

Del desmantelamiento de redes a la resiliencia sistémica

Por Juan Manuel Llenderozas

El dato más elocuente revelado por Europol en su última evaluación estratégica sobre las redes criminales más amenazantes no radica únicamente en que el 76 % de las 821 organizaciones identificadas en 2024 haya dejado de figurar en el mapa prioritario de la Unión Europea. La verdadera dimensión del desafío reside en la capacidad de recomposición que tienen el ecosistema criminal: sobre un núcleo de 198 redes persistentes y la irrupción o detección de 533 nuevas estructuras, el censo se sitúa en 731 redes en 2026. Esta metamorfosis demuestra que el paradigma tradicional de descabezamiento policial es insuficiente frente a redes fluidas, transnacionales y que están profundamente incrustadas en el tejido económico y digital legítimo.

Introducción: del actor criminal al sistema que lo sostiene

Durante décadas, las políticas de seguridad interior, el análisis de inteligencia y los dispositivos de control fronterizo han operado bajo una premisa predominantemente centrada en los actores: identificar a la cúpula, cartografiar el organigrama, neutralizar a los cabecillas e incautar los alijos o los activos inmediatos. Sin embargo, las evaluaciones analíticas más exhaustivas producidas por los servicios policiales europeos ponen de manifiesto que este modelo clásico se enfrenta a límites estructurales evidentes.

Las organizaciones delictivas contemporáneas han dejado de comportarse como corporaciones cerradas o clanes herméticos para transformarse en redes abiertas, altamente dinámicas y resilientes. Operan dentro de ecosistemas de criminalidad como servicio (*Crime-as-a-Service*, CaaS), donde las capacidades críticas (desde el blanqueo de capitales y la intrusión informática hasta la logística portuaria y la corrupción institucional) se contratan, externalizan y sustituyen con una fricción operativa mínima.

Para los responsables de la seguridad pública, la gestión integral de fronteras, la inteligencia estratégica y el cumplimiento corporativo, la lección es unívoca: descabezar una red ya no garantiza dismantelar su actividad delictiva. La amenaza no reside únicamente en quién ejecuta la operación, sino en las infraestructuras, dependencias y vulnerabilidades sistémicas que permiten que el flujo criminal continúe casi sin interrupción.

Dos fotografías de una misma amenaza: 2024 y 2026

El análisis comparativo de las dos evaluaciones estratégicas publicadas por Europol sobre las redes criminales más amenazantes (*Most Threatening Criminal Networks*, MTCN) ofrece una perspectiva privilegiada sobre la velocidad y el alcance de esta transformación.

Conviene, no obstante, establecer una precisión metodológica fundamental: las cifras de 2024 y 2026 proceden de procesos de recolección de inteligencia adaptativos y priorizaciones

operativas dinámicas de los Estados miembros. No constituyen una serie estadística homogénea ni un censo cerrado y acumulativo, sino dos instantáneas transversales de la cúspide de la delincuencia grave y organizada en Europa.

Parámetro analítico	Informe Europol 2024	Informe Europol 2026	Interpretación estratégica
Volumen de redes (MTCN)	821 redes prioritarias	731 redes prioritarias	Reconfiguración de prioridades operativas; 198 persistentes y 533 nuevas/identificadas.
Rotación del catálogo	Base de referencia	76 % de las redes de 2024 ya no figura	Alta volatilidad operativa, reestructuración y respuesta policial eficaz pero sustituible.
Individuos vinculados	> 25.000 miembros clave	> 400.000 miembros / afiliados	El salto cuantitativo refleja la inclusión de redes masivas de cibercrimen y fraude online (no es un tamaño medio).
Especialización funcional	82 % monodelito central	77 % especializadas en una actividad principal	Fuerte núcleo de especialización técnica combinado con diversificación oportunista accesorio.
Cohesión organizativa	Predominio jerárquico	64 % estructura jerárquica	Coexistencia de mando vertical con células modulares y contratación externa de servicios.
Composición nacional	Amplia multinacionalidad	118 nacionalidades (63 % composiciones mixtas)	Carácter intrínsecamente global; dilución de los cárteles monoétnicos tradicionales.
Penetración económica	86 % uso de empresas	85 % uso de estructuras empresariales legales (LBS)	Utilización masiva de la economía legal como escudo operativo y vehículo de lavado.
Longevidad operativa	Mayoría consolidadas	~80 % activas ≥ 3 años (34 % ≥ 10 años)	Elevada resistencia temporal e institucional frente a la persecución penal.

