperación internacional y las brechas de la transición global

La naturaleza transnacional de las problemáticas requiere respuestas coordinadas. La cooperación internacional se manifiesta en programas como PACCTO 2.0 de la Unión Europea, que financia investigaciones sobre el uso de IA por redes criminales, y en la colaboración bilateral entre Estados Unidos y países latinoamericanos para compartir inteligencia y bloquear las rutas financieras que abastecen al crimen organizado.

Sin embargo, esta cooperación enfrenta serios obstáculos. La interoperabilidad institucional es limitada y las capacidades de ciberdefensa de muchos países son débiles. Se requiere no solo una masiva inversión en tecnología, sino también en formación de personal especializado, protocolos de intercambio de datos y supervisión ética para evitar la proliferación de sesgos antidemocráticos en los algoritmos.

6.4. La IA en la disputa global por la hegemonía

La confrontación global entre China y Estados Unidos introduce, además, una contradicción profunda que agrava la asimetría descrita. China ofrece alta tecnología —drones, chips, sistemas de vigilancia, servicios en la nube— a quien esté dispuesto a comprarla, sin exigir alineamiento político ni imponer condicionalidades de seguridad. El crimen organizado, que no rinde cuentas a ningún electorado, no enfrenta controles de exportación ni procesos de licitación y dispone de capital líquido abundante, accede a ese mercado con una libertad de la que carecen los propios Estados.

Estos quedan atrapados en la disputa hegemónica porque acceder a la tecnología china puede traducirse en costos diplomáticos frente a Washington; acceder a tecnología estadounidense implica aceptar condicionalidades, dependencia y precios más elevados. El alineamiento internacional se convierte así en un filtro de acceso tecnológico que beneficia al crimen organizado y perjudica a los Estados nacionales de la región. El resultado es paradójico: el actor que no detenta soberanía formal —la organización criminal— goza de mayor libertad de acceso a la alta tecnología que el actor que sí la detenta —el Estado—. Lejos de ser un fenómeno marginal, el crimen organizado y su apropiación de la inteligencia artificial quedan insertos en la disputa misma por la hegemonía global.

7. Conclusiones

La convergencia entre crimen organizado e inteligencia artificial representa una transformación paradigmática en la naturaleza de las problemáticas de seguridad en América Latina. Los cárteles del narcotráfico han dejado de ser organizaciones tradicionales para convertirse en entidades tecnológicas capaces de operar con una sofisticación comparable a las corporaciones multinacionales.

El uso de la IA por el crimen organizado abarca múltiples dimensiones: extorsión automatizada mediante deepfakes y clonación de voz, optimización logística mediante análisis predictivo, drones armados para vigilancia y ataque, y reclutamiento automatizado a través de las redes sociales. Estas capacidades permiten a las organizaciones criminales reducir costos y riesgos mientras amplían su alcance e impacto.

La asimetría tecnológica entre el crimen organizado y el Estado constituye el principal desafío. Mientras los cárteles capitalizan rápidamente las tecnologías emergentes, las instituciones estatales enfrentan limitaciones presupuestarias, burocráticas y de conocimiento especializado. Esta brecha no solo incrementa la eficacia de las operaciones criminales, sino que erosiona la soberanía digital y la capacidad del Estado para proteger a la

ciudadanía.

El fenómeno del Crime-as-a-Service y el Violence-as-a-Service representa un desafío emergente que democratiza el acceso a las capacidades criminales sofisticadas. Las plataformas clandestinas que ofrecen servicios basados en IA eliminan las barreras técnicas para los actores menos capacitados, ampliando el universo de las problemáticas potenciales.

Frente a este escenario se requieren respuestas integrales que combinen inversión en tecnología, formación de personal especializado, marcos regulatorios claros y cooperación internacional. La "soberanía algorítmica" —la capacidad de supervisar, auditar y gobernar sistemas de IA utilizados en seguridad— emerge como concepto clave para preservar la autonomía estratégica de los Estados.

La pregunta no es si el crimen organizado puede usar tecnología avanzada, lo cual es un hecho comprobado, sino saber si el Estado tiene capacidad de alcanzarlo antes de que la brecha tecnológica sea tan amplia que el crimen organizado se vuelva completamente autónomo. En ese supuesto, aunque el Estado tenga más armas y personal en tierra, el crimen organizado estará posicionado en la nube comprendiendo mejor los datos emanados del territorio.

Referencias

- Aguilar Antonio, J. M. (2025). Uso de la Inteligencia Artificial por Redes Criminales de Alto Riesgo. PACCTO 2.0.
- Aguilar Antonio, J. M. (2026). *Hired by the Algorithm: How criminal networks are using AI to recruit across the EU, Latin America and the Caribbean*. PACCTO 2.0 Innovation Lab. Zenodo.
- Diálogo Américas. (2026, 30 de marzo). "Cómo la IA y la tecnología avanzada han fortalecido a los grupos criminales latinoamericanos". Diálogo Américas.
- Diálogo Américas. (2026, 8 de enero). "Drones del narco: la revolución tecnológica que transforma la violencia en México". Diálogo Américas.
- Diario Extra. (2026, 12 de agosto). "Guerra de drones en Ecuador: cómo el crimen y el Estado pelean el control aéreo". Diario Extra.
- El Imparcial. (2026, 21 de agosto). "Estudio de la UNAM revela cómo el crimen organizado utiliza la Inteligencia Artificial para clonar voces de familiares en extorsiones telefónicas y optimizar rutas de tráfico de drogas para evadir controles policiales". El Imparcial.
- El Telégrafo. (2026, 20 de enero). "Noboa se reúne con Palantir en Davos y apunta a cooperación tecnológica para seguridad y defensa". El Telégrafo.
- Infobae. (2025, 20 de septiembre). "El crimen organizado capitaliza la tecnología más que el gobierno: el peligro que representa". Infobae.
- La Tribuna. (2026, 8 de septiembre). "CNN: Crimen organizado usa cada vez más drones". La Tribuna.
- La Razón de México. (2026, 8 de abril). "IA ayuda a crimen a bajar costos y a ampliar capacidades de extorsión". La Razón de México.
- Malay Mail. (2026, 28 de febrero). "El Mencho se ha ido, pero el caos digital persiste: cómo los cárteles de la droga mexicanos convierten las redes sociales en armas". Malay Mail.
- N+. (2025, 23 de septiembre). "Cártel de Sinaloa y CJNG usan IA para ampliar sus negocios criminales". N+.
- Revista de la Academia de Guerra del Ejército Ecuatoriano. (2026). Análisis de las interacciones entre la inteligencia artificial y las redes criminales en la frontera norte del Ecuador. Revista de la Academia de Guerra del Ejército Ecuatoriano, 19(01), 13.
- Vanguardia MX. (2025, 29 de mayo). "Detectan mayor uso de tecnología en crimen organizado". Vanguardia MX.