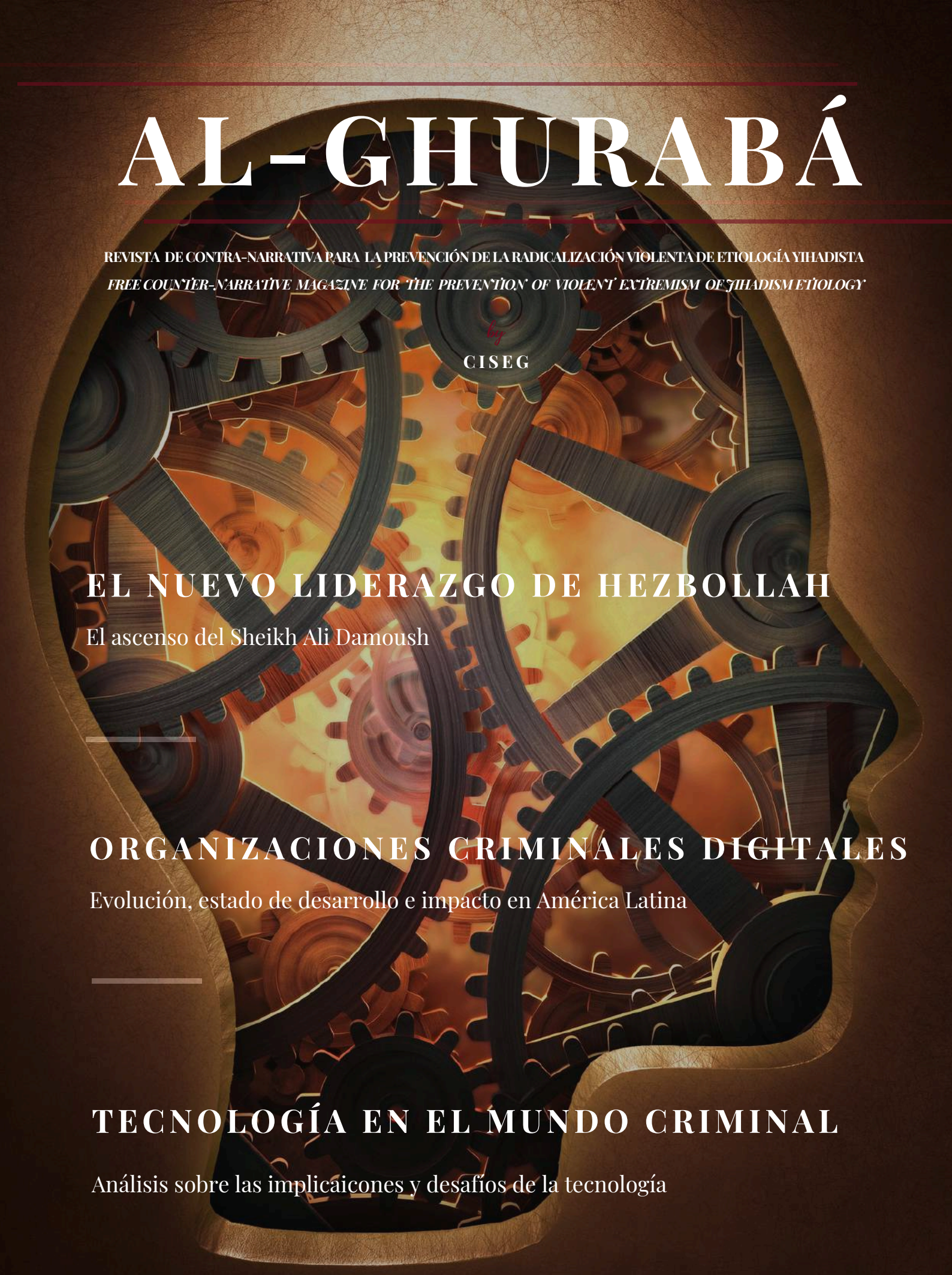
AL-GHURABÁ

REVISTA DE CONTRA-NARRATIVA PARA LA PREVENCIÓN DE LA RADICALIZACIÓN VIOLENTA DE ETIOLOGÍA YIHADISTA

FREE COUNTER-NARRATIVE MAGAZINE FOR THE PREVENTION OF VIOLENT EXTREMISM OF JIHADISM ETIOLOGY

by

CISEG



EL NUEVO LIDERAZGO DE HEZBOLLAH

El ascenso del Sheikh Ali Damoush

ORGANIZACIONES CRIMINALES DIGITALES

Evolución, estado de desarrollo e impacto en América Latina

TECNOLOGÍA EN EL MUNDO CRIMINAL

Análisis sobre las implicaicones y desafíos de la tecnología

ISSUE 96 SEPTIEMBRE 2025 ISSN 2565-2222

Revista indexada en Revistas Científicas de América Latina,el Caribe, España y Portugal

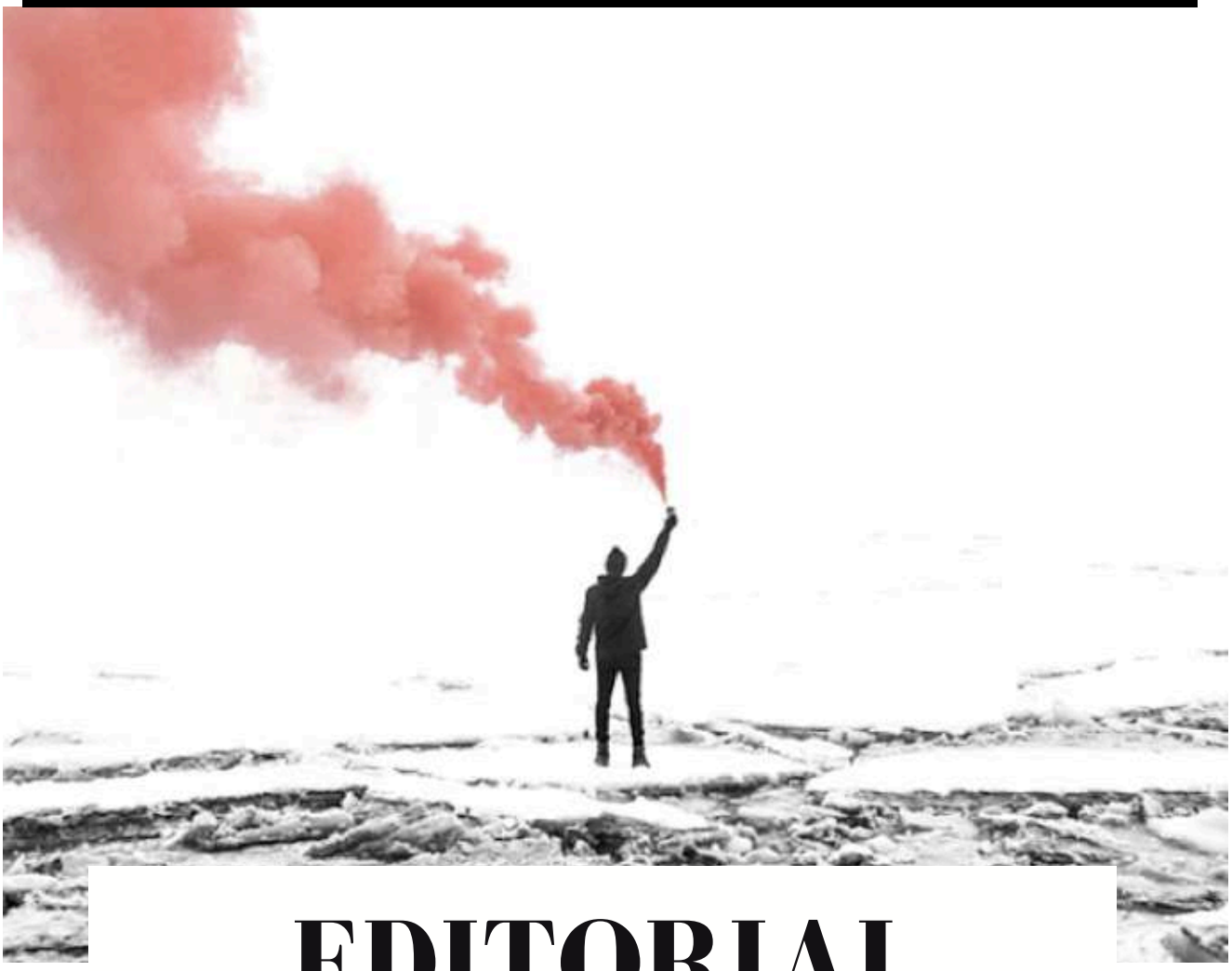
AL-GHURABÁ

NÚMERO 96 / SEPTIEMBRE 2025 / ISSN 2565-2222

CISEG
info@intelciseg.com

Web
www.alghuraba.org

Envío de artículos
alghuraba@intelciseg.com



EDITORIAL

La revista Al-Ghurabá de CISEG, es una herramienta de narrativas alternativas para prevenir la radicalización violenta de etiología yihadista y nace en agosto de 2017 como un proyecto de la Comunidad de Inteligencia y Seguridad Global. Al-Ghurabá es gratuita, on-line y mensual y persigue implicar a la sociedad civil en este sector y ofrecer herramientas de prevención y de contra-narrativa para prevenir la radicalización violenta en el seno de las comunidades a través de publicaciones accesibles realizadas por analistas.

Esta problemática nace en las comunidades, entre las personas y cualquiera puede hallarse en una situación de cercanía con un perfil radicalizado o un agente radicalizador. En consecuencia, brindar herramientas a la sociedad civil permite que sean personas empoderadas, informadas y formadas. Por otro lado, también sirve para difundir contra-narrativa frente a esta radicalización destinada a los grupos más vulnerables a ser radicalizados. El objetivo es crear contenido que analice la situación actual y consiga erosionar y deslegitimar los discursos que facilitan estas organizaciones terroristas.

SUMARIO

Un libro de

Ilham Majure y David Garriga

INTELIGENCIA

WWW.ALGHURABA.ORG

LA PIRÁMIDE ESTRATÉGICA

UNA GUÍA PARA DEFINIR RUMBOS EN TODOS LOS ASPECTOS DE SERVIR Y PROTEGER

Cecilio Andrade.
Hopólogo, conferencista, autor, prologuista. Director académico en Mano de Tyr.
Delegado de CISEG

INTRODUCCIÓN

Suelo trabajar habitualmente con ese colectivo, incluso me atrevo a incluirme en el mismo, que en contra de su más básico instinto de supervivencia corre hacia el peligro en lugar de rehuirlo, hablo del colectivo de la seguridad, ya sea de emergencias o armados… no hay diferencias en su trabajo contra natura.

Instruir a profesionales de ese 1% de la humanidad dedicados a Servir y Proteger no es una tarea fácil ni sencilla. Requiere conocimientos, capacidades, experiencia, empeño, pasión, paciencia, tino, así como unos Valores, Principios y Ética en tan justa y alta medida que nos hace entender las razones de que sean, los verdaderamente buenos, tan rara avis en nuestro mundo profesional.

Las redes (a)sociales nos hacen creer que sólo los aventureros rudos e intensos son los que tienen éxito en su instrucción, cuando en realidad, detrás de las cualidades del párrafo anterior existen mentes planificadoras, analíticas y estratégicas que miden los riesgos antes de tomarlos y tienen una visión clara de a dónde quieren llegar y cómo hacerlo.

El camino, la senda o la guía a seguir, sobre la cual se darán los pasos que se requieren tanto en una empresa, como en la instrucción de una unidad o institución, así como de un profesional armado individual, parten desde la Visión como inicio hasta la ejecución de los objetivos.

La Pirámide Estratégica no nace de la planificación, muy al contrario es su punto de partida.

ESTRATEGIA EXITOSA. ¿CUANTIFICABLES? ¿MEDIBLES?

Una estrategia, tanto operativa como de instrucción, bien ejecutada determina el éxito. Debe ser clara y con objetivos definidos que permitan medir los resultados a través de métricas e indicadores de rendimiento, "lo que no se puede medir no existe" suelo repetir tan a menudo que hasta mis mejores amigos lo parodian, pero es que si no se lleva a cabo correctamente la planificación previa, la estrategia será difícilmente ejecutada... y aún menos medible.

En mi experiencia, nueve de cada diez profesionales de la seguridad, armados o no, fallan en la implementación de estrategias efectivas. Pero también he podido constatar que raramente el fracaso se debe a una definición deficiente de su estrategia previa, en el antes. El problema no se halla en esa fase, si no más adelante: cuando los planes deben ser ejecutados, en el durante, ya sea este durante un enfrentamiento armado, un problema logístico, una catástrofe o una emergencia. Una vez aplicada, toda estrategia bien ejecutada debe permitir su medición a través de una evaluación de sus puntos clave. Como primer paso debemos partir de la definición del objetivo de la evaluación, puntualizando los aspectos que se desean medir o evaluar. Abarcando desde una nueva estrategia hasta la identificación de algún problema.

El segundo punto es la identificación de los conductos que se aplican en el funcionamiento efectivo de la nueva estrategia o el desarrollo del problema.

La siguiente etapa pasa por el análisis del estado y la optimización de dichos conductos. Se tienen cuenta las herramientas que permiten medir el rendimiento de la nueva estrategia o del generador del problema evaluado.

Como cuarto aspecto, se identificarán las oportunidades de mejora. Para ello ello es necesario contrastar los resultados propios con los de equipos similares, tanto en proyectos comerciales como operativos, así como con los objetivos propuestos. La comparación detectará las áreas de mejora y optimización de las estrategias aplicadas.

El quinto punto se refiere a la implementación de las acciones de mejora y/o poner en marcha las estrategias diseñadas para solucionar los problemas encontrados en la evaluación inicial.

Finalmente, como sexto y último matiz, es obligado elaborar un informe a modo de lecciones aprendidas y seguimiento. Debemos documentar los resultados de la evaluación, las acciones que se implementaron, y hacer un seguimiento continuo ya que las condiciones cambian constantemente.

PIRÁMIDE ESTRATÉGICA . ORIGEN DEL CONCEPTO

La Pirámide Estratégica, en su concepción original y empresarial, es un modelo ideado por la investigadora Wendy McGuinness en 2011, que busca facilitar la planeación y ejecución en el desarrollo de las empresas.

Este concepto lo divide en tres categorías a modo de pilares clave.

- Propósito.
- Estrategia.
- Ejecución.

El primer pilar lo definió como el Propósito de la empresa, campaña o proyecto, es decir:

- Su visión, hacia dónde quieren llegar.
- Su misión, su razón de existir, el motivo por el cual la empresa fue fundada.
- Sus valores, aquello en lo que los fundadores creen, sus principios irrenunciables.

En el segundo pilar, inmediatamente después del primero, situó a la Estrategia, compuesta por:

- La intención, que define los objetivos generales.
- Los impulsores, que son los factores claves del éxito de la empresa las fortalezas.
- Los facilitadores, aquellos recursos y capacidades necesarios para cumplir con los objetivos.

Finalmente, la base de la pirámide, donde podemos señalar la mayor cantidad de problemas, encontramos la Ejecución.

- Los objetivos e iniciativas, las metas específicas y medibles.
- Los indicadores de desempeño, que son medidos con métricas e hitos específicos.
- El mapa de la estrategia, el cual debe ser claro y conciso para ser entendido por todos en la organización.

Este marco busca ayudar a articular el propósito para desarrollar una estrategia clara y ejecutarla efectivamente, asegurando el éxito organizacional.

Lo cual me lleva a preguntarles…

- ¿Es tan distinto en un programa de trabajo y adiestramiento de una unidad de emergencias?
- ¿Un equipo de Protección Ejecutiva?
- ¿Una Unidad policial o militar?
- ¿De un operador armado en cualquier contexto?
- ¿Del trabajo de nuestros bomberos, sanitarios o profesionales en general?
- ¿Es aplicable a ese 1% de la humanidad?

En mi experiencia es un claro y definido SI.

Mi visión de la Pirámide Estratégica.

Aprendí el concepto de Pirámide Estratégica hace algunos años estudiando la licenciatura de Gestión de Empresa, algo en apariencia totalmente ajeno a mi mundo habitual del profesional armado. Lo cierto que los conceptos del combate empresarial no son tan dispares de los plasmados por Sun Tzu, Musashi, Maquiavelo y/o Clausewitz.

En el mundo empresarial, tener una visión clara del rumbo que debe tomar una organización es tan fundamental como en el mundo armado generar procedimientos tácticos operativos, así como de procesos de instrucción, claros y efectivos. E igualmente, en ambos mundos muchas veces las estrategias se quedan en el aire porque no están estructuradas ni comprendidas por todos los niveles de la empresa, organizaciones e individuos.

Es ahí donde entra en juego la sencilla y a la vez poderosa herramienta de la Pirámide Estratégica, ya que permite, y facilita, visualizar cómo deben alinearse todos los elementos estratégicos para que tanto una organización, del tipo que sea, como un profesional o equipo de seguridad funcionen de forma coherente y efectiva.

Hablamos de un modelo conceptual que organiza los diferentes niveles de la estrategia operacional en forma de pirámide, desde lo más genérico hasta lo más específico. Cada nivel depende del anterior, pero todos deben estar alineados de tal forma que garanticen el éxito organizacional, empresarial, operativo y/o táctico. Es tan útil porque traduce las grandes ideas, meramente filosóficas en apariencia como la Visión y la Misión, en acciones concretas y medibles.

A continuación, desglosaré cada uno de los niveles de esta pirámide y su función en la construcción generalista de una estrategia sólida.

ETAPAS DE LA PIRÁMIDE ESTRATÉGICA

1ª. Visión.

La Visión es la base de la pirámide, sin la cual no posee cimientos de crecimiento. Representa el sueño o la aspiración máxima de la empresa o la Unidad. Es una declaración que describe hacia dónde quiere dirigirse, y llegar, la organización en el largo plazo.