En 2024, Europol consolidó el **marco ABCD** para caracterizar a estas organizaciones críticas, un esquema analítico que mantiene plena vigencia en 2026:

- **Agile (Ágiles):** Capacidad extrema de adaptación a las contramedidas policiales, marcos regulatorios cambiantes, disrupciones geopolíticas y fluctuaciones de los mercados ilícitos.
- **Borderless (Sin fronteras):** Despliegue operativo multinacional nativo. En 2026, el 76 % de las redes actúa de forma simultánea en hasta siete países, y más de la mitad extiende sus tentáculos dentro y fuera de las fronteras de la Unión Europea.
- **Controlling (Controladoras):** Ejercicio de un control férreo sobre sus operaciones mediante liderazgo estratégico (el 64 % mantiene estructuras jerárquicas directivas), sistemas de disciplina interna y un uso instrumental de la violencia selectiva y la corrupción sistemática.

- **Destructive (Destructivas):** Capacidad de infligir un daño profundo y prolongado al Estado de derecho, la seguridad ciudadana, la libre competencia y la integridad del sistema financiero y comercial.



El informe de 2026 demuestra que, lejos de atenuarse, las características del marco ABCD se han acelerado mediante la convergencia digital y la explotación de vulnerabilidades logísticas globales.

La mutación decisiva: del grupo a la «red de redes»

El cambio morfológico más significativo de la delincuencia organizada contemporánea radica en la disolución de los límites organizativos clásicos. La noción tradicional de la pertenencia formal a una banda u organización mafiosa ha cedido el paso a un ecosistema fluido, horizontal y modular.



En este nuevo entorno, las redes criminales más amenazantes funcionan mediante alianzas transitorias y contratos *ad hoc*. Un grupo especializado en el tráfico transatlántico de estupefacientes no necesita desarrollar internamente capacidades criptográficas, esquemas de blanqueo en paraísos fiscales o acceso a credenciales portuarias comprometidas, recurre a intermediarios independientes (*brokers*) y a proveedores de servicios criminales (*Crime-as-a-Service*).

Esta dinámica genera tres consecuencias estratégicas de primer orden:

1. **Indefinición de los perímetros organizativos:** Las fronteras entre miembro orgánico, colaborador puntual y proveedor externo de servicios profesionales se vuelven extremadamente porosas. Cuando una red contrata una infraestructura digital de servidores o una ruta logística marítima, el proveedor puede desconocer la identidad final del cliente o trabajar simultáneamente para múltiples redes rivales.
2. **Redundancia y sustituibilidad sistémica:** La neutralización de una célula operativa no paraliza el negocio. Si un facilitador aduanero o un especialista en blanqueo es detenido, el núcleo directivo licita el servicio a otro operador dentro del ecosistema delictivo en cuestión de días.
3. **Economías de escala y barreras de entrada reducidas:** Pequeños grupos delictivos o actores emergentes pueden acceder a capacidades de nivel de ciberataques avanzados o complejas estructuras fiduciarias simplemente abonando tarifas fijas o comisiones de éxito a plataformas especializadas.

La frontera ya no es una línea: transnacionalidad y gestión integral

Para las autoridades aduaneras, los cuerpos policiales y los operadores de transporte, la concepción decimonónica de la frontera como una línea física de contención territorial ha quedado definitivamente obsoleta. La delincuencia organizada actúa a lo largo de corredores

logísticos de dimensión transfronteriza y cadenas de suministro globales donde los puntos de vulnerabilidad se sitúan a miles de kilómetros de los mercados de consumo final.

Los datos de Europol de 2026 son categóricos: el **76 % de las redes más amenazantes opera en hasta siete países diferentes**, y más de la mitad despliega actividad operativa tanto dentro como fuera de la Unión Europea. Destaca de forma muy particular la conexión con América Latina, presente en una de cada cinco redes identificadas, vínculo especialmente preponderante en el tráfico de clorhidrato de cocaína y en los flujos financieros ilícitos conexos.

Dimensión transnacional (Europol 2026)
76 % de las redes opera hasta en 7 países simultáneamente
> 50 % despliega actividad dentro y fuera de la UE
20 % (1 de cada 5) mantiene conexiones operativas con América Latina

En este contexto, la **Gestión Integrada de Fronteras** (*Integrated Border Management*, IBM) adquiere una dimensión cualitativamente distinta. Los grandes nodos de transbordo intermodal (especialmente los puertos de gran calado del norte y sur de Europa) no constituyen mero s puntos de paso geográfico, sino auténticos terrenos de fricción sistémica. La delincuencia explota:

- **La velocidad y densidad del comercio legítimo:** La inspección intrusiva física masiva es inviable en entornos comerciales que exigen tiempos de despacho de horas; las redes aprovechan la saturación de los circuitos aduaneros para camuflar envíos ilícitos en contenedores mercantiles estándar.
- **Asimetrías regulatorias y jurisdiccionales:** Diseñan rutas indirectas y triangulaciones marítimas y aéreas a través de terceros países con controles laxos para oscurecer el origen real de las mercancías.
- **Vulneración del factor humano en la cadena de custodia:** La captación, coacción o soborno selectivo de estibadores, transitarios, transportistas terrestres y funcionarios de inspección permite la extracción de cargamentos ilegales antes de los controles aduaneros formales (técnicas de rescate rápido, clonación de precintos y uso fraudulento de códigos PIN de retirada de contenedores).

La seguridad fronteriza moderna ya no se dirime exclusivamente en la vigilancia del perímetro costero o terrestre, sino en la capacidad de integrar análisis de riesgo avanzado sobre datos de manifiestos de carga, trazabilidad de contenedores, titularidad real de empresas importadoras y monitorización de la integridad de los ecosistemas portuarios.

La infraestructura legal como terreno de disputa

Uno de los hallazgos más contundentes y transversales de la inteligencia europea es que el crimen organizado no vive al margen de la economía formal, sino parasitándola. El **85 % de las redes criminales más amenazantes en 2026 utiliza estructuras empresariales legales**

(*Legal Business Structures*, LBS) para encubrir sus operativas, blanquear rendimientos y maximizar sus beneficios.

Penetración en la Economía Legal (85 % de las redes utiliza LBS) para:

- Transporte y Logística → Control de rutas, flota y despachos
- Importación / Exportación → Cobertura comercial y triangulación
- Inmobiliario y Construcción → Absorción masiva de capital y revalorización
- Hostelería y Ocio → Integración de efectivo y blanqueo transaccional
- Sectores Intensivos en Efectivo → Ocultación de fondos opacos

El uso de estas empresas legales no se limita a sociedades patrimoniales pasivas o meras corporaciones fantasma en jurisdicciones *con ventajas fiscales*. Las redes controlan, adquieren o infiltran empresas operativas en sectores clave de la actividad económica:

- **Transporte, paquetería y logística:** Para disponer de infraestructura propia de camiones, almacenes y almacenes de depósito temporal sin depender enteramente de terceros.
- **Import-export:** Para generar un flujo constante de facturación comercial simulada que justifique transferencias internacionales de fondos y justifique discrepancias de peso o valor en aduana.
- **Inmobiliario y construcción:** Sectores predilectos para absorber ingentes volúmenes de capital ilícito en activos tangibles de alta revalorización y difícil tasación comparativa inmediata.
- **Hostelería, comercio minorista y ocio nocturno:** Negocios intensivos en efectivo que permiten mezclar ingresos legítimos con dinero procedente de actividades delictivas, eludiendo las alertas automatizadas del sistema bancario.