Debe ser inspiradora, clara y ambiciosa.

Ejemplos:

- Ser la empresa líder en soluciones IA sostenibles.
- Ser la Unidad de referencia para la ejecución de determinados operativos.
- Ser el equipo de instrucción y adiestramiento que prevea y se adelante a los problemas que se puedan encontrar en el futuro los profesionales de seguridad.

2ª. Misión.

La Misión explica el por qué existe la empresa, el proyecto o la Unidad, cuál es su propósito y a quién sirve.
Es el puente entre la visión y la acción.

Una buena definición de misión debe ser concisa, significativa y diferenciadora.

Ejemplos:

• Ofrecer servicios IA generando valor que mejoren la calidad de vida de nuestros clientes.
• Que el ciudadano observe y disfrute de un servicio mejorado, profesional y asertivo que lo hagan confiar más en sus Fuerzas de Seguridad.
• Que la calidad de la instrucción impartida salve y proteja las vidas tanto del personal instruido como de los ciudadanos que reciban el servicio y protección.

3ª. Valores.

Los Valores son los Principios y creencias fundamentales que guían la Ética del comportamiento de la organización.
Actúan como brújula ética y cultural, y son esenciales para crear coherencia interna.

Ejemplo:

- Innovación, sostenibilidad, trabajo en equipo, integridad y compromiso con el cliente.
- Respeto, honestidad, responsabilidad, justicia, libertad y fidelidad.
- Patriotismo, lealtad, disciplina, honor, compañerismo, servicio, valor y espíritu de sacrificio.

4ª. Objetivos Estratégicos.

Aquí es donde la estrategia comienza a volverse medible y alcanzable.

. os Objetivos Estratégicos son metas a mediano y largo plazo que permiten avanzar hacia la Visión. Siendo fácilmente definidos por el acrónimo anglosajón SMART:

•Specific - Específicos, claros, concretos y perfectamente definidos.
•Measurable - Medible, y cuantificable para conocer el progreso hacia los objetivos.
•Achievable - Alcanzables, realistas y factibles, en base a los recursos y capacidades disponibles.
•Relevant - Relevante, con propósito y sentido, alineados con la Visión de la persona o equipo.
•Timely/Time-bound -Limitado en el Tiempo, con plazo definido, con lineas temporales.

Ejemplos:

- Aumentar las ventas en un 40% en los próximos 3 años.
- Reducir el número de expedientes por Uso Excesivo de Fuerza por los componentes de la Unidad en los próximos 2 años.
- Aumentar de forma contrastable sobre el terreno las capacidades operativas de todo el personal a instruir en los próximos 2 años.

5ª. Iniciativas Estratégicas.

Las Iniciativas Estratégicas son todos los programas o proyectos clave que ayudan a cumplir los Objetivos. Se traducen en planes de acción y recursos asignados.

Ejemplos:

- Lanzar una línea de productos respetuosos con el medio ambiente y el crecimiento sostenible.
- Expandir la capacidad de intervención operativa a escenarios específicos no cubiertos hasta ahora.
- Aumentar los programas de instrucción, capacitación y entrenamiento por especialidades de la institución.

6ª. Indicadores de Desempeño (KPIs)

En el culmen final de la pirámide se encuentran los KPIs, Key Performance Indicators, Indicadores Clave de Desempeño, que permiten monitorear si las acciones e iniciativas están generando los resultados esperados.

Son esenciales para la gestión y mejora continua.

Ejemplos:

- Tasa de conversión de ventas, satisfacción del cliente, retorno de la inversión, etc.
- Mejora en la efectividad y capacidades del personal instruido.

Mejora de los servicios, reducir de intervenciones violentas, acciones más eficaces y efectivas, etc.

Figura-1: Elaboración propia

¿ES IMPORTANTE LA PIRÁMIDE ESTRATÉGICA?

La principal fortaleza de su conocimiento y aplicación es que ayuda a alinear a toda la organización en torno a una dirección común.

Permitiendo:

- Claridad en los objetivos y prioridades.
- Cohesión entre departamentos e integrantes de una unidad o institución.
- Mayor compromiso del equipo humano.
- Facilita la toma de decisiones.
- Mejora el rendimiento y la ejecución.
- Ayuda a estructurar el crecimiento desde los cimientos.

En un entorno global, empresarial, académico u operativo, donde el cambio es constante, tener una estrategia clara, bien comunicada y estructurada puede ser la diferencia entre avanzar o estancarse. La Pirámide Estratégica ayuda a construir ese camino desde la Visión hasta la ejecución diaria, asegurando que cada acción contribuya a los grandes objetivos buscados.

A modo de resumen para su adaptación a la instrucción táctica. Piensen en una triste realidad, en un enfrentamiento armado, del tipo que sea, el 90% de los profesionales armados no logran ejecutar lo que se supone que conocen “perfectamente” y practican “asiduamente”. Pero, el otro 10% si lo logra con mayor o menor eficacia… ¿en qué se diferencian?

Permítanme un resumen de todo lo anterior con una ligera adaptación al propósito de la conclusión del presente artículo. Como ya hemos visto la Pirámide Estratégica es el modelo de gestión que organiza los niveles de planificación tanto de un individuo como de una organización, desde lo más general hasta lo más específico, conectando la Visión y Misión con los Objetivos, las Estrategias y las acciones concretas que en este punto concreto representan las tácticas.

Su función principal es alinear el propósito de la instrucción con las actividades diarias, asegurando que todas las partes trabajen de manera coherente para lograr los objetivos deseados. Aunque pueden existir diferentes diseños, los niveles y componentes en mi forma de trabajo incluyen, de forma muy resumida…

Propósito/Base (Nivel superior):

•Misión: La razón de existir de la empresa y su papel en la sociedad.

•Visión: El estado futuro deseado y lo que la empresa quiere ser.

•Valores: Los principios fundamentales que guían las acciones y la cultura organizacional.

Estrategia (Nivel intermedio):

• Intención Estratégica: Los objetivos generales que la empresa busca alcanzar para materializar su visión.

•Estrategias: El "plan de juego" y la filosofía que guían a la empresa, delineando como se conseguirán los objetivos.

Ejecución/Tácticas (Nivel inferior):

•Objetivos e Iniciativas: Metas específicas, medibles y concretas que se desprenden de la estrategia.

•Plan de Acción/Tácticas: Las actividades específicas, los recursos necesarios y los plazos para llevar a cabo los objetivos.

Las utilidades observadas de su aplicación fueroN:

• Alineación.. Conectando las ideas generales con las tareas diarias, asegurando que toda la institución, equipo e individuos trabajen hacia los mismos objetivos.

• Claridad.:. Proporcionando una estructura que ayude a entender y comunicar la estrategia de manera sencilla.

• Toma de decisiones. Permitiendo que cada decisión y acción sea coherente con la Visión y los Valores tanto colectivos como individuales.

•. Medición del éxito. Facilitando la definición de indicadores de desempeño para evaluar el progreso hacia los objetivos.

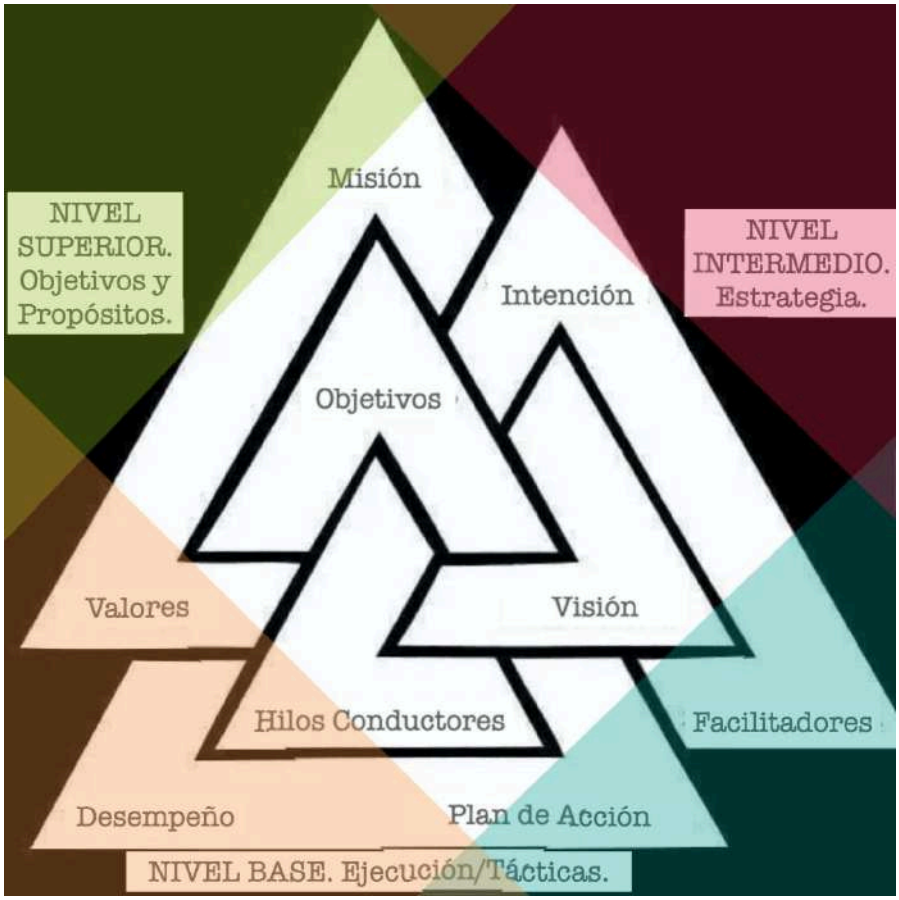


Figura-2: Elaboación propia

DE LA PIRÁMIDE ESTRATÉGICA A MI MUY PERSONAL VALKNUT TÁCTICO

Me he tomado la libertad de modificar y adaptar las preguntas de cada elemento al concepto de “Profesional Armado” y a su vez a mi muy personal “Valknut táctico”. La razón de emplear un símbolo tan antiguo, emblemático, complejo y multifacético, tiene que ver con la interrelación inseparable de cada uno de los puntos reseñados; además de ser un símbolo muy querido e importante en mi propia vida.

1°- Nivel Superior - Objetivos y/o propósitos.

A- Misión.
•¿Por qué soy “profesional armado”?
•¿Cuál es mi principal razón para serlo?
•¿Por qué y para qué instruyo al personal?

B-Valores.
•¿Cuáles son los Principios y Valores que me guían?
•¿Y a mi Unidad? ¿e Institución?
•¿Se alinean con los estándares éticos y los comportamientos deseados en mi institución?

C- Visión.
•¿Tengo una imagen convincente del futuro que deseo?
•¿Dónde aspiro a estar en los próximos años?
•¿Qué deseo lograr finalmente?

2°- Nivel Intermedio - Estrategia.

A- Intención.
•¿Cuáles son mis principales metas y objetivos?
•¿Puedo definir los resultados que busco?
•¿Y cómo lograrlos?
•¿Coinciden con los de mi institución, equipo y/o alumnos?

B- Hilos conductores.
•¿Sé cuáles son los factores clave que me impulsan hoy?
•¿Y en el futuro?
•¿De qué forman pueden cambiar?
•¿Soy adaptable a esos cambios?

C- Facilitadores.
•¿De qué herramientas, recursos y capacidades dispongo?
•¿Son necesarias para implementar crecimiento y mejora?
•¿Qué me/nos falta?
•¿Qué es superfluo, innecesario e incluso contraproducente?

3°- Nivel Base - Ejecución/Tácticas.

A- Objetivos e iniciativas.

•¿Sabría definir qué pasos y metas medibles debo seguir para lograr los objetivos que busco?
•¿Podría ordenarlos por orden de aplicación?
•¿Y de importancia pragmática?
•¿Y de relevancia moral?

B- Desempeño.

•¿Tengo una honesta medida de mi desempeño?
•¿Acepto evaluaciones de ese desempeño?
•¿Corrijo o mantengo mi actuación en base a esas medidas y evaluaciones?

C- Plan de acción.

•¿Poseo una clara visión del proceso que debo seguir para garantizar el crecimiento personal y colectivo?
•¿Me veo con la disciplina de seguir el proceso?
•¿Qué estoy dispuesto a sacrificar por dicho proceso de crecimiento?

Este esquema adaptado ayudará a los profesionales armados a:

1. Definir el objetivo buscado y el propósito del mismo.
2. Generar una estrategia enfocada y coherente.
3. Ejecutarlo con precisión y orden.

Para tener éxito en la ascensión de nuestro Valknut Estratégico debemos definir claramente lo que buscamos ejecutar. Siendo muy importante respetar que cada factor es vital, y que descuidar uno cualquiera puede poner en peligro todo el proceso.

¿Estamos dedicando suficiente atención a crear nuestra estrategia de crecimiento y… supervivencia?

¿Y a la aplicación de la misma al equipo y a la sociedad que juramos Servir y Proteger?

Cuídense y cuiden de los suyos.

COMING SOON...

AGENCIA DE INTELIGENCIA ANTITERRORISTA

NERTOM

SEGURIDAD

WWW.ALGHURABA.ORG

EL NUEVO LIDERAZGO DE HEZBOLLAH

EL ASCENSO DEL SHEIKH ALI DAMOUSH

Danilo Gelman.
Analista de terrorismo y extremismos violentos.

Foto: www.saba.ye

INTRODUCCIÓN

La transición de liderazgo en Hezbollah marca un desarrollo significativo en la dinámica interna y las actividades externas de la organización. Tras la eliminación de Hashem Safi al-Din, exjefe del Consejo Ejecutivo, el 4 de octubre de 2024, varios informes indican que Sheikh Ali Damoush ha sido nombrado el nuevo jefe del Consejo Ejecutivo, lo que lo convierte en uno de los responsables principales de la gestión interna del grupo, supervisando sus actividades políticas, sociales y administrativas en el Líbano. También ha sido señalado como uno de los portavoces más visibles de la organización y un enlace importante con otros grupos y líderes en la región.

Este cambio plantea interrogantes sobre la dirección futura de Hezbollah, tanto dentro del Líbano como en el escenario internacional. Este artículo analiza el perfil de Sheikh Ali Damoush, su ascenso dentro de Hezbollah y las posibles implicaciones de su liderazgo.

PERFIL DEL SHEIKH ALI DAMAOUSH

Nacido en 1962, Sheikh Ali Damoush creció en un hogar islámico tradicional. Su padre era un erudito en enseñanzas islámicas, y su madre provenía de la comunidad alauita. Su crianza religiosa y su temprana exposición al conocimiento islámico sentaron las bases para sus futuros roles en Hezbollah.

La educación religiosa de Damoush comenzó con mayor profundidad después de la guerra civil libanesa en 1977, cuando se trasladó a Najaf, Irak. Sin embargo, sus estudios fueron interrumpidos por el régimen de Saddam Hussein, que lo arrestó y lo deportó de regreso al Líbano. Lejos de desanimarse, Damoush continuó su formación religiosa en el Instituto de Sharia Islámica en Beirut. Tras la victoria de la Revolución Islámica en Irán en 1979, se trasladó a Qom, Irán, donde pasó catorce años estudiando, enseñando y realizando giras de da'wah (predicación) en Irán, Líbano y África.

Al regresar al Líbano en 1994, Damoush se unió al Instituto de Sharia Islámica como parte de su cuerpo administrativo y científico. Poco después, comenzó su participación en Hezbollah. Entre 1994 y 1998, se desempeñó como juez en los tribunales de sharia de Hezbollah antes de unirse al Consejo Ejecutivo.

Ha ocupado el cargo de representante del líder de Hezbollah, Hassan Nasrallah, en varios eventos y reuniones de alto nivel, siendo considerado parte de su círculo íntimo y uno de sus asesores de confianza. Su nombre ha sido mencionado en múltiples informes internacionales debido a su participación en la expansión de la red global de Hezbollah, particularmente en actividades vinculadas al financiamiento y reclutamiento. Como resultado de su rol en estas operaciones, Estados Unidos lo sancionó por su relación directa con las actividades internacionales del grupo, especialmente aquellas relacionadas con la propaganda y la recaudación de fondos.

COMPARACIÓN CON SU PREDECESOR Y CAMBIOS ESPERADOS

En comparación con su predecesor, Hashem Safi al-Din, Damoush representa una versión más pragmática del liderazgo de Hezbollah. Mientras que Safi al-Din se centraba en la coordinación estratégica con Irán y la supervisión de la estructura militar del grupo, Damoush se ha destacado por su enfoque en la expansión ideológica y en la consolidación de las redes de Hezbollah en el extranjero, particularmente en América Latina y África.

Damoush también es visto como un líder con una base religiosa más fuerte, lo que podría reforzar la influencia del componente teocrático en la toma de decisiones del grupo.

EL ROL DE DAMOUSH EN HEZBOLLAH

Damoush ha ocupado varios puestos clave dentro de Hezbollah, contribuyendo a las estrategias políticas, culturales y de relaciones exteriores de la organización. En 1998, se unió al Consejo Ejecutivo y supervisó la Unidad de Cultura hasta el 2001. Posteriormente, se convirtió en el jefe de la Unidad de Relaciones Exteriores, desempeñando efectivamente el papel de ministro de relaciones exteriores de Hezbollah.

LA UNIDAD DE RELACIONES EXTERIORES

La Unidad de Relaciones Exteriores del Consejo Ejecutivo de Hezbollah funciona como un enlace crítico entre Hezbollah y gobiernos extranjeros, partidos políticos y otras entidades. Proporciona apoyo logístico a los miembros de Hezbollah en el extranjero, incluidos aquellos en la Unidad 910, responsable -entre otras tareas- de ataques terroristas fuera del Líbano.

Bajo el liderazgo de Damoush, la unidad desempeñó un papel central en la captación y operación de colaboradores, ofreciendo apoyo logístico y garantizando la seguridad de las actividades internacionales de Hezbollah. La unidad también organizó manifestaciones en apoyo de Hezbollah e Irán en el extranjero.