Esta realidad traslada una presión regulatoria y operativa sin precedentes al sector privado legítimo. Las empresas de logística, las entidades financieras, las consultorías legales y las corporaciones multinacionales se enfrentan al riesgo constante de contaminación de sus cadenas de valor, exposición a sanciones por blanqueo de capitales (*AML*) y daño reputacional irreparable. Resulta imperativo trascender los controles formales de cumplimiento normativo (*checklist compliance*) para adoptar auditorías basadas en riesgo real, identificación profunda del beneficiario último (*Ultimate Beneficial Owner*, UBO) y monitorización continua de subcontratistas y socios comerciales.

Digitalización, IA y crimen como servicio

La transformación digital ha proporcionado a las redes criminales un multiplicador de fuerza sin parangón en términos de escala, velocidad, automatización y anonimato operativo. Las herramientas tecnológicas contemporáneas han reducido drásticamente los costes de transacción del delito y han eliminado las fricciones geográficas.

A nivel estratégico, la delincuencia organizada explota cuatro vectores tecnológicos principales:

1. **Canales de comunicación y coordinación cifrada:** Tras la desarticulación sucesiva de plataformas de comunicación cerrada por parte de consorcios policiales internacionales, los grupos criminales han migrado hacia soluciones descentralizadas, aplicaciones comerciales con cifrado de extremo a extremo, servidores efímeros y protocolos peer-to-peer, combinados con estrictos protocolos de contrainteligencia interna.
2. **Infraestructuras de anonimización y plataformas de datos comprometidos:** El acceso generalizado a bases de datos masivas filtradas (credenciales de acceso, historiales crediticios, identidades sintéticas) alimenta esquemas a gran escala de fraude en línea, estafas a directivos (*Business Email Compromise*, BEC) y extorsiones digitales. A esto se suma el uso de dispositivos de comunicación masiva no identificados, como baterías de enrutadores y servicios de *SIM-box*, que permiten coordinar ataques de ingeniería social desde cualquier parte del mundo.
3. **Modelos de ciberdelincuencia como servicio y Ransomware:** La hiperespecialización digital ha consolidado plataformas donde se alquila acceso a infraestructuras comprometidas (*initial access brokers*), código malicioso y servicios de cobro y negociación, permitiendo que actores sin capacidades técnicas avanzadas ejecuten campañas de extorsión contra infraestructuras críticas, administraciones públicas y empresas esenciales.
4. **Automatización e Inteligencia Artificial:** La IA generativa y las herramientas de automatización están transformando la velocidad y personalización de las operaciones ilícitas. Se emplean en la creación a escala de contenidos creíbles para estafas de ingeniería social de alto nivel, la generación de documentación mercantil e identidades fiduciarias indistinguibles de las reales, y el desarrollo de algoritmos capaces de testear y optimizar vulnerabilidades informáticas y financieras de manera ininterrumpida.

Esta aceleración digital no sustituye a la criminalidad física; la complementa y potencia, dotando al narcotráfico, a la trata de personas o al tráfico ilícito de mercancías de una infraestructura logística y financiera digitalizada y opaca.

Finanzas, corrupción y oportunidades geopolíticas

El motor primordial de la delincuencia organizada sigue siendo la maximización y aseguramiento del beneficio económico. Según los datos documentados por Europol en 2026, **más del 90 % de las redes delictivas más amenazantes gestiona y blanquea sus propios beneficios de forma directa o semicontrolada**, recurriendo paralelamente a profesionales habilitadores externos para las operaciones de mayor complejidad fiduciaria.