ROL ACTUAL EN EL NUEVO LIDERAZGO

Como jefe del Consejo Ejecutivo, Damoush es el máximo responsable de las actividades no militares de Hezbollah, gestionando los proyectos sociales, educativos y económicos que permiten a la organización mantener una base de apoyo fuerte entre la población chiita del Líbano. Esto lo convierte en un líder clave en la estructura de poder interna, con influencia directa en el control de los fondos y programas de asistencia social.

Damoush actúa como intermediario entre las alas política y religiosa del movimiento. Tiene un discurso cargado de referencias ideológicas y religiosas, consolidando su posición como uno de los principales ideólogos del grupo. Esto le permite mantener la cohesión doctrinaria y estratégica en tiempos de crisis interna. Expansión internacional y relaciones externas: Aunque no es directamente parte de la Unidad 910 (el brazo externo operativo de Hezbollah), Damoush supervisa las actividades de apoyo internacional, incluyendo la coordinación con la diáspora libanesa y redes de financiamiento en América Latina, África y Europa. Es una figura clave en la promoción del discurso de resistencia y en la consolidación del soft power de Hezbollah a nivel global. Con el avance del tiempo y el desgaste de líderes históricos como Hassan Nasrallah, Ali Damoush representa la transición generacional del liderazgo. Pertenece a una nueva camada de dirigentes más pragmáticos, capaces de combinar la tradición ideológica del grupo con la necesidad de una estructura de poder más funcional.

IMPACTO EN AMÉRICA LATINA

Bajo la dirección de Damoush, Hezbollah podría intensificar su presencia en América Latina mediante el refuerzo de redes de financiamiento y lavado de dinero en la región de la Triple Frontera (Argentina, Brasil y Paraguay). Históricamente, la organización ha utilizado la comunidad chiita libanesa en esta área para movilizar fondos y recursos. Damoush, con su experiencia en la expansión internacional de Hezbollah, podría fortalecer estas redes y consolidar la influencia del grupo en la región.

EL IMPACTO DEL LIDERAZGO DE DAMOUSH

El nombramiento del Sheikh Ali Damoush como jefe del Consejo Ejecutivo indica una continuación de los estrechos vínculos de Hezbollah con Irán y su énfasis en mantener una presencia externa robusta. Sin embargo, el trasfondo de Damoush en la educación religiosa y su experiencia en relaciones exteriores sugieren que su liderazgo puede centrarse en fortalecer la influencia ideológica y las redes internacionales de Hezbollah.

APARICIONES DE DAMOUSH EN LOS MEDIOS

Sheikh Ali Damoush ha tenido una presencia notable en los medios de comunicación alineados con Hezbollah, donde sus declaraciones refuerzan el discurso de resistencia y desafío hacia Israel y Estados Unidos. Según Al-Ahed News, Damoush realizó declaraciones en las que destacó que las amenazas repetidas de Israel hacia el Líbano se han vuelto "aburridas y vacías" y reflejan la confusión, la ansiedad y el miedo que tiene el enemigo hacia Hezbollah.

Damoush subrayó que la situación en Gaza demuestra la debilidad de Israel, señalando que el enemigo que está "dando tumbos en Gaza y hundiéndose en sus arenas" es demasiado débil para llevar a cabo sus amenazas contra el Líbano. Además, enfatizó que la brutalidad estadounidense-sionista solo puede ser contenida mediante la fuerza y las acciones de la resistencia. Según sus palabras, si no fuera por la fortaleza de la resistencia en el Líbano, sus misiles, armas y las estrategias creadas por Hezbollah, Israel habría expandido su agresión desde el primer día.

Concluyó diciendo que cualquier intento del enemigo de dañar la soberanía libanesa o cambiar la realidad existente en el sur del Líbano es una fantasía. "Esta tierra es nuestra tierra y nadie puede arrancarnos de ella ni restringir nuestro movimiento en ella", afirmó Damoush, dejando claro el compromiso de Hezbollah de defender el territorio y su libertad de acción en el sur del Líbano.

DESIGNACIÓN POR EL DEPARTAMENTO DE ESTADO DE EE. UU.

El 9 de enero de 2016, el Departamento de Estado de los Estados Unidos designó a Sheikh Ali Damoush como Terrorista Global Especialmente Designado en virtud de la Orden Ejecutiva 13224. Esta designación destaca su papel central en las actividades internacionales de Hezbollah, incluidas sus operaciones externas y su apoyo a actos terroristas.

Implicaciones Regionales

El liderazgo de Damoush podría tener importantes implicaciones para la política interna del Líbano y para el Medio Oriente en general. Sus estrechos vínculos con Irán pueden reforzar el papel de Hezbollah como proxy de los intereses de Teherán en la región. Además, su experiencia en la gestión de relaciones exteriores indica que Hezbollah probablemente continuará participando en actividades internacionales, incluidas las de apoyo logístico y operativo para sus miembros en el extranjero.

Implicaciones Internacionales

Las actividades de Hezbollah en países extranjeros, particularmente a través de la Unidad 910, han sido motivo de preocupación para varios gobiernos. El liderazgo de Damoush podría dar lugar a un enfoque más sofisticado en las operaciones externas de Hezbollah, aumentando potencialmente el alcance y la influencia de la organización más allá del Medio Oriente.

DESAFÍOS FUTUROS

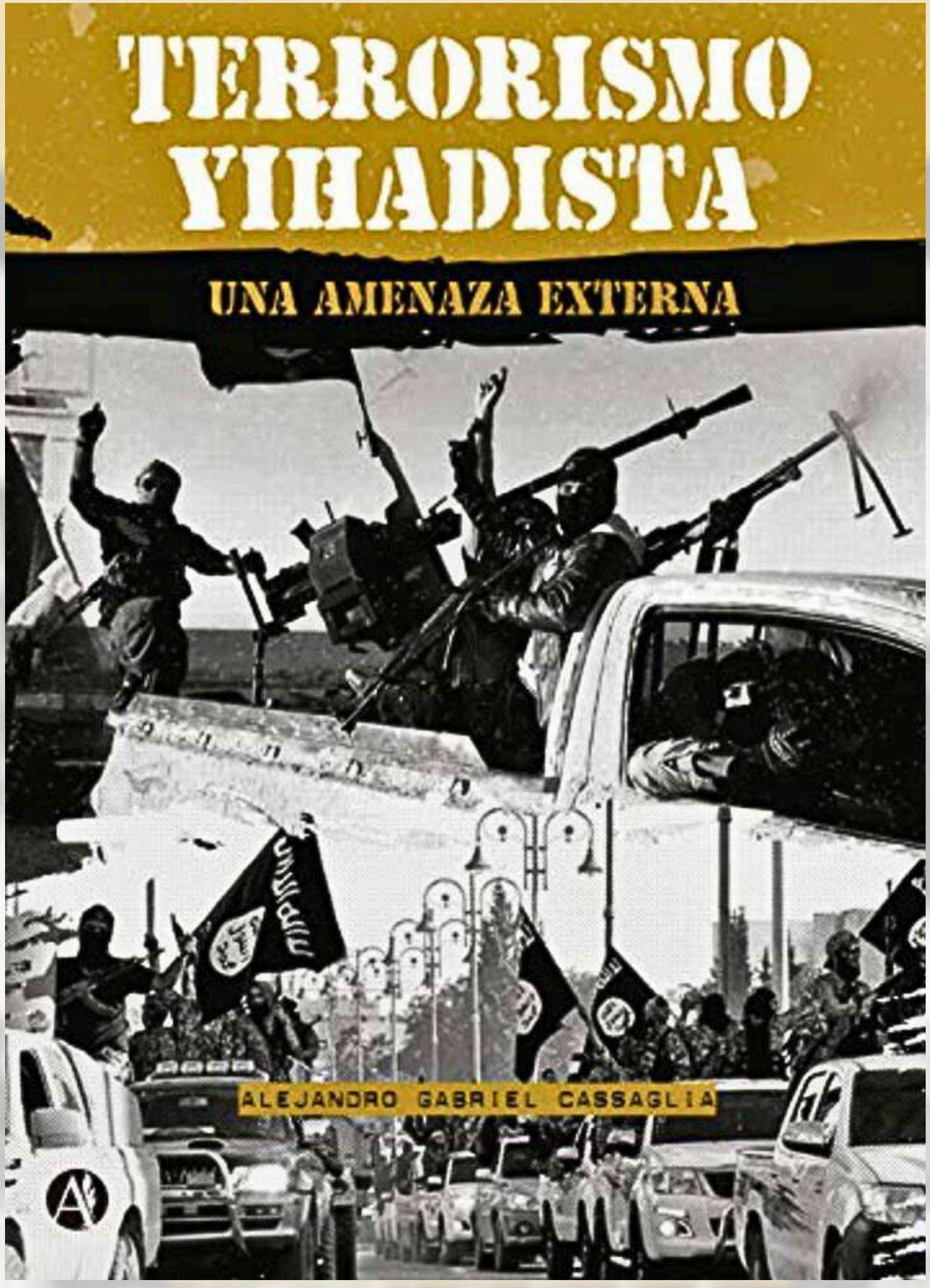
A pesar de su vasta experiencia, Damoush enfrenta varios desafíos como nuevo jefe del Consejo Ejecutivo. La situación financiera de Hezbollah, su participación en conflictos regionales y la creciente oposición interna en el Líbano podrían dificultar la implementación de su visión para la organización.

Además, la designación de Hezbollah como organización terrorista por varios países plantea desafíos constantes a sus actividades internacionales. Damoush tendrá que sortear estos desafíos mientras mantiene los objetivos ideológicos y operativos de la organización.

CONCLUSIÓN

El ascenso de Sheikh Ali Damoush como nuevo jefe del Consejo Ejecutivo de Hezbollah marca un momento crucial para la organización. Su formación en educación religiosa y su amplia experiencia en relaciones exteriores lo posicionan como una figura clave para moldear el futuro de Hezbollah. Sin embargo, su liderazgo será puesto a prueba por desafíos internos y externos mientras Hezbollah navega un complejo panorama geopolítico.

Los próximos meses revelarán la dirección que Damoush pretende tomar para Hezbollah y las implicaciones de su liderazgo para el Líbano y el Medio Oriente en general. Comprender sus prioridades y estrategias es esencial para los responsables políticos y expertos en seguridad que buscan abordar la amenaza evolutiva que representa Hezbollah.



CÓMPRALO EN AMAZON

¡Haz clic aquí!

TINTA IMPRESCINDIBLE

ARANZADI

Título: Los grupos juveniles violentos de origen latino y su consideración jurídica en España

Autor: Dr. José. Miguel Romero Parra

Los grupos juveniles violentos de origen latino se han consolidado en España, aumentando sus actividades delictivas y su violencia. Aunque se ha investigado este fenómeno desde perspectivas criminológicas y sociológicas, es esencial abordarlo desde el ámbito jurídico-penal. Esta obra tiene como objetivo analizar estos grupos como organizaciones criminales y examinar los problemas de probar la pertenencia de sus miembros para fundamentar sentencias condenatorias. También se explorarán las dificultades en la obtención de pruebas, que afectan el principio de presunción de inocencia.La violencia es una constante en la vida de estos jóvenes, manifestándose como violencia estructural por limitaciones económicas y física entre bandas rivales. Además, se analiza el uso de las redes sociales por menores para captar nuevos miembros y organizar actividades violentas, así como para difundir su identidad y simbología.

CONTRA-NARRATIVA

WWW.ALGHURABA.ORG

LA TECNOLOGÍA EN EL MUNDO CRIMINAL

ANÁLISIS SOBRE LAS IMPLICACIONES Y DESAFÍOS (2ª PARTE)

Sergio Colado.
Psicólogo, ingeniero, analista de comportamiento. Profesor y divulgador sobre ciencia y tecnología.

INTRODUCCIÓN

El impacto de la tecnología en la sociedad ha sido transformador, redefiniendo desde las interacciones cotidianas hasta los modelos económicos y las estructuras de seguridad global. Sin embargo, el mismo avance tecnológico que ha impulsado el desarrollo en múltiples sectores, ha sido aprovechado por actores criminales para perfeccionar sus tácticas, optimizar sus operaciones y ampliar el alcance de sus delitos.

El surgimiento de herramientas avanzadas como la inteligencia artificial (IA), el Internet de las Cosas (IoT) y la automatización, ha generado una nueva dimensión del crimen digital, donde las actividades ilícitas pueden ejecutarse con una sofisticación, velocidad y nivel de anonimato sin precedentes.

La ciberdelincuencia ha evolucionado más allá de los ataques informáticos tradicionales, adoptando modelos como el Crime-as-a-Service (CaaS), donde los criminales pueden alquilar herramientas de hacking o contratar ataques personalizados

en la dark web. Del mismo modo, el uso de deepfakes en fraudes financieros, la explotación de criptomonedas para el lavado de dinero y la automatización de ataques de ransomware, han permitido que tanto individuos como organizaciones criminales maximicen su rentabilidad y reduzcan los riesgos de detección. Además, el crimen organizado ha incorporado tecnologías emergentes en sus operaciones, utilizando drones autónomos para el tráfico de drogas, IoT para el rastreo de operativos policiales y algoritmos predictivos para ajustar sus estrategias de evasión.

A nivel geopolítico, el ciberterrorismo y la radicalización en línea han convertido al ciberespacio en un campo de batalla estratégico, donde los grupos extremistas utilizan redes sociales, foros y plataformas de mensajería encriptada para reclutar miembros, financiar actividades ilícitas y planificar atentados. A su vez, la manipulación de la información mediante campañas de desinformación basadas en IA ha demostrado ser una herramienta eficaz para influir en procesos electorales, desestabilizar gobiernos y generar polarización social.

Frente a esta nueva era del crimen digital, las estrategias tradicionales de seguridad y regulación han quedado rezagadas, lo que ha permitido que los delincuentes se mantengan un paso por delante de las autoridades. La falta de marcos regulatorios globales y la ausencia de cooperación internacional efectiva han facilitado que los ciberdelincuentes operen desde jurisdicciones con legislaciones laxas, lo que dificulta la persecución y extradición de estos actores.
La rápida evolución de las amenazas digitales ha expuesto las debilidades de los sistemas de ciberseguridad en sectores críticos como infraestructura energética, salud, transporte y servicios financieros, donde un solo ataque exitoso puede desencadenar consecuencias devastadoras a nivel nacional e internacional.

Este estudio tiene como objetivo analizar cómo la tecnología ha transformado el crimen, y también evaluar los riesgos emergentes asociados con la digitalización de las actividades delictivas. A través de un enfoque multidisciplinario que combina criminología, ciberseguridad, inteligencia artificial y estudios sobre terrorismo, se examinarán las tendencias delictivas impulsadas por la tecnología, las estrategias de mitigación implementadas y los desafíos regulatorios que aún persisten. Asimismo, se explorarán soluciones innovadoras que permitan garantizar un equilibrio entre seguridad, privacidad y derechos digitales en un mundo cada vez más interconectado.

SABOTAJE DE INFRAESTRUCTURAS CRÍTICAS A TRAVÉS DEL IoT

La integración del Internet de las Cosas (IoT) en sistemas industriales, hospitales y redes de transporte ha generado una revolución en la eficiencia y automatización de infraestructuras críticas. Sin embargo, esta interconectividad también ha expuesto a estos sistemas a nuevas y sofisticadas ciberamenazas, convirtiéndolos en objetivos estratégicos para el sabotaje y el ciberterrorismo.

Según un informe de la ONU (2024), los ataques dirigidos a dispositivos IoT en infraestructuras clave han aumentado drásticamente, afectando la estabilidad y seguridad de múltiples sectores. Uno de los sectores más vulnerables es el de redes eléctricas y plantas de energía, donde el control de sistemas basados en IoT ha sido objeto de ataques con consecuencias devastadoras. En 2022, el grupo hacker Sandworm, vinculado a Rusia, lanzó un ataque contra los sistemas de control industrial IoT en Ucrania, provocando cortes de energía en varias ciudades. Este ataque demostró la capacidad de los ciberdelincuentes para manipular infraestructuras eléctricas a gran escala, generando un impacto significativo en la operatividad de hospitales, redes de transporte y servicios de emergencia (Journal of Infrastructure Security, 2024).

El sector sanitario también ha sido gravemente afectado por el sabotaje de dispositivos médicos IoT. En 2021, un hospital en Alemania fue víctima de un ataque de ransomware dirigido a sus dispositivos IoT conectados, afectando equipos médicos esenciales como respiradores y monitores de signos vitales. Como resultado del bloqueo de estos sistemas, un paciente falleció al no poder recibir atención médica oportuna, marcando el primer caso documentado de una muerte directamente relacionada con un ciberataque a IoT en el ámbito sanitario (European Journal of Emergency Medicine, 2024).

El transporte inteligente es otro ámbito en el que los ataques a sistemas IoT han causado graves interrupciones. Investigaciones de la Unión Europea (2024) han revelado que ciberataques dirigidos a redes de semáforos y trenes automatizados han generado deliberadas alteraciones en el tráfico urbano en ciudades como Londres y Nueva York. Al explotar vulnerabilidades en los sistemas de control de tráfico, los atacantes han logrado desincronizar semáforos, generar congestión masiva e incluso forzar la detención de trenes automatizados, evidenciando el impacto que estos ataques pueden tener en la movilidad y la seguridad ciudadana. El Foro Económico Mundial (2025) advierte que el sabotaje de infraestructuras críticas mediante IoT podría convertirse en una de las principales amenazas de seguridad en la próxima década. A medida que las ciudades y los sectores estratégicos continúan adoptando dispositivos conectados, la falta de medidas de ciberseguridad robustas aumenta el riesgo de que estos sistemas sean explotados para espionaje, interrupciones masivas o incluso ataques cibernéticos coordinados con conflictos geopolíticos.