El ecosistema Financiero Ilícito (Europol 2026):

- El 90 % de las redes gestiona o blanquea sus propios beneficios

- Criptoactivos y sistemas bancarios alternativos (Hawala / Feichien)
- Facilitadores profesionales (abogados, asesores, contables, notarios)
- Corrupción selectiva en puertos, aduanas y judicatura
- Vínculos con terrorismo limitados (5 %, de carácter parcial y oportunista)

La arquitectura del lavado de dinero combina mecanismos arcaicos con innovaciones de última generación:

- **Sistemas bancarios clandestinos y tradicionales:** El uso de redes de compensación informal de fondos como el *Hawala* o el *Feichien* sigue siendo fundamental para mover grandes sumas de valor entre continentes sin dejar rastro en el sistema bancario regulado.
- **Criptoactivos y finanzas descentralizadas:** Empleo de criptomonedas con características de privacidad mejorada, servicios de mezcla descentralizada (*mixers*), intercambios entre cadenas de bloques (*cross-chain bridges*) y compras de activos virtuales para fracturar la trazabilidad forense de las carteras digitales.
- **Facilitadores profesionales (*enablers*):** Asesores fiscales, abogados, contables y administradores fiduciarios que aportan la arquitectura jurídica necesaria para registrar corporaciones en cascada, crear fideicomisos opacos y eludir los filtros de diligencia debida del sector bancario.
- **La corrupción como vector facilitador esencial:** La delincuencia organizada no busca derrocar al Estado, sino neutralizar su capacidad de respuesta. La corrupción se ejerce de forma quirúrgica sobre inspectores de aduanas, agentes policiales, personal de logística portuaria, funcionarios judiciales y responsables políticos locales para garantizar impunidad, información privilegiada y libre paso de cargas.

En el plano geopolítico, las crisis internacionales, los conflictos armados y las sanciones comerciales unilaterales o multilaterales abren extraordinarias ventanas de oportunidad para las redes ilícitas. Estas estructuras capitalizan la alteración de las cadenas de suministro tradicionales para ofrecer servicios de contrabando de bienes de doble uso, elusión de embargos energéticos, transporte de dinero en efectivo y tráfico de personas en rutas migratorias desestabilizadas.

Precisión analítica sobre actores híbridos y terrorismo. Conviene diferenciar rigurosamente los hechos comprobados de las hipótesis estratégicas. El informe de Europol documenta que solo un **5 % de las redes presenta vínculos con el terrorismo**, tratándose casi invariablemente de conexiones oportunistas, logísticas o de financiación cruzada en prisiones o mercados secundarios de armas, sin que exista una convergencia ideológica formal. Del mismo modo, aunque analíticamente se observa una creciente explotación del crimen organizado por parte de actores estatales para acciones híbridas (sabotajes encubiertos, desinformación o desestabilización), las

evidencias documentadas en los informes policiales describen estos nexos como ocasionales, instrumentales y frecuentemente difíciles de acreditar judicialmente.

Implicaciones para la inteligencia y la seguridad corporativa

Frente a una amenaza que actúa como una red interconectada, la respuesta institucional y corporativa no puede limitarse a la reacción puntual ante incidentes aislados. Se requiere una doctrina de seguridad integral articulada en torno a **cinco líneas operativas y estratégicas prioritarias**:

1. Inteligencia orientada a nodos y dependencias críticas

Desplazar el foco del organigrama jerárquico hacia el análisis de grafos y redes complejas. Identificar a los intermediarios no sustituibles (*chokepoints*): corredores de datos, proveedores de comunicaciones seguras, agentes de aduanas cooptados y administradores de empresas pantalla comunes a múltiples organizaciones. Desconectar estos nodos genera un impacto disruptivo sistémico superior a la detención de mandos operativos fácilmente reemplazables.

2. Investigaciones financieras paralelas sistemáticas

Toda investigación criminal o auditoría corporativa de seguridad debe incorporar desde el día cero una línea de trazabilidad económica. No basta con incautar el producto físico del delito; es imperativo mapear los flujos de criptoactivos, los créditos documentarios fraudulentos, las inversiones inmobiliarias y los honorarios de los facilitadores jurídicos, activando mecanismos tempranos de embargo preventivo y comiso sin condena previa cuando la legislación lo ampare.

3. Blindaje de cadenas de suministro e infraestructuras portuarias

Los operadores de transporte, puertos y plataformas logísticas deben consolidar esquemas de gobernanza de seguridad avanzados: controles de acceso biométricos y segmentados, rotación obligatoria de turnos en tareas sensibles, auditorías sorpresivas de inventario, y uso de gemelos digitales e inteligencia artificial para detectar patrones anómalos de pesaje, tiempos de permanencia o modificación de manifiestos marítimos.