USO DEL IoT EN EL CRIMEN ORGANIZADO

El Internet de las Cosas ha sido adoptado por carteles de narcotráfico y redes criminales como una herramienta estratégica para optimizar sus operaciones, mejorar su logística y reducir su exposición a las fuerzas del orden. La creciente conectividad de dispositivos ha permitido que estos grupos utilicen tecnologías avanzadas para monitorear rutas de tráfico ilegal, evadir operativos de seguridad y maximizar sus ganancias a través de actividades delictivas tecnológicamente sofisticadas.

Uno de los usos más preocupantes del IoT en el crimen organizado es el empleo de drones autónomos para el narcotráfico. En México, se ha reportado que carteles han comenzado a utilizar drones equipados con inteligencia artificial para transportar drogas a través de la frontera con Estados Unidos sin intervención humana. Estos dispositivos pueden ajustar su trayectoria en tiempo real, evadir radares y cambiar de ruta automáticamente en función de las condiciones de vigilancia, lo que los convierte en una herramienta eficaz para el contrabando de sustancias ilegales (Interpol Criminal Intelligence Report, 2023).

Otra aplicación clave del IoT en actividades criminales es el rastreo de operativos policiales mediante el uso de sensores IoT y rastreadores GPS. Carteles en América Latina han implementado estos dispositivos en vehículos, drones y escondites estratégicos para monitorear en tiempo real el movimiento de las fuerzas de seguridad y ajustar sus rutas de transporte ilegal para evitar controles y redadas. Esta tecnología permite a los criminales anticiparse a los operativos, planificar rutas seguras y minimizar el riesgo de incautaciones y arrestos (Journal of Illicit Networks, 2024).

Además, el IoT también ha sido explotado para actividades ilícitas como la cripto minería ilegal. Grupos criminales han secuestrado miles de dispositivos IoT vulnerables, como cámaras de seguridad, routers domésticos y electrodomésticos conectados, para utilizarlos en la minería de criptomonedas sin el conocimiento de sus propietarios. Este tipo de ataque, conocido como cryptojacking, permite a los delincuentes aprovechar el poder computacional de estos dispositivos de forma distribuida, generando ingresos millonarios con un impacto mínimo en el consumo energético de cada equipo infectado, lo que dificulta su detección (MIT Blockchain & Security Journal, 2024).

El uso del IoT por el crimen organizado representa un desafío creciente para las fuerzas de seguridad y la ciberseguridad global, ya que estas tecnologías permiten a los delincuentes automatizar sus operaciones, reducir el riesgo de exposición y explotar vulnerabilidades en infraestructuras digitales sin necesidad de interacción humana directa.

ESTRATEGIAS DE MITIGACIÓN Y DESAFÍOS REGULATORIOS

El crecimiento de la ciberdelincuencia impulsada por la inteligencia artificial (IA) y el Internet de las Cosas (IoT) ha desafiado los marcos regulatorios y las estrategias tradicionales de seguridad digital.

A medida que los ataques se vuelven más sofisticados, los gobiernos, organismos internacionales y empresas tecnológicas han desarrollado estrategias para mitigar los riesgos y fortalecer la ciberseguridad global. Sin embargo, la evolución acelerada de estas amenazas ha generado desafíos regulatorios significativos.

El análisis identificó cinco áreas clave en la mitigación del crimen digital y los desafíos regulatorios asociados:

1)Inteligencia artificial en la detección del crimen digital.
2)Cooperación internacional en ciberseguridad.
3)Regulación del uso de IA e IoT.
4)Avances en ciberdefensa para infraestructuras críticas.
5)Educación y formación en ciberseguridad.

INTELIGENCIA ARTIFICIAL EN LA DETECCIÓN Y PREVENCIÓN DEL CRIMEN DIGITAL

La inteligencia artificial se ha convertido en una herramienta clave para la identificación temprana de ciberataques y la automatización de respuestas ante amenazas digitales. Gracias a su capacidad para analizar grandes volúmenes de tráfico en tiempo real, los algoritmos de aprendizaje automático pueden detectar patrones anómalos y ataques en curso con una precisión superior al 90%, lo que ha revolucionado el ámbito de la ciberseguridad (Glickman & Sharot, 2024).

Las aplicaciones de IA en ciberseguridad han permitido mejorar la detección de fraudes financieros, utilizando algoritmos de machine learning (aprendizaje automático) que analizan transacciones en redes bancarias en milisegundos para identificar comportamientos sospechosos y bloquear operaciones fraudulentas antes de que se concreten. Este enfoque proactivo ha sido implementado por entidades financieras en todo el mundo, reduciendo el impacto de ataques como el phishing bancario y el fraude con tarjetas de crédito (European Financial Security Report, 2024).

Otra de las aplicaciones más relevantes de la IA en la ciberseguridad es el análisis de patrones en ataques de denegación de servicio (DDoS). Los sistemas de IA pueden predecir y bloquear intentos de sobrecarga de servidores antes de que causen daños significativos, utilizando modelos de detección de tráfico anómalo y adaptándose a nuevas tácticas de ataque en tiempo real. Este tipo de soluciones ha sido clave en la protección de infraestructuras críticas y en la defensa de servicios en la nube, que son objetivos recurrentes de los ciberdelincuentes (MIT AI & Security Journal, 2024).

La IA también ha demostrado ser eficaz en la identificación de deepfakes y fraudes de identidad, un problema creciente en la era de la desinformación y la manipulación digital. Algunas herramientas avanzadas han logrado una precisión del 99% en la detección de videos falsificados, lo que representa un avance significativo en la lucha contra la manipulación mediática y el fraude en identidades digitales (Journal of Cybercrime & AI, 2024).

Uno de los casos más destacados de aplicación de IA en la ciberseguridad es el sistema desarrollado por Google DeepMind, que ha conseguido identificar intentos de phishing con una tasa de detección del 98%, superando a los enfoques tradicionales basados en listas negras y heurísticas. Este sistema emplea modelos de IA capaces de analizar la estructura de correos electrónicos y páginas web fraudulentas, identificando anomalías en tiempo real y bloqueando intentos de robo de credenciales antes de que lleguen a los usuarios (IEEE Transactions on Cybersecurity, 2023).

La incorporación de inteligencia artificial en la detección y prevención del crimen digital no solo ha fortalecido la seguridad en redes corporativas y gubernamentales, sino que también ha permitido a los sistemas de defensa adaptarse dinámicamente a las amenazas emergentes, mitigando los ataques de manera más efectiva que los enfoques convencionales.

Sin embargo, a medida que la IA se convierte en un arma esencial en la lucha contra el cibercrimen, los atacantes también han comenzado a emplearla para evadir medidas de seguridad y desarrollar métodos de ataque más sofisticados. Esto plantea un desafío constante, donde la innovación en ciberseguridad debe evolucionar a la misma velocidad que las tácticas de los ciberdelincuentes para garantizar la protección de la infraestructura digital global.

COOPERACIÓN INTERNACIONAL EN CIBERSEGURIDAD

El crimen digital no conoce fronteras, lo que ha llevado a los países a fortalecer la cooperación internacional en la lucha contra la ciberdelincuencia. La creciente sofisticación de los ataques informáticos y su impacto en infraestructuras críticas, instituciones financieras y ciudadanos ha obligado a los organismos de seguridad a unir esfuerzos, compartir inteligencia y establecer marcos legales comunes para combatir estas amenazas de manera más efectiva.

Según un informe de INTERPOL (2024), algunas de las iniciativas de cooperación internacional más relevantes incluyen el Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001 y actualizado en 2022. Este tratado representa el primer marco legal internacional diseñado para facilitar la extradición de ciberdelincuentes y la cooperación en investigaciones de delitos digitales, estableciendo procedimientos para el acceso a evidencia electrónica y la persecución de delitos informáticos a nivel transnacional.

Otra iniciativa clave es la INTERPOL Cybercrime Directorate, una plataforma de intercambio de inteligencia entre cuerpos de seguridad de más de 150 países. Este organismo permite a los países coordinar esfuerzos para rastrear redes criminales, identificar patrones de ataque y desarrollar estrategias conjuntas para la prevención y respuesta ante ciberamenazas. De manera similar, la EUROPOL Internet Referral Unit es un programa de la Unión Europea especializado en el rastreo y eliminación de contenido ilegal en la web, con un enfoque particular en la distribución de material ilícito, propaganda terrorista y actividades fraudulentas en línea.

En 2023, la Operación HAECHI III, coordinada por INTERPOL, permitió la detención de más de 1,300 ciberdelincuentes en Asia y Europa, logrando la incautación de 130 millones de dólares en fondos ilícitos provenientes de fraudes financieros, ataques de ransomware y estafas en línea. Esta operación demostró la efectividad de la cooperación internacional en la lucha contra la ciberdelincuencia y el impacto que pueden tener las acciones conjuntas para desarticular redes criminales transnacionales (Interpol Cybercrime Report, 2024).

Sin embargo, a pesar de los avances logrados en cooperación internacional, aún existen desafíos significativos en la armonización de los esfuerzos globales contra el cibercrimen. La falta de uniformidad en las legislaciones nacionales, las diferencias en la protección de datos y derechos digitales, y la resistencia de algunos países a compartir información sobre amenazas cibernéticas siguen siendo obstáculos que dificultan una respuesta global más efectiva (OCDE, 2021).

Para fortalecer la lucha contra la ciberdelincuencia, es fundamental avanzar hacia una mayor armonización legislativa, mejorar los mecanismos de cooperación en tiempo real y garantizar que las políticas de ciberseguridad globales incluyan sanciones efectivas contra los ciberdelincuentes y sus redes de financiación. Solo mediante un enfoque coordinado y una mayor colaboración internacional será posible mitigar los riesgos del crimen digital y garantizar la seguridad del ecosistema digital a nivel global.

REGULACIÓN DEL USO DE LA IA E IoT EN LA SEGURIDAD DIGITAL

La regulación de las tecnologías emergentes, como la inteligencia artificial y el Internet de las Cosas, se ha convertido en un desafío global. Mientras algunos países han avanzado en la implementación de normativas estrictas para regular su uso, otros carecen de marcos regulatorios sólidos, lo que deja vacíos legales que pueden ser explotados por ciberdelincuentes y actores malintencionados. La falta de un consenso internacional sobre cómo regular estas tecnologías ha dificultado la lucha contra el crimen digital y la protección de la privacidad y la seguridad de los ciudadanos.

Uno de los avances más importantes en esta área es la Ley de IA de la Unión Europea (2024), considerada la primera legislación integral que regula el uso de la inteligencia artificial en sistemas críticos. Esta normativa impone restricciones estrictas sobre el uso de IA en vigilancia masiva, identificación biométrica en tiempo real y toma de decisiones automatizadas con impacto significativo en derechos fundamentales. Además, establece niveles de riesgo para diferentes aplicaciones de IA, prohibiendo aquellas que representen un peligro claro para la privacidad y la seguridad de los ciudadanos (EU AI Act, 2024).

En el ámbito del Internet de las Cosas, Estados Unidos implementó en 2020 la Ley de Seguridad en IoT, la cual exige que todos los dispositivos conectados utilizados por el gobierno cumplan con estándares de seguridad estrictos. Esto incluye actualizaciones automáticas de firmware, encriptación de datos y mecanismos de autenticación robustos, con el objetivo de reducir la vulnerabilidad de estos dispositivos ante ataques cibernéticos. Sin embargo, este tipo de regulación solo aplica a dispositivos gubernamentales, dejando desprotegido un gran porcentaje de los dispositivos IoT utilizados en entornos privados y comerciales (U.S. National Institute of Standards and Technology, NIST, 2023).

Por otro lado, China ha establecido un marco de regulación más restrictivo sobre IA y reconocimiento facial. En 2024, el gobierno chino implementó controles sobre el uso de estas tecnologías para evitar abusos en privacidad y garantizar el consentimiento explícito de los ciudadanos antes de ser sometidos a procesos de identificación biométrica. Esta medida responde a preocupaciones crecientes sobre el uso masivo de cámaras de vigilancia y software de reconocimiento facial en espacios públicos, lo que ha llevado a debates sobre el equilibrio entre seguridad y derechos individuales (Asian Cybersecurity Review, 2024).

A pesar de estos avances, la falta de una regulación global unificada sigue siendo un obstáculo en la lucha contra el crimen digital. Según Velasco et al. (2024), la ausencia de estándares internacionales dificulta la persecución de delitos cibernéticos, ya

que muchos ciberdelincuentes operan desde países con legislaciones laxas o sin tratados de extradición, lo que les permite evadir la justicia.

Para mitigar estos riesgos, es crucial que los gobiernos trabajen en acuerdos multilaterales que permitan la creación de un marco regulatorio global sobre IA e IoT, estableciendo estándares mínimos de seguridad y privacidad. Además, es fundamental que las empresas tecnológicas asuman una mayor responsabilidad en la transparencia y supervisión de sus algoritmos, evitando el uso indebido de estas tecnologías para la vigilancia masiva o la manipulación de la información.

Sin una regulación coordinada y efectiva, la rápida evolución de la IA y el IoT continuará representando una amenaza para la seguridad digital, la privacidad y los derechos fundamentales a nivel global.

AVANCES EN CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRÍTICAS

Las infraestructuras críticas, como redes eléctricas, hospitales y sistemas de transporte, se han convertido en objetivos estratégicos para ciberataques cada vez más sofisticados, lo que ha impulsado el desarrollo de nuevas estrategias de ciberdefensa. La creciente digitalización y la integración del Internet de las Cosas en estos sistemas han aumentado su vulnerabilidad, exigiendo la implementación de medidas avanzadas de seguridad para prevenir interrupciones y sabotajes que podrían tener consecuencias devastadoras.

Una de las estrategias más innovadoras en este ámbito es la ciberseguridad basada en IA. Algunas empresas han desarrollado sistemas de inteligencia artificial capaces de detectar y responder a ciberataques en infraestructuras críticas en tiempo real. Estos sistemas utilizan modelos de aprendizaje automático para identificar patrones anómalos, lo que permite neutralizar amenazas antes de que causen daños significativos. A diferencia de los métodos tradicionales, la IA puede adaptarse dinámicamente a nuevas tácticas de ataque, brindando una defensa más efectiva contra amenazas emergentes (MIT Technology Review, 2024).

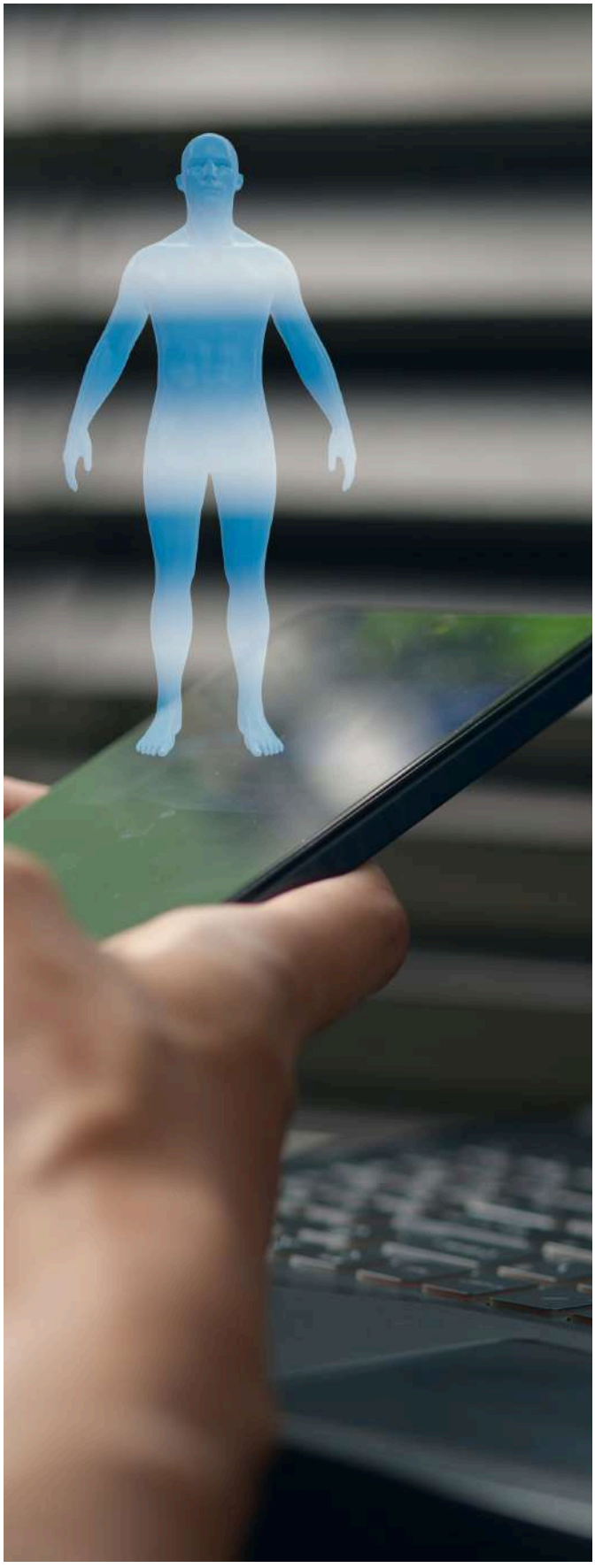
Otra tecnología clave en la ciberdefensa proactiva es la simulación de ataques con digital twins. Mediante el uso de gemelos digitales, las organizaciones pueden modelar ciberataques en un entorno virtual, permitiendo evaluar la efectividad de las defensas sin exponer los sistemas reales a riesgos. Esta técnica ha sido utilizada para probar la resiliencia de infraestructuras críticas ante ataques de ransomware y sabotajes cibernéticos, proporcionando información valiosa para fortalecer las estrategias de seguridad antes de que ocurra un incidente real (Journal of Critical Infrastructure Protection, 2024).

La segmentación de redes y la protección del IoT también han sido fundamentales para la defensa de infraestructuras críticas. La implementación de arquitecturas de confianza cero (zero-trust architectures) ha permitido restringir el acceso a dispositivos IoT en entornos industriales, evitando que una brecha de seguridad en un solo dispositivo comprometa sistemas enteros. Estas arquitecturas exigen autenticación y verificación constante para cada dispositivo y usuario, minimizando el impacto de accesos no autorizados y limitando la propagación de ataques dentro de las redes (Cisco Zero Trust Security Whitepaper, 2023).

El impacto de estas estrategias ya ha sido demostrado en la práctica. En 2023, la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. (CISA) evitó un ciberataque dirigido contra una planta de tratamiento de agua gracias a la implementación de inteligencia artificial, segmentación de redes y simulación de ataques con gemelos digitales. Estas

tecnologías permitieron detectar la intrusión antes de que los atacantes pudieran comprometer los sistemas operativos de la planta, evitando potenciales interrupciones en el suministro de agua potable (CISA Annual Report, 2024).

El futuro de la ciberdefensa para infraestructuras críticas dependerá de la capacidad de los gobiernos y empresas para integrar estas tecnologías de manera eficiente y coordinada. La combinación de IA para detección de amenazas, modelos predictivos basados en digital twins y arquitecturas de seguridad avanzadas representa la mejor oportunidad para proteger los sistemas esenciales de la sociedad frente a las amenazas cibernéticas en constante evolución. Sin una estrategia de seguridad robusta y en constante actualización, las infraestructuras críticas seguirán siendo vulnerables a ataques que podrían tener consecuencias económicas, sociales y políticas a gran escala.



EDUCACIÓN Y FORMACIÓN EN CIBERSEGURIDAD

La formación en ciberseguridad se ha convertido en un aspecto fundamental en la prevención de ataques informáticos, dado que el 90% de los ciberataques exitosos involucran errores humanos (Foro Económico Mundial, 2025). La falta de conciencia sobre buenas prácticas digitales y el desconocimiento de tácticas de ingeniería social han facilitado la propagación de ataques como el phishing, ransomware y el acceso no autorizado a infraestructuras críticas. Por ello, invertir en educación y capacitación en ciberseguridad es una estrategia esencial para fortalecer la defensa contra el crimen digital.

Diversos programas e iniciativas han sido diseñados para mejorar la formación en ciberseguridad tanto en el ámbito corporativo como en el sector público. Un ejemplo de ello es el programa "Cyber Awareness Europe" (2024), que busca capacitar a empleados del sector público y privado en la Unión Europea en la prevención de amenazas digitales, ofreciendo cursos especializados en manejo de datos sensibles, detección de ataques y respuesta ante incidentes. Esta iniciativa busca reducir la vulnerabilidad en infraestructuras críticas y

minimizar los errores humanos que facilitan los ataques informáticos. En el ámbito corporativo y profesional, la Certificación en Ciberseguridad de Google (2023) ha permitido a miles de personas adquirir conocimientos en seguridad digital, análisis de riesgos y respuesta a incidentes, con un enfoque accesible y adaptado a los desafíos actuales. Este tipo de certificaciones está facilitando la incorporación de nuevos profesionales en el sector de la ciberseguridad, ayudando a cerrar la brecha de talento en un campo que demanda cada vez más especialistas.

Además de la formación teórica, las simulaciones de ciberataques en empresas se han convertido en una herramienta clave para entrenar a equipos de seguridad en la identificación y mitigación de amenazas en tiempo real. A través de la implementación de red-teaming, las organizaciones pueden evaluar la efectividad de sus protocolos de seguridad mediante ataques simulados, mejorando la capacidad de respuesta de sus equipos frente a situaciones de riesgo real. Estudios recientes han demostrado que estas prácticas reducen el tiempo de detección de amenazas en un 40% y mejoran la resiliencia de los sistemas ante ataques avanzados (Harvard Business Review on Cybersecurity, 2024).

La inversión en educación y concienciación en ciberseguridad no solo protege a empresas y gobiernos de ciberataques, sino que también empodera a los ciudadanos para proteger su información personal y evitar caer en fraudes digitales. A medida que el panorama de amenazas sigue evolucionando, la capacitación continua y la actualización de conocimientos se convierten en la mejor defensa contra el cibercrimen y la manipulación digital. La ciberseguridad ya no es solo una responsabilidad de los profesionales del sector, sino una competencia esencial para toda la sociedad en la era digital.

HALLAZGOS CLAVE DEL ESTUDIO

La evolución tecnológica ha generado un cambio estructural en la naturaleza del crimen, otorgando a los delincuentes acceso a herramientas avanzadas como la inteligencia artificial, el Internet de las Cosas y la automatización, lo que ha perfeccionado sus tácticas y aumentado su capacidad de evasión. La convergencia de estas tecnologías ha permitido la diversificación de delitos digitales, la sofisticación de ataques cibernéticos y la consolidación de redes criminales con un grado de anonimato sin precedentes.

Uno de los hallazgos más significativos de este estudio es que la IA ha facilitado la automatización del crimen digital, proporcionando a los delincuentes nuevas formas de perpetrar fraudes financieros, realizar ciberataques avanzados y manipular la información con fines maliciosos.

Los algoritmos de machine learning han sido utilizados para mejorar la precisión y eficiencia de los ataques, permitiendo la evasión de sistemas de detección de amenazas y generando una ventaja significativa sobre los mecanismos tradicionales de ciberseguridad.

El ransomware basado en IA ha demostrado ser particularmente devastador, ya que optimiza el cifrado de datos, personaliza las demandas de rescate en función de la capacidad financiera de las víctimas y automatiza la negociación con los afectados a través de chatbots inteligentes.

La aparición de los deepfakes ha revolucionado la suplantación de identidad, permitiendo la clonación de voces y rostros con una fidelidad alarmante, facilitando fraudes financieros, manipulación de pruebas judiciales y campañas de desinformación a gran escala.

Otro aspecto clave del estudio es que el Internet de las Cosas ha ampliado la superficie de ataque del crimen cibernético, exponiendo infraestructuras críticas, redes industriales y dispositivos personales a nuevos tipos de amenazas. La proliferación masiva de dispositivos IoT sin protocolos de seguridad adecuados ha permitido la creación de botnets avanzadas utilizadas para lanzar ataques de denegación de servicio (DDoS), los cuales han comprometido la estabilidad de servidores gubernamentales, empresas de tecnología y operadores de infraestructuras esenciales.

El uso de IoT por parte del crimen organizado ha demostrado ser una tendencia creciente, facilitando el espionaje, el monitoreo de operativos policiales y la optimización de rutas de tráfico ilícito mediante rastreadores GPS y sensores inteligentes. Asimismo, la explotación de vulnerabilidades en dispositivos IoT ha sido documentada en ataques dirigidos a redes eléctricas, hospitales y sistemas de transporte, lo que evidencia su potencial para el sabotaje de infraestructuras críticas y la disrupción de servicios esenciales.

El estudio también revela que el crimen organizado ha integrado tecnologías emergentes para mejorar la eficiencia de sus operaciones y minimizar el riesgo de detección. La IA ha sido utilizada en la planificación y ejecución de delitos, permitiendo a los carteles de narcotráfico emplear drones autónomos para el transporte de drogas, optimizar sus estrategias de lavado de dinero a través de blockchain y criptomonedas, y diseñar ataques cibernéticos con precisión milimétrica.

El Crime-as-a-Service (CaaS) ha experimentado un auge significativo, con redes criminales vendiendo herramientas avanzadas de hacking y ofreciendo ataques de ransomware como un modelo de negocio rentable y accesible para actores sin conocimientos técnicos avanzados.

A nivel regulatorio, el estudio evidencia que los marcos normativos actuales son insuficientes para hacer frente a la ciberdelincuencia, ya que la falta de una legislación global uniforme permite que los delincuentes operen desde jurisdicciones con regulaciones laxas o sin tratados de extradición. Si bien existen iniciativas como el Convenio de Budapest sobre Ciberdelincuencia, la falta de adhesión de algunos países limita su efectividad y dificulta la persecución internacional de los ciberdelincuentes. En cuanto a la regulación de la inteligencia artificial y la ciberseguridad, la mayoría de las políticas gubernamentales han sido reactivas en lugar de preventivas, lo que permite que los delincuentes se mantengan un paso adelante en la explotación de nuevas vulnerabilidades.

Otro hallazgo clave es el papel crítico de la cooperación internacional y la educación en ciberseguridad como estrategias para mitigar el crimen digital. La implementación de plataformas de intercambio de inteligencia en tiempo real entre gobiernos, empresas de ciberseguridad y organismos multilaterales ha demostrado ser una estrategia efectiva para mejorar la detección y respuesta ante amenazas emergentes. Sin embargo, la falta de estandarización en las regulaciones de privacidad y ciberseguridad sigue siendo una barrera significativa.

Por otro lado, la educación y formación en ciberseguridad ha sido identificada como una herramienta fundamental para reducir la incidencia de ataques de ingeniería social, phishing y manipulación digital. La concienciación sobre buenas prácticas de seguridad digital, la capacitación de profesionales en ciberseguridad y la implementación de simulaciones de ciberataques en empresas y entidades gubernamentales han demostrado ser estrategias efectivas para fortalecer la resiliencia digital y minimizar los riesgos asociados al factor humano.

Los hallazgos de este estudio ponen de manifiesto que la inteligencia artificial, el Internet de las Cosas y la automatización han revolucionado tanto el crimen digital como las estrategias de mitigación y defensa.

A medida que la tecnología avanza, los actores criminales seguirán explotando sus capacidades para desarrollar métodos de ataque más sofisticados y difíciles de rastrear. Esto exige una respuesta coordinada entre gobiernos, organismos de seguridad y el sector privado, la adopción de regulaciones más estrictas sobre IA e IoT, y una inversión sostenida en educación en ciberseguridad y desarrollo de tecnologías defensivas avanzadas.

El futuro de la seguridad digital dependerá de la capacidad de las sociedades para adaptarse y anticiparse a los desafíos emergentes del crimen tecnológico, asegurando que la tecnología siga siendo una herramienta para el progreso y la protección, y no un arma en manos de actores malintencionados.

RECOMENDACIONES

Para mitigar los riesgos emergentes asociados con la transformación digital del crimen, es fundamental adoptar un enfoque integral que combine avances tecnológicos, regulación efectiva, cooperación internacional y educación en ciberseguridad. La rápida evolución de las herramientas digitales ha permitido a los delincuentes explotar vulnerabilidades en inteligencia artificial, el Internet de las Cosas y la automatización, lo que requiere estrategias innovadoras y multidisciplinarias para contrarrestar sus efectos.

Uno de los aspectos más urgentes es el desarrollo de inteligencia artificial aplicada a la detección y prevención de ciberdelitos, lo que permitiría fortalecer la identificación de fraudes financieros en tiempo real y mejorar la capacidad de respuesta ante ataques de suplantación de identidad y deepfakes.

La implementación de sistemas de machine learning podría contribuir significativamente a la predicción de ataques cibernéticos, optimizando la protección de infraestructuras críticas mediante el análisis de comportamiento y la detección de patrones anómalos.

La adopción de IA defensiva en ciberseguridad facilitaría la automatización de respuestas ante ataques, permitiendo bloquear amenazas antes de que comprometan redes y sistemas esenciales.

Desde una perspectiva regulatoria, es fundamental establecer estándares internacionales obligatorios para la seguridad en dispositivos IoT, incluyendo autenticación multifactor, cifrado avanzado y actualizaciones automáticas de firmware. La falta de normativas homogéneas ha permitido la proliferación de hardware vulnerable en el mercado, exponiendo a empresas y ciudadanos a ataques masivos de denegación de servicio, espionaje y sabotaje de infraestructuras críticas.

Es esencial ampliar la aplicación del Reglamento General de Protección de Datos (GDPR) para garantizar que los dispositivos conectados cumplan con protocolos de seguridad robustos y requisitos de protección de datos en la nube. Paralelamente, se recomienda la creación de mecanismos de supervisión y sanción para las empresas que incumplan estos estándares, asegurando que los fabricantes de tecnología asuman responsabilidad por la seguridad de sus productos.

En el ámbito de cooperación internacional, es imprescindible fomentar la adhesión de más países al Convenio de Budapest sobre Ciberdelincuencia, garantizando que todos los estados miembros cuenten con marcos legales armonizados para la persecución del crimen digital. La falta de regulación uniforme ha permitido que ciberdelincuentes operen desde jurisdicciones con regulaciones laxas o sin tratados de extradición, lo que dificulta su captura y enjuiciamiento.

Para fortalecer la respuesta global ante estos delitos, se recomienda la creación de plataformas de intercambio de inteligencia en tiempo real entre gobiernos, empresas de ciberseguridad y organismos internacionales, lo que permitiría una respuesta más rápida y efectiva ante amenazas emergentes. Además, la consolidación de un Centro Global de Ciberseguridad liderado por la ONU garantizaría la coordinación de esfuerzos en regulación, prevención e intervención de delitos digitales, promoviendo la colaboración entre sectores públicos y privados a nivel mundial.

La educación en ciberseguridad es otro pilar clave para la mitigación de amenazas digitales. La inclusión de formación en ciberseguridad en programas educativos desde la educación secundaria contribuiría a preparar a la población desde una edad temprana, fortaleciendo la resiliencia digital y reduciendo la incidencia de ataques basados en ingeniería social. En el ámbito corporativo y gubernamental, es crucial implementar simulaciones de ciberataques y ejercicios de red-teaming, que entrenen a empleados en la identificación de amenazas y en la respuesta ante incidentes críticos.

Las campañas de concienciación en ciberseguridad dirigidas a la ciudadanía pueden desempeñar un papel esencial en la reducción de ataques de phishing, fraudes en línea y robo de datos personales, fortaleciendo así la cultura de seguridad digital a nivel global.

La lucha contra la criminalidad digital requiere una combinación de tecnologías avanzadas, regulaciones efectivas, cooperación internacional y una educación en ciberseguridad estructurada. La implementación de estas estrategias permitirá anticiparse a las tácticas delictivas emergentes, fortaleciendo la protección de infraestructuras críticas y minimizando los impactos negativos del crimen digital en la sociedad.

CONCLUSIONES

El avance tecnológico ha redefinido la naturaleza del crimen, proporcionando a los delincuentes herramientas cada vez más sofisticadas para operar en el ámbito digital. La inteligencia artificial, el Internet de las Cosas y la automatización han ampliado exponencialmente el alcance del crimen digital, permitiendo la proliferación de ataques cibernéticos más rápidos, precisos y difíciles de rastrear. Estos avances han generado un desafío sin precedentes para la seguridad global, ya que los modelos tradicionales de prevención y respuesta han quedado obsoletos ante la velocidad con la que evolucionan las amenazas digitales.

A lo largo de este estudio, se ha demostrado que, si bien se han implementado estrategias de mitigación y cooperación internacional, la falta de marcos regulatorios sólidos y la incapacidad de las legislaciones actuales para adaptarse a la rápida evolución del crimen tecnológico representan desafíos significativos para la ciberseguridad. La automatización del crimen mediante IA, la explotación de vulnerabilidades en dispositivos IoT y el uso de criptomonedas y blockchain para el financiamiento de redes criminales han creado un entorno en el que la identificación, rastreo y enjuiciamiento de ciberdelincuentes se ha vuelto más complejo que nunca.

El crimen organizado, por su parte, ha encontrado en la tecnología una herramienta clave para optimizar sus operaciones y mejorar su capacidad de evasión. Desde el uso de drones autónomos para el narcotráfico hasta la implementación de sistemas de inteligencia artificial para predecir operativos policiales y ajustar rutas de contrabando, la digitalización ha permitido que estas organizaciones incrementen su eficiencia y reduzcan su exposición a las fuerzas del orden. Sin una respuesta coordinada y efectiva, estas amenazas continuarán afectando a gobiernos, empresas y ciudadanos, comprometiendo la estabilidad económica y la seguridad global.

El futuro de la seguridad digital dependerá de la capacidad de la sociedad para anticipar, adaptarse y responder a estos desafíos. La clave para un mundo digital más seguro no radica únicamente en la implementación de nuevas tecnologías defensivas, sino en el desarrollo de estrategias de innovación responsable y colaboración efectiva entre gobiernos, empresas y ciudadanos.

Para contener la amenaza del crimen digital en la próxima década, es imperativo que la regulación de la inteligencia artificial y la ciberseguridad evolucionen al mismo ritmo que las amenazas, asegurando que estas herramientas continúen siendo instrumentos de progreso y no armas en manos de actores malintencionados. La cooperación internacional jugará un papel fundamental en la lucha contra el crimen digital. La estandarización de marcos regulatorios, la creación de plataformas de intercambio de inteligencia en tiempo real y la consolidación de tratados multilaterales como el Convenio de Budapest sobre Ciberdelincuencia serán esenciales para reducir la impunidad con la que operan los ciberdelincuentes. La colaboración entre sectores público y privado también será clave para fortalecer la ciberseguridad en infraestructuras críticas y reducir el impacto de los ataques sobre la estabilidad económica y social.

Finalmente, la inversión en educación y concienciación en ciberseguridad será determinante para garantizar una respuesta efectiva ante las amenazas digitales emergentes. La incorporación de programas de alfabetización digital en los sistemas educativos, la formación de profesionales en ciberseguridad y la concienciación de la ciudadanía sobre los riesgos asociados al uso de la tecnología contribuirán a reducir la vulnerabilidad frente a ataques de ingeniería social, phishing y manipulación de información. A medida que las amenazas digitales continúan evolucionando, la única manera de contenerlas será mediante un enfoque multidimensional que combine tecnología, legislación, cooperación internacional y formación continua. La era digital trae consigo oportunidades sin precedentes, pero solo un uso responsable y ético de la tecnología garantizará que su impacto sea positivo para la seguridad y el bienestar global.