4. Resiliencia digital y gobernanza de datos

Las organizaciones públicas y privadas deben asumir el principio de compromiso previo (*assumed breach*). Esto exige aplicar arquitecturas de confianza cero (*Zero Trust*), cifrado robusto de repositorios confidenciales, monitorización continua de credenciales filtradas en la red profunda (*Darknet*), y planes rigurosos de continuidad de negocio frente a ataques de secuestro digital y extorsión masiva de datos.

5. Integridad institucional y protección de personas vulnerables

El eslabón humano permanece como la principal vulnerabilidad explotada por la corrupción criminal. Resulta prioritario desplegar sistemas de alerta temprana basados en indicadores conductuales y financieros de riesgo, canales de denuncia anónimos y seguros con protección legal efectiva para el alertador (*whistleblower*), e implementar programas de apoyo y protección para personal operativo y sus familias frente a intentos de coacción o intimidación física por parte de redes delictivas.

Hacia una gestión integral de fronteras

La respuesta a esta amenaza mutante exige construir una arquitectura de seguridad integrada que trascienda los silos departamentales y las barreras corporativas. Esta arquitectura debe vertebrarse sobre cuatro principios doctrinales consolidados en los estándares internacionales más avanzados:



- **Inteligencia Criminal como Guía (*Intelligence-Led Policing*, ILP):** Las operaciones no deben basarse en la inercia o en la inspección aleatoria ineficiente, sino en la asignación estratégica y táctica de recursos a partir de modelos analíticos de riesgo, minería de datos y prospectiva criminal.
- **Gestión Integrada de Fronteras Europea (IBM):** Coordinación interinstitucional plena entre guardias de fronteras, servicios aduaneros, autoridades fitosanitarias, policías nacionales, autoridades judiciales y agencias europeas e internacionales (Europol, Frontex, Eurojust, Interpol, OMA).
- **Enfoque de Sociedad Completa (*Whole-of-Society Approach*):** La lucha contra el crimen organizado no puede ser monopolio exclusivo de los cuerpos policiales. Exige

la participación de los organismos tributarios, el sector bancario, las navieras, los colegios de abogados y notarios, las empresas de ciberseguridad y las administraciones locales, facultadas estas últimas para aplicar clausuras y controles administrativos preventivos sobre locales y licencias comerciales de riesgo.

- **Prevención por Diseño (*Prevention by Design*):** Concepción de procesos administrativos, portuarios, mercantiles y digitales diseñados desde su origen para eliminar las vulnerabilidades que facilitan el fraude y la infiltración ilícita (identificación fiduciaria obligatoria, trazabilidad de accesos digitales a precintos, licitaciones públicas blindadas contra empresas opacas).

Esta cooperación debe apoyarse en marcos jurídicos robustos y transparentes que posibiliten el intercambio de información estratégico y operativo entre el sector público y el privado de forma ágil, proporcional y con plenas garantías en materia de protección de datos y secretos comerciales.

Qué puede cambiar la ecuación: del descabezamiento a la disrupción de infraestructuras

La insistencia en focalizar los éxitos operativos exclusivamente en la detención de líderes carismáticos o en la confiscación puntual de cargamentos genera una falsa sensación de victoria que el mercado criminal absorbe de inmediato como un mero coste operativo amortizable.

Para quebrar la resiliencia del ecosistema delictivo es indispensable ponderar las ventajas y limitaciones de los diferentes modelos estratégicos de intervención:

Modelo Estratégico	Foco de Actuación	Ventajas Operativas	Limitaciones Críticas
Actor-Céntrico (<i>Enfoque tradicional</i>)	Cabecillas, lugartenientes y miembros directos de la organización.	Alto impacto mediático y reputacional. Retirada de actores violentos específicos. Resultados tangibles en procesos penales clásicos.	Rápida sucesión en la cúpula. Mantenimiento de la infraestructura operativa intacta. No reduce la oferta global ni altera las vulnerabilidades del mercado.
Infraestructura-Céntrico (<i>Enfoque intermedio</i>)	Canales logísticos, sistemas de comunicación cifrada, activos fiduciarios.	Bloqueo de corredores de transporte completos. Caída en cadena de múltiples células dependientes de un mismo servicio. Aumento drástico de los costes operativos criminales.	Capacidad de las redes de migrar a proveedores alternativos en el mercado CaaS. Exige coordinación internacional prolongada y costosa.