REFERENCIAS

Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA). (2024). Annual report on cybersecurity threats and mitigation strategies. U.S. Department of Homeland Security. https://www.cisa.gov

Check Point Research. (2024). Cyber espionage through IoT vulnerabilities: A global threat analysis. Check Point Software Technologies Ltd. https://research.checkpoint.com

Cisco Systems. (2024). Annual cybersecurity threat report. Cisco Security. https://www.cisco.com/cybersecurity

Colado García, S. (2019). Influencia de la tecnología en el desarrollo del pensamiento y conducta humana: Tesis Doctoral. Amazon

Colado García, S. (2021). Multiversos digitales: La tecnología como palanca evolutiva. Universo de las Letras

European Cybersecurity Agency (ENISA). (2024). Cybersecurity challenges in IoT: Policy recommendations for the European Union. European Commission. https://www.enisa.europa.eu

European Journal of Criminology. (2023). The evolution of AI-driven cybercrime: Trends and countermeasures. European Journal of Criminology, 20(3), 145-162. https://journals.sagepub.com/home/euc

European Journal of Emergency Medicine. (2024). Cyberattacks on healthcare: The growing risks of IoT vulnerabilities in medical devices. European Journal of Emergency Medicine, 32(1), 88-101. https://journals.lww.com/ejem

European Journal of Information Security. (2024). Machine learning in cybersecurity: How AI is used to prevent and perpetrate cybercrime. European Journal of Information Security, 29(2), 77-95. https://www.springer.com/journal/ijis

Foro Económico Mundial. (2025). Artificial intelligence and cybersecurity: Balancing risks and rewards. AI Governance Alliance. https://www.weforum.org/reports

Foro Económico Mundial. (2025). The future of cybersecurity: Preparing for AI-driven threats. AI Governance Alliance. https://www.weforum.org

Glickman, M., & Sharot, T. (2024). How human–AI feedback loops alter human perceptual, emotional and social judgments. Nature Human Behaviour, 8(4), 520-536. https://doi.org/10.1038/s41562-024-02077-2

Google DeepMind. (2023). Advancing AI for cybersecurity: Automated threat detection and risk mitigation. Google Research. https://www.deepmind.com

Harvard Business Review. (2024). Cybersecurity leadership: Building resilience against AI-driven threats. Harvard Business Review, 102(1), 44-58. https://hbr.org

Instituto Nacional de Estándares y Tecnología (NIST). (2023). Security framework for IoT devices: Recommendations for manufacturers and policymakers. U.S. Department of Commerce. https://www.nist.gov

INTERPOL. (2020). Report on artificial intelligence for law enforcement: Challenges and opportunities. INTERPOL Cybercrime Directorate. https://www.interpol.int

INTERPOL. (2024). Global cybercrime trends and countermeasures. INTERPOL Cybercrime Directorate. https://www.interpol.int
Journal of Cybercrime & AI. (2024). Deepfake detection in financial security: AI-driven solutions and ethical implications.Journal of Cybercrime & AI, 17(3), 211-230. https://www.cybercrimejournal.com

Journal of Cybersecurity. (2024). The future of AI-driven ransomware: Emerging threats and defensive strategies. Journal of Cybersecurity, 19(2), 102-118. https://academic.oup.com/cybersecurity

Journal of Critical Infrastructure Protection. (2024). Threats to energy grids: Cyberattacks and the role of IoT security .Journal of Critical Infrastructure Protection, 27(1), 15-39. https://www.sciencedirect.com/journal/journal-of-critical-infrastructure-protection

Journal of Illicit Networks. (2024). Drug cartels and AI: How organized crime is leveraging IoT for trafficking and logistics. Journal of Illicit Networks, 10(1), 55-72. https://www.illicitnetworks.org

Journal of Organizational Security. (2024). Cyberattack simulations: How red-teaming improves corporate resilience. Journal of Organizational Security, 16(2), 89-106. https://www.springer.com/journal/organizational-security

Li, Y., Wu, B., Huang, Y., & Luan, S. (2024). Developing trustworthy artificial intelligence: Insights from research on human-AI trust. Frontiers in Psychology, 15, 1382693. https://doi.org/10.3389/fpsyg.2024.1382693

MIT AI & Security Journal. (2024). Artificial intelligence in cyber defense: Applications, limitations, and future trends.MIT AI & Security Journal, 12(2), 88-109. https://www.mit.edu/research/cybersecurity

MIT Technology Review. (2023). How AI-powered cybercrime is reshaping global security policies. MIT Technology Review, 130(5), 56-72. https://www.technologyreview.com

Naciones Unidas. (2024). Cybersecurity challenges and global responses: A UN initiative for digital security. United Nations Office on Drugs and Crime. https://www.unodc.org

OCDE. (2021). Recomendación del Consejo sobre Inteligencia Artificial y Ciberseguridad. Organización para la Cooperación y el Desarrollo Económicos. https://www.oecd.org

Symantec Threat Intelligence Report. (2024). Global trends in cybercrime: AI, ransomware, and IoT vulnerabilities. Broadcom Inc. https://www.broadcom.com/company/newsroom

U.S. National Institute of Standards and Technology (NIST). (2023). Cybersecurity guidelines for Internet of Things (IoT) security: A national framework. U.S. Department of Commerce. https://www.nist.gov

Velasco, C., García Periche, J., De Dios, J., Gómez G., & Bueno Benedí, M. (2024). Inteligencia Artificial y crimen organizado. EL PACCTO 2.0. https://www.elpaccto.eu

Wang, Y., & Hu, X. (2023). AI-driven botnets: Evolution, detection, and mitigation strategies. IEEE Transactions on Information Forensics & Security, 18(4), 2025-2042. https://ieeexplore.ieee.org

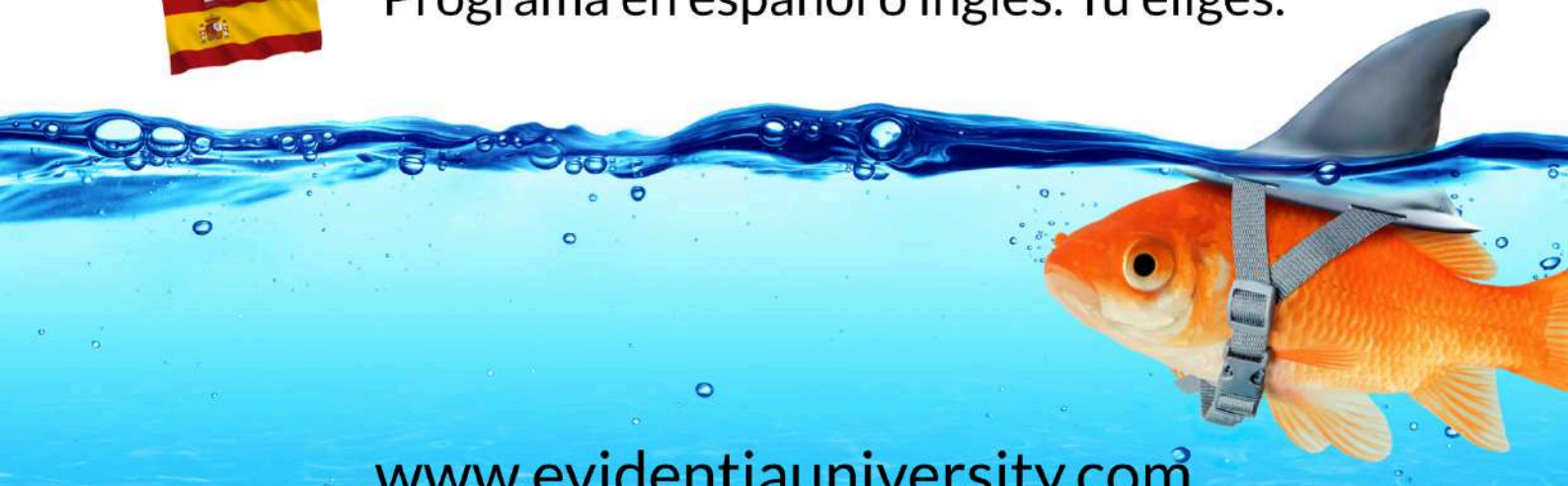
Evidentia University
of Behavioral & Forensic Sciences

Master of Science in Nonverbal & Deceipt Detection

Este máster es el original, el pionero en esta formación. Su objetivo es formar analistas de la conducta no verbal que sean capaces de interpretar el comportamiento humano basándose en la evidencia científica, y aplicarlo a su entorno profesional.

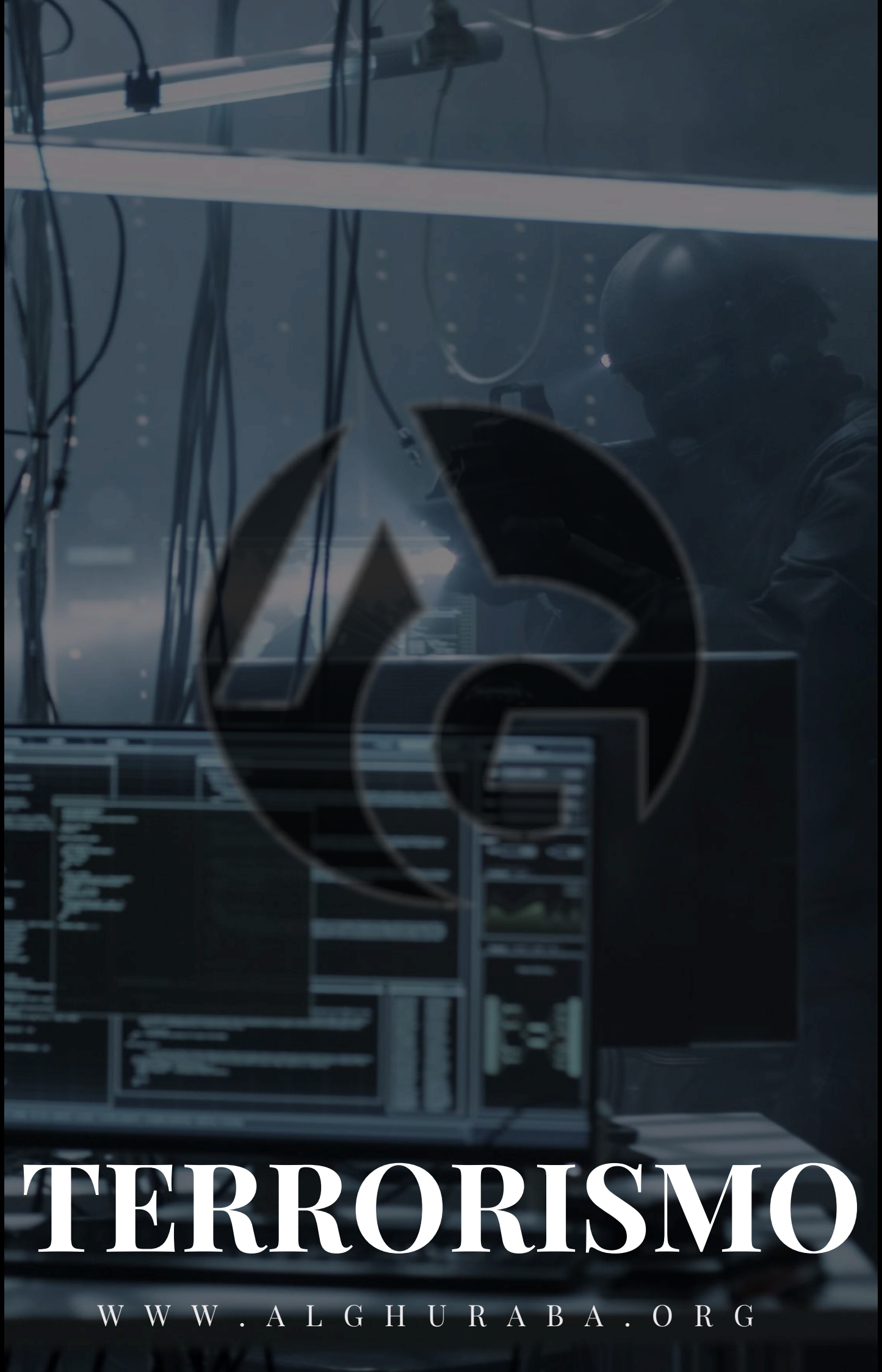
- **100 % Online con clases semanales en vivo.**
- **Metodología de estudio de caso.**
- **Profesorado internaciónal.**

Programa en español o inglés. Tú eliges.



www.evidentiauniversity.com

111 E Monumernt Av. 34741 Kissimmee, Florida. USA



TERRORISMO

WWW.ALGHURABA.ORG

¿QUÉ ES EL TERRORISMO?

UN ANÁLISIS DE SUS MÚLTIPLES INTERPRETACIONES

Francisco Javier Moreno Oliver.
Doctor en Psicología. ORCID iD: https://orcid.org/0000-0002-9306-2125

INTRODUCCIÓN

El terrorismo es un fenómeno complejo que ha sido abordado desde múltiples perspectivas teóricas, cada una de las cuales aporta elementos esenciales para comprender sus causas, manifestaciones e implicaciones sociales.

Este artículo presenta un análisis multidimensional del terrorismo a partir de distintos paradigmas que permiten explicar tanto sus raíces estructurales y funcionales como sus dimensiones simbólicas y comunicativas. Desde el paradigma funcionalista, que concibe el terrorismo como una disfunción del sistema social que altera el equilibrio y la integración, se exploran también las aportaciones del paradigma estructuralista, el cual vincula la violencia política con profundas desigualdades y exclusiones sociales.

Asimismo, el enfoque culturalista enfatiza el simbolismo y la dimensión existencial del terrorismo, mientras que el paradigma funcional-jurídico destaca su carácter instrumental y político como método de comunicación.

Finalmente, se incorporan perspectivas psicosociales sobre la radicalización, así como una visión crítica posmoderna, propuesta por Jean Baudrillard, que otorga un papel simbólico y disruptivo a la acción terrorista en la sociedad contemporánea.

Todo ello se articula dentro de un paradigma multidisciplinar con una visión ecléctica y el de alta o baja intensidad como modalidad. De este modo, el análisis busca ofrecer una comprensión más amplia y profunda del terrorismo en sus múltiples manifestaciones y contextos.

PARADIGMA FUNCIONALISTA

Este paradigma, representado principalmente por Talcott Parsons y Robert K. Merton, aborda el terrorismo desde una perspectiva sociológica que lo vincula con la estabilidad del sistema social y sus posibles disfunciones. Parsons (1951) concibe la sociedad como un sistema conformado por partes interdependientes que trabajan en conjunto para mantener el equilibrio y el orden social. En su modelo, plantea que toda sociedad debe cumplir con cuatro funciones básicas: adaptación, logro de metas, integración y mantenimiento de los patrones culturales. Desde esta visión, el terrorismo se interpreta como una manifestación disfuncional que rompe la integración social y debilita los valores y normas compartidos, afectando de forma negativa la estabilidad general del sistema. Esta disrupción genera un desequilibrio que amenaza la cohesión social y expone las fallas internas del sistema ante determinadas tensiones sociales o políticas.

Por su parte, Merton (1938) amplió el marco funcionalista al diferenciar entre funciones manifiestas y latentes, y al señalar que no todas las estructuras sociales contribuyen de manera positiva al funcionamiento del sistema: algunas pueden, de hecho, ser disfuncionales. En este sentido, el terrorismo se entiende como una forma de disfunción social que surge cuando se producen tensiones derivadas de la frustración entre los objetivos culturales promovidos por la sociedad y los medios legítimos disponibles para alcanzarlos.

Basándose en el concepto de anomia de Durkheim, Merton sostiene que cuando los individuos o grupos no encuentran caminos institucionalizados para lograr sus metas, pueden optar por vías alternativas o desviadas. Entre estas vías se incluyen la violencia política y el terrorismo. Así, el terrorismo puede verse como una forma de "innovación desviada" o incluso de "rebelión", en la que se rechazan los medios y fines establecidos, y se los reemplaza por otros que justifican el uso de la violencia con fines políticos o sociales.

En síntesis, desde el enfoque funcionalista, el terrorismo no es solo un acto criminal, sino un fenómeno estrechamente vinculado a tensiones estructurales, desigualdades, falta de integración y crisis de legitimidad. Se trata de una respuesta extrema ante fallos del sistema social que, al no ofrecer canales adecuados de participación o resolución de conflictos, puede conducir a expresiones violentas que buscan, paradójicamente, restablecer un nuevo orden (Parsons, 1951; Merton, 1938).

PARADIGMA ESTRUCTURALISTA

Este constructo, fuertemente vinculado a las corrientes de la nueva izquierda y a los análisis críticos del sistema político, interpreta el terrorismo como un fenómeno resultado de profundas disfunciones estructurales en las sociedades contemporáneas. Según esta perspectiva, las desigualdades sociales, económicas y políticas, así como la exclusión sistemática de ciertos grupos, generan condiciones propicias para la emergencia de la violencia política y el terrorismo.

Eduardo González (2012) destaca que el terrorismo no puede entenderse sin considerar las fallas inherentes al sistema, que marginan y oprimen a sectores sociales específicos, fomentando así la radicalización y la respuesta violenta como formas de resistencia o reivindicación política.

Este enfoque se aleja de visiones que atribuyen el terrorismo únicamente a factores individuales o culturales, situándolo en un marco más amplio de conflicto social estructural y luchas de poder. La violencia terrorista, entonces, es interpretada como un síntoma visible de tensiones y contradicciones acumuladas dentro del orden establecido, lo que implica también un cuestionamiento a la legitimidad y capacidad del sistema político para ofrecer soluciones inclusivas y pacíficas. De esta manera, el paradigma estructuralista contribuye a explicar el terrorismo como un fenómeno interrelacionado con dinámicas de dominación, explotación y desigualdad que atraviesan las sociedades, enfatizando la necesidad de abordar las causas raíz para comprender su persistencia y manifestación (González, E.,2012).

PARADIGMA CULTURALISTA

Roger Griffin analiza el terrorismo desde una perspectiva culturalista que pone énfasis en su dimensión simbólica, existencial y utópica, vinculándolo a respuestas específicas frente a la modernidad y a procesos de radicalización que involucran a "gente corriente" dispuesta a actuar en nombre de causas suprapersonales (Griffin, 2012). Según el autor, el propósito fundamental de la violencia terrorista no radica tanto en el daño físico inmediato, sino en el impacto psicológico y simbólico que produce al desafiar el monopolio estatal de la violencia, generando miedo, inseguridad e inestabilidad en la sociedad. Desde este enfoque, la violencia terrorista se interpreta como un acto metapolítico; es decir, una acción que trasciende el ámbito político convencional para comunicar narrativas sobre el bien y el mal, en el marco de una guerra ideológica y casi cósmica. Los terroristas, en este contexto, se perciben a sí mismos como agentes de renovación o defensores de un orden sagrado, aunque sus motivaciones puedan resultar incomprensibles o irracionales para quienes no comparten su cosmovisión (Griffin, 2012).

Griffin distingue dos grandes tipos de terrorismo: uno de carácter fanático y regresivo, orientado a preservar supuestos órdenes sociales eternos o inmutables; y otro de tipo moderno y utópico, que busca la construcción de una nueva cultura en oposición a la modernidad occidental dominante. No obstante, también reconoce la existencia de formas híbridas que combinan elementos de ambos modelos.

En este sentido, la perspectiva culturalista ofrece una interpretación del terrorismo que va más allá del análisis funcionalista, centrado únicamente en la lógica de medios y fines tácticos. En su lugar, integra dimensiones simbólicas, emocionales y subjetivas, proporcionando claves para comprender por qué personas aparentemente comunes pueden llegar a una radicalización extrema, incluso hasta el punto de sacrificar su vida en nombre de causas colectivas (Griffin, 2012).

PARADIGMA FUNCIONAL-JURÍDICO

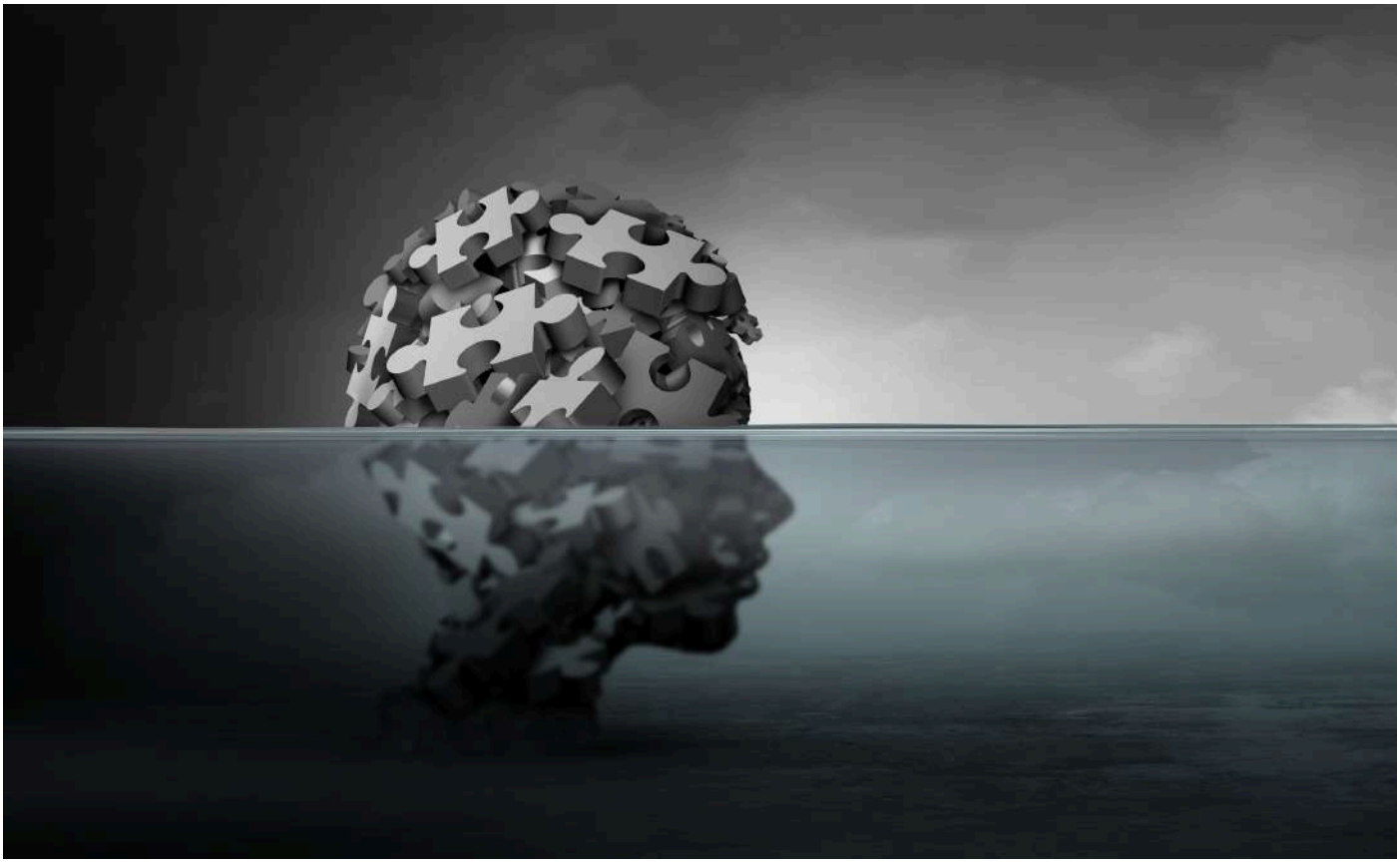
Dentro del enfoque funcional-jurídico, autores como Kai Ambos (2011), desde la perspectiva del derecho penal internacional, así como Cancio Meliá y J. P. Mañalich (2009), sostienen que el terrorismo debe entenderse fundamentalmente como un método o estrategia de comunicación política. Según estos autores, el acto terrorista no se define tanto por la naturaleza del delito

cometido, sino por la intención colectiva y organizacional de generar coacción y transmitir un mensaje político a través del miedo. Es decir, el terrorismo se caracteriza por la instrumentalización del delito con fines de presión y comunicación, orientados a influir en la toma de decisiones políticas o a alterar el orden social establecido (Ambos, 2011; Cancio, M.; Mañalich, J. P., 2009).

A esta visión se suma la crítica de Eduardo González (2012), quien considera que el elemento central para identificar el terrorismo radica en la generación de intimidación colectiva, la cual puede operar incluso sin una finalidad política manifiesta. La amenaza a la seguridad colectiva y la expansión del miedo social constituyen los elementos que otorgan especificidad al fenómeno terrorista, más allá de cualquier motivación ideológica o política (González, E. 2019). De este modo, el paradigma funcional-jurídico enfatiza el carácter instrumental y comunicativo del terrorismo, así como su capacidad de afectar la estructura social mediante la generación de temor y coacción en la población.

PARADIGMA PSICOSOCIAL DE LA RADICALIZACIÓN

El enfoque psicosocial de la radicalización sostiene que el terrorismo surge como resultado de procesos dinámicos en los que intervienen tanto factores sociales como individuales, descartando así la existencia de perfiles psicopatológicos exclusivos. Investigadoras de reconocimiento internacional, como Jessica Stern y Martha Crenshaw, han señalado que la radicalización no puede explicarse únicamente desde patologías individuales, sino que implica interacciones complejas entre la persona y su entorno social, político y cultural (Stern, 2003; Crenshaw, 2011).



En el ámbito hispanohablante, Horgan (2009) coincide en que la radicalización terrorista es un fenómeno multifacético, producto de la interacción entre vulnerabilidades personales y contextos grupales. Advierte, además, sobre la necesidad de evitar reduccionismos que atribuyan el terrorismo a trastornos mentales específicos o a estructuras de personalidad desviadas. Desde esta perspectiva, el énfasis se traslada hacia la comprensión de los procesos de socialización, la influencia de las redes sociales y la construcción de identidades colectivas que favorecen la adopción de ideologías extremistas. Se destaca así la importancia de los factores sociales y culturales por encima de enfoques individualistas o clínicos.

PARADIGMA DE JEAN BAUDRILLARD

Jean Baudrillard, uno de los pensadores más influyentes del posmodernismo, abordó el fenómeno del terrorismo desde una perspectiva profundamente simbólica y crítica. Según él, los atentados terroristas —en particular los del 11 de septiembre de 2001— no solo constituyen un acto violento, sino que representan un contraataque simbólico frente al orden global dominado por Occidente, y especialmente por Estados Unidos.

En su ensayo "El espíritu del terrorismo" (2006), Baudrillard sostiene que los ataques del 11-S fueron una "respuesta simbólica" al poder global del sistema capitalista:

"Es el sistema mismo el que ha producido esta figura terrorista, y el terrorismo es el espejo en el que el sistema se contempla a sí mismo" (Baudrillard, 2006, p. 11).

El autor argumenta que el poder hegemónico global —representado por Estados Unidos— ha impuesto un orden mundial basado en la saturación de imágenes, el control y el simulacro. Ante esta lógica, el terrorismo se presenta como una disrupción: un acto que escapa al control del sistema, devolviendo al mundo una dimensión de lo real que había sido absorbida por el simulacro mediático. Baudrillard no justifica el terrorismo, pero lo interpreta como una forma de desafío simbólico. Desde su perspectiva, el atentado fue un "acto poético" en el sentido provocador del término, que emplea el propio lenguaje del sistema para destruirlo simbólicamente:

"El terrorismo, como forma simbólica, nos recuerda que hay acontecimientos que no pueden ser reducidos al código de lo real televisado" (Baudrillard, 2006, p. 19).

En este sentido, la teoría de Baudrillard resulta controvertida, pero ofrece una crítica profunda sobre la manera en que el poder moderno y los medios de comunicación enmarcan la violencia, el conflicto y la realidad misma.

PARADIGMA MULTIDISCIPLINAR

La óptica jurídica define el terrorismo principalmente a partir de la pertenencia a una organización, el tipo de delitos cometidos y la finalidad política o intimidatoria de los actos. En diversas legislaciones penales se enfatizan el elemento organizativo y la intención política como factores esenciales. Además, se distingue entre el terrorismo individual y el perpetrado por organizaciones, resaltando la intención de desestabilizar el orden social o político (Jakobs, G., 2009). De este modo, el terrorismo

se describe legalmente como una serie de actos de violencia organizados que buscan infundir terror en la población o coaccionar a las autoridades para alcanzar fines políticos, económicos o sociales (Presburger, E., 2025). Desde el modelo sociológico, el terrorismo se interpreta como una reacción social ante la pérdida de consenso o el fracaso de los mecanismos de legitimación política. Se concibe como una forma de violencia ilegítima, dirigida principalmente contra civiles e inocentes, que transgrede las normas establecidas con el objetivo de reconfigurar el orden social o político (Conti, U., 2016). Asimismo, desde la perspectiva de los movimientos sociales, el terrorismo se examina como una variante extrema de estos, destacando su dimensión colectiva y la lógica interna que lo convierte en un instrumento de contestación política (de la Calle, L.; Sánchez-Cuenca, I., 2024).

El constructo psicopatológico de la conducta terrorista plantea que el acto terrorista se origina en una alteración neuropsicológica o en un trastorno mental, en interacción con otras variables psicosociales. (Pretus et al., 2018; Martín, J.,2006). Además, desde la psicología, el terrorismo se comprende como un fenómeno de "normalidad psicológica", donde no existe un perfil único del terrorista, sino una multiplicidad de factores motivacionales e identitarios que convergen en el proceso de radicalización (Pearse, J., 2015). Los paradigmas centrados en la radicalización y la motivación se enfocan en los procesos mediante los cuales individuos y grupos adoptan ideologías extremas y justifican la violencia. En particular, destacan modelos como el de las ”3N”, que plantea que la búsqueda de significado, las narrativas que legitiman la violencia y las redes grupales son elementos clave para comprender la radicalización violenta (Webber, D.; Kruglanski, A., 2017).

Asimismo, el “modelo de los actores devotos” resalta el papel de los valores sagrados y la fusión de la identidad individual con la grupal. Por su parte, el “enfoque de las dos pirámides” distingue entre creencias radicales y la decisión de actuar violentamente, abordando la diferencia entre el apoyo ideológico al extremismo y la participación en actos terroristas.

Finalmente, el “modelo político y normativo” concibe el terrorismo como una herramienta de lucha política, especialmente en contextos donde actores no estatales carecen de acceso al poder o a estructuras institucionales. Este enfoque subraya que la definición de terrorismo depende del punto de vista del actor estatal, lo que genera tensiones entre lo que se considera resistencia legítima y violencia terrorista (Conti, U., 2016).

PARADIGMA DEL TERRORISMO DE ALTA O BAJA INTENSIDAD

Este paradigma distingue dos formas de manifestación terrorista según la escala, los objetivos y los métodos empleados. El terrorismo de baja intensidad se caracteriza por ataques focalizados, con un nivel de violencia limitado y objetivos políticos, ideológicos o territoriales específicos. Este tipo de terrorismo se desarrolla principalmente en contextos nacionales o regionales, empleando recursos reducidos y, por lo general, vinculado a grupos clandestinos que buscan influir en las estructuras de poder local mediante acciones controladas y de menor impacto (Sharp, G., 2015; Fernández, J., 2009).

En cambio, el terrorismo de alta intensidad representa un modelo más reciente y de mayor alcance, caracterizado por ataques masivos y violentos que trascienden las fronteras nacionales y buscan generar impactos globales significativos. Este enfoque cobró especial relevancia tras los atentados del 11 de septiembre de 2001, un punto de inflexión en el que el terrorismo adquirió una dimensión planetaria y una capacidad destructiva sin precedentes. Sus objetivos van más allá de las reivindicaciones territoriales tradicionales y adoptan con frecuencia matices totalitarios o pseudo-religiosos (Alonso-Fernández, F., 2002).

En este sentido, el terrorismo de alta intensidad implica una "violencia ilimitada" orientada a alterar la distribución global del poder, lo que introduce nuevas complejidades en la lucha antiterrorista. La distinción entre ambos modelos permite comprender la evolución histórica del fenómeno y las diferentes estrategias necesarias para su análisis y enfrentamiento. Asimismo, resalta la transición de un terrorismo clásico, limitado y focalizado, hacia uno contemporáneo, global y de alta intensidad (Horgan, J., 2009). Esta categorización resulta útil para contextualizar las causas, formas y objetivos que motivan los atentados, así como para diseñar políticas de seguridad ajustadas a las características específicas de cada manifestación terrorista.

CONCLUSIONES

El terrorismo es un fenómeno complejo y multifacético que carece de una definición única y universalmente aceptada, debido a su naturaleza política, social y cultural. A lo largo del análisis, se ha evidenciado que el terrorismo se caracteriza principalmente por el uso deliberado de la violencia —o la amenaza de su uso— con el fin de generar terror psicológico en la población o en objetivos específicos, buscando un impacto político, ideológico o estratégico que trascienda el acto violento en sí.

Este fenómeno puede manifestarse en distintas escalas, desde individuos o grupos no estatales hasta organizaciones transnacionales que intentan influir en estructuras políticas y sociales a nivel global. Es fundamental diferenciar el terrorismo de otras formas de violencia, como los actos de guerra o el terrorismo de Estado. Este último, aunque utiliza tácticas similares, cuenta con respaldo institucional, mientras que el terrorismo clásico suele estar asociado a actores no estatales que intentan modificar el orden político sin legitimidad oficial.

Las definiciones oficiales, como las adoptadas por la ONU o la Unión Europea, destacan la intención de provocar terror y desestabilización, rechazando cualquier justificación política, religiosa o ideológica para tales actos. La ausencia de consenso sobre una definición clara del terrorismo plantea desafíos prácticos, dificultando la creación de marcos legales internacionales coherentes y abriendo la puerta al uso político del término con fines deslegitimadores.

Por ello, es imprescindible abordar el terrorismo desde una perspectiva multidisciplinaria que contemple sus causas sociopolíticas, sus diversas formas de manifestación y su impacto sobre los derechos humanos y la seguridad internacional. Solo así será posible diseñar estrategias más eficaces para su prevención y combate.

REFERENCIAS

Alonso-Fernández, F. (2002). Fanáticos terroristas. Salvat.

Ambos, K. (2011). La parte general del derecho penal internacional. Tirant lo Blanch.

Baudrillard, J. (20026). El espíritu del terrorismo y la guerra. Editorial Trotta.

Cancio, M.; Mañalich, J. P. (2009). Derecho penal internacional: Parte general. Marcial Pons.

REFERENCIAS

Conti, U. (2016). Elementi per una sociologia del terrorismo. Rubbettino.

Crenshaw, M. (2011). Explaining terrorism: Causes, processes, and consequences. Routledge.

de la Calle, L; Sánchez-Cuenca, I. (2024). La naturaleza del terrorismo: Violencia política y clandestinidad. Catarata.

Fernández, J. (2009). El delito del terrorismo de baja intensidad. Análisis del art. 577 Tirant lo Blanch.

González Calleja, E. (2012). Terrorismo y violencia política. Editorial AKAL.

González, E. (2012). El laboratorio del miedo: Una historia general del terrorismo, de los sicarios a Al Qa'ida . Crítica.

Griffin, R (2012) Terrorist's Creed. Fanatical Violence and the Human Need for Meaning, Basingstoke: Palgrave Macmillan.

Horgan, J. (2009). Psicología del terrorismo. Gedisa

Jokobs, G. (2009). Terrorismo y Estado de derecho. FisiscalBooks.