Sistémico Integrado (<i>Enfoque transformador</i>)	Vulnerabilidades estructurales, economía legal infiltrada, facilitadores y marcos regulatorios.	Reducción duradera de la resiliencia criminal. Desinfección de sectores económicos clave (LBS). Dificulta la sustitución automática de capacidades ilícitas.	Requiere reformas legislativas, coordinación público-privada profunda y recursos multidisciplinares a largo plazo.
---	---	--	--

El cambio de ecuación definitivo pasa por combinar la acción penal selectiva con el estrangulamiento de los recursos facilitadores: expulsar al crimen de las infraestructuras empresariales legales, neutralizar la oferta de servicios profesionales opacos e incrementar drásticamente los costes de fricción en los nodos logísticos y digitales.

Conclusión y prospectiva

La delincuencia grave y organizada ha superado definitivamente la fase en la que podía ser tratada como un fenómeno puramente marginal o policial. Hoy constituye un desafío de primer orden a la seguridad nacional, la soberanía económica y la integridad de las democracias europeas.

En el horizonte de los próximos cinco a siete años, la evolución de esta amenaza se dirimirá en **tres escenarios prospectivos**:

1. **Escenario 1: Adaptación incremental.** Las organizaciones delictivas mantienen su tasa de absorción de medidas policiales, adaptando gradualmente sus empresas pantalla y circuitos financieros a las nuevas directivas comunitarias sin que se altere sustancialmente el balance de poder.
2. **Escenario 2: Fragmentación resiliente (*Gig Crime*).** La presión policial provoca la desaparición casi total de organizaciones identificables de tamaño medio y grande, dando paso a una red altamente fragmentada de miles de operadores autónomos y microcélulas que se ensamblan y disuelven dinámicamente para cada operación, haciendo ineficaces los métodos de investigación convencionales.
3. **Escenario 3: Convergencia criminal-digital e híbrida.** Se produce una integración profunda entre el crimen transnacional, el ecosistema de ciberdelincuencia a escala industrial y actores estatales o paraestatales que instrumentalizan redes delictivas para operaciones de sabotaje logístico, elusión de sanciones, desestabilización social y financiación encubierta.

Las principales señales de alerta temprana ante estos escenarios incluyen el aumento de la violencia selectiva contra funcionarios y operadores logísticos en puertos europeos, la consolidación de proveedores CaaS inmunes a la jurisdicción internacional y la aceleración de compras de activos estratégicos por estructuras fiduciarias de origen no verificado.

La prioridad estratégica para los decisores públicos y privados es inequívoca, asumir que **la frontera de la seguridad ya no se sitúa en el perímetro exterior del territorio**. La verdadera frontera atraviesa hoy las transacciones financieras, los servidores de datos, las cadenas de suministro intermodales, los registros mercantiles y la confianza en nuestras instituciones. Defender esa frontera requiere abandonar la ilusión del desmantelamiento total y construir, con rigor analítico y visión de Estado, una resiliencia sistémica inquebrantable.

Fuentes

1. **Europol (2024):** *Decoding the EU's most threatening criminal networks*, Publications Office of the European Union, Luxemburgo.
2. **Europol (2026):** *Decoding the EU's most threatening criminal networks – Issue 2: The blueprint of criminal opportunism*, Publications Office of the European Union, Luxemburgo.

#Seguridad #Inteligencia #CrimenOrganizado #SeguridadPública #GuardiaCivil #España #SeguridadEuropea
#CrimenTransnacional #GestiónDeFronteras #Resiliencia