Martín, J. (2006). Bioquímica de la agresión. Psicopatología Clínica, Legal y Forense, 5, 43-66.

Merton, R. K. (1938). Social structure and anomie. American Sociological Review, 3(5), 672–682.

Parsons, T. (1951). The social system. Free Press.

Pearse, J. (2015). Investigating Terrorism: Current Political, Legal and Psychological Issues. Wiley-Blackwell.

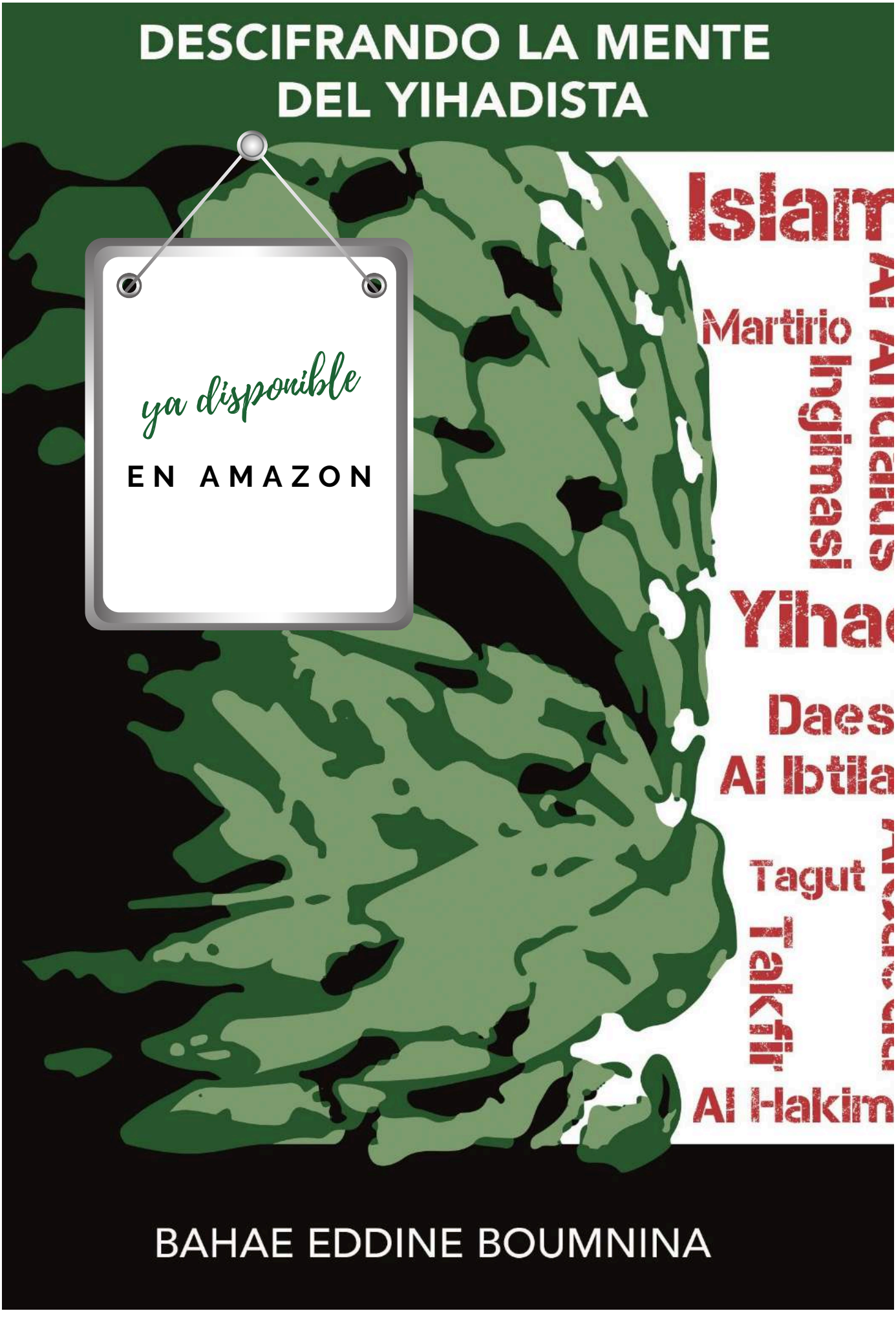
Pretus, C., Hamid, N., Sheikh, H., Ginges, J., Tobeña, A., Davis, R., Vilarroya, O., & Atran, S. (2018). Neural and behavioral correlates of sacred values and vulnerability to violent extremism. Frontiers in Psychology, 9, 24-62.

Sharp, G. (2015). De la dictadura a la democracia. Boston-USA.

Stern, J. (2003). Terror in the name of God: Why religious militants kill. Ecco.

Webber, D.; Kruglanski., A. (2017). "Factores psicológicos en la radicalización: Un enfoque de las "3N"". En el Manual de Criminología del Terrorismo, eds. Gary LaFree y Joshua Freilich. West Sussex: Wiley Blackwell, pp. 33-46.

DESCIFRANDO LA MENTE DEL YIHADISTA



ya disponible

EN AMAZON

BAHAE EDDINE BOUMNINA

ENTREVISTA

WWW.ALGHURABA.ORG

DR. JOSÉ MIGUEL ROMERO PARRA

DOCTOR EN DERECHO Y CIENCIAS SOCIALES

José Miguel Romero es Doctor en Derecho y Ciencias Sociales; Máster Universitario en Seguridad, Salud en el Trabajo y Prevención de Riesgos Laborales; Licenciado en Criminología y Graduado en Derecho.

Colabora como docente en diferentes estudios universitarios en las universidades de UDIMA y VIU compaginándolo con su labor como miembro de las FCSE.

Desde hace años viene realizando investigaciones en el ámbito del crimen y delincuencia organizada, bandas juveniles y tipologías criminales. Fruto de sus investigaciones tiene diferentes publicaciones entre las que podemos destacar su libro “Los grupos juveniles violentos de origen latino y su consideración jurídica en España”.

En primer lugar, queremos agradecer que haya querido participar en esta entrevista, la cual nos parece de gran relevancia observando el panorama delincuencial actual.

1.José Miguel, ¿cómo llegó a interesarse por el fenómeno de los grupos juveniles violentos?

En el año 2010 más o menos tomé contacto por mi actividad profesional con este fenómeno, comencé a interesarme por esta temática y ya en el año 2012 cuando finalicé mis estudios del grado de derecho, realicé el primer análisis jurídico de este fenómenos delincuencial, continuando desde entonces mis investigaciones hasta el año 2022 donde finalice mi tesis doctoral basada en dicho fenómeno.

2.¿Cuál considera que ha sido la evolución más significativa en la dinámica de estos grupos en las últimas décadas?

Son muchos los cambios que han sufrido estas bandas, pero quizás los más importantes serían:

Expansión territorial y diversificación:
Inicialmente, estas bandas juveniles violentas eran fenómenos circunscritos a grandes núcleos urbanos como Madrid o Barcelona. Sin embargo, en los últimos años han experimentado una expansión territorial notable, alcanzando sus tentáculos a ciudades situadas en los extrarradios de las capitales además de una más que reseñable diversificación geográfica significativa hacia territorios como Zaragoza, Valladolid, Toledo, Sevilla, Palma de Mallorca o Valencia entre otras.

Consolidación estructural y jerarquización:
Se ha pasado de bandas juveniles como microestructuras relativamente informales, poco organizadas y con objetivos principalmente relacionados con la protección territorial y conflictos menores, hacia estructuras más jerarquizadas, complejas y organizadas. Las bandas actuales muestran una clara jerarquía interna con líderes claramente definidos, estructura piramidal, disciplina exacerbada y fuertes normas de funcionamiento.

Incremento en la violencia y sofisticación criminal:
Se observa un aumento en la gravedad de los delitos cometidos. Los enfrentamientos han pasado de peleas callejeras a delitos graves como homicidios, tráfico de drogas, tráfico de armas, delitos de ocupación etc. La disponibilidad y uso de armas de fuego y blancas es también una problemática sobre la que fijar el foco por su amplia utilización por estas bandas.

Impacto de las redes sociales y nuevas tecnologías:
Las redes sociales y las tecnologías de la información han revolucionado la forma en que estas bandas se comunican, se coordinan y reclutan nuevos miembros. Plataformas digitales como Instagram, TikTok , Telegram, Youtube han incrementado su capacidad de visibilidad, facilitado procesos de reclutamiento y permitido una difusión más rápida y amplia de mensajes violentos y de sus actividades delictivas.

Cambios en los perfiles criminológicos:
Es alarmante el progresivo descenso en la edad de los integrantes que se ha identificado, observando cada vez más adolescentes muy jóvenes involucrados en estos grupos. Asimismo, aunque inicialmente los integrantes tenían perfiles socioculturales similares y vinculados por lo general a su origen latino, en la actualidad se observan perfiles más diversos, incluyendo jóvenes provenientes de clases medias con recursos familiares adecuados y de multitud de nacionalidades.

3.¿Qué elementos permiten diferenciar una pandilla juvenil de una banda criminal organizada, si es que hay diferencias?

En la actualidad son conceptos que no deben ser confundidos, el fenómeno criminológico de las bandas juveniles ha existido desde hace muchos años sin ser considerados estructuras criminales, pero en la actualidad y más concretamente las de "origen o referencia latina" cumplen perfectamente con los requisitos típicos establecidos en nuestro Código Penal, configurándose como organizaciones criminales del artículos 570 bis principalmente, hecho este confirmado reiteradamente por la jurisprudencia del Tribunal Supremo.

4.Nos puede indicar qué factores influyen principalmente en la incorporación de jóvenes a estos grupos.

Sería muy complicado en la actualidad sintetizar su pregunta en varios factores como ocurría cuando aparecido el fenómeno en nuestro país, pero si es cierto que los factores que refiero a continuación pueden ser preponderantes a la hora de iniciar su contacto con estas bandas juveniles violentas.

-Factores psicológicos individuales (baja autoestima, necesidad de validación y reconocimiento externo…)
-Factores identitarios y culturales (necesidad de sentirse parte de un grupo que proporcione protección, pertenencia…)
-Factores de status social (Desean parecerse a ellos y tener lo que ellos muestran)
-Factores educativos y sociales (abandono escolar, fracaso escolar…)
-Factores familiares como el escaso control parental o violencia intrafamiliar…
-El deseo de participar en sus vídeos musicales (el denominado sueño musical).

5.En cuanto a los perfiles criminológicos, ¿existen perfiles comunes dentro de los líderes de estos grupos y de sus miembros?

Generalmente los líderes presentan personalidades dominantes, capaces de ejercer influencia y control sobre otros miembros, mostrando carisma y autoridad. Además una característica muy habitual es la "experiencia criminal previa" ya que suelen tener un amplio historial delictivo y en muchas ocasiones hechos de extrema gravedad, lo que les proporciona ese reconocimiento y autoridad ante los demás integrantes.

6.Bajo su amplio conocimiento del tema, ¿qué rol juegan las redes sociales y las tecnologías de la información en la organización, visibilidad y reclutamiento de estos jóvenes?

Un papel fundamental, ya que facilitan por un lado la organización y comunicación interna a través de grupos/chats cerrados de comunicación en Whatsapp y Telegram por ejemplo, pero además, redes como Tik ToK, Youtube, Snapchat sirven para proyectar y dar publicidad la imagen de fuerza, poder y estatus social de las bandas al igual que sirven como herramienta de captación y reclutamiento de los nuevos integrantes. Además las redes sociales son fuente de radicalización al crear entornos digitales cerrados donde los integrantes se refuerzan mutuamente su creencias y actitudes violentas, legitimando la violencia y el delito como formas aceptadas de vida.

7.Nos puede hablar un poco más del uso de símbolos, códigos o lenguajes propios entre estos jóvenes.

Estos aspectos que refiere en la pregunta junto con otros como la música, los "grafitis" territoriales, los "handsigns" son elementos que ayudan a fortalecer la cohesión interna de la banda y realzar y empoderar la identidad grupal de la propia banda, sirviendo a su vez como desafío hacia el resto de las bandas juveniles violentas consolidando así la posición y status en el entorno social en el que se actúa.

8.**Desde su experiencia, ¿cree que se están llevando a cabo estrategias de prevención adecuadas, en caso afirmativo nos puede poner algún ejemplo?**

Sinceramente y desde mi conocimiento le puedo indicar que se están realizando estrategias de prevención a nivel social en municipios como Madrid, a nivel educativo como los protocolos de prevención de pertenencia a bandas de la Comunidad de Madrid y Aragón e incluso fomentando esa prevención primaria se desarrolla por parte de las Fuerzas y Cuerpos de Seguridad del Estado el Plan Director para la convivencia y mejora escolar en los centros educativos y sus entornos. Además existen trabajos con jóvenes vulnerables y por su puestos hay un trabajo excepcional con jóvenes ya vinculados a estos grupos y que han delinquido por parte de organismos como la Agencia de Reeducación y Reinserción del Menor Infractor de Madrid.

No obstante, creo que es necesario una concienciación mayor sobre esta problemática y una coordinación a nivel nacional para poder ser capaces de dar una respuesta adecuada a este fenómeno tan peligroso.

9.**¿Cómo afectan los conflictos entre bandas a la seguridad pública?**

Estos conflictos afectan gravemente al concepto de seguridad pública por varios motivos, primeramente y más visible por los enfrentamientos con armas en lugares públicos con el consiguiente peligro para los ciudadanos generando esa percepción de inseguridad en la población que ven alterada su vida cotidiana. Además, muchas veces estos incidentes generan una reacción en cadena alimentando esa espiral de violencia difícil de controlar. Por último y no menos importante indicar que los recursos policiales se ven obligados a prestar más atención a estos hechos con patrullas adicionales y unidades especializadas implicadas en estos dispositivos.

10.Sabemos que los centros educativos o la familia pueden jugar un papel crucial en la detección temprana, ¿cómo cree que realmente vienen actuando estos núcleos de control informal en la detección temprana?

Desde hace mucho tiempo, los centros educativos y las familias han venidos actuando como figuras de protección ante una posible vía de captación, pero en la actualidad, creo que el acceso a las redes sociales ha pasado por la derecha a ambas para evitar que puedan servir de estructuras de detección temprana, es necesario concienciar e identificar tanto a las familias como a los centros educativos de lo que supone la integración en una de estas estructuras criminales.

11.¿Considera que las políticas públicas actuales están alineadas con las necesidades reales del fenómeno? ¿Qué cambios propondría?

Creo sinceramente, que se deben reforzar extraordinariamente las políticas preventivas, ya que desde un punto de vista punitivo, se están proporcionando respuestas adecuadas a este fenómeno, pero existe un déficit en políticas públicas de prevención primario y secundaria para tratar de minimizar o limitar los altos % de integración de menores de edad en estas estructuras criminales.

12.¿Cree que puede conseguirse la reintegración de exmiembros de bandas en la sociedad?

Rotundamente sí, existen altos 5 de reintegración de miembros principalmente tras su estancias en centros adscritos por ejemplo al ARRMI en Madrid, donde excelentes profesionales de varios campos trabajan de forma individual para conseguir esa reintegración y resocialización de estos menores que una vez que se integran, se inician en la carrera criminal de una forma u otra.

13.En un mundo globalizado como el que vivimos, cómo considera que ha afectado la globalización y la migración a la configuración de los grupos juveniles violentos.

Sin vincular la migración a las actividades delictivas de estas bandas juveniles violentas, hay que ser conscientes, que esta tipología criminológica de banda juveniles apareció en España a partir del 2000 cuando ,como todos conocemos, hubo un aumentos de la inmigración de origen latinoamericano, pero esas estructuras eran microestructuras de protección social que no se parecen a la mutación que hoy en día tenemos en nuestro país y que se constituyen como auténticas estructuras criminales.

14.En esta línea de la globalización, qué influencia tienen las bandas internacionales en las locales

Un ejemplo de banda trasnacional podría ser las “maras”, donde este mundo de globalización ha servido para que expandan sus actividades a muchos territorios del globo, no obstante, las bandas juveniles violentas “de origen o referencia latino” no tienen a día de hoy ese carácter transnacional, aunque a mi parecer si tienen contacto con las estructuras de otros países como puede ser República dominicana.

15.¿Qué retos emergentes identifica, por ejemplo, en relación con el ciberespacio, el narcotráfico o la radicalización ideológica?

En primer lugar se podría hablar de un “ciber-reclutamiento”, es decir, las redes sociales se han convertido en una plataforma clave para captar nuevos miembros, sobre todo niños que no tienen contacto previo con el mundo digital y que se constituye como un reto el limitar el éxito de esta captación con los medios digitales. Por otro lado, cada vez más bandas juveniles se ven cercanas al mundo del narcotráfico, participando en la distribución a pequeña y mediana escala ya que se constituye como una gran fuente de ingresos. Por último, estas bandas son “incubadoras” de jóvenes radicalizados e identificados con un mundo delincuencial lo que favorece el comienzo de la denominada carrera criminal.

16.Qué mensaje daría a los jóvenes que hoy se sienten atraídos por la pertenencia a estos grupos.

Que busquen alternativas, que estos grupos lo único que pretenden es instrumentalizarles para realizar o favorecer sus acciones delictivas y que todo lo que representan en la actualidad son valores y principios vinculados a actividades delictivas y una vinculación extrema de la violencia. Que confíen en sus familiares o en los recursos de centros educativos ante cualquier tipo de acercamiento y por último que tengan claro que la salida de estos grupos no es tan sencilla una vez se den cuenta de donde se han integrado.

17.Y para finalizar, qué consejo ofrecería a los profesionales de la seguridad, la educación y la intervención social que trabajan con esta población.

Es esencial para todo profesional que intervenga con estos grupos y sus integrantes, la especialización en materia propia de esta temática, pero además se deben ser conscientes de la importancia que tiene el tratar de evitar la integración de los menores en estas bandas y cuanto antes se realice esa actuación mucho más sencillo será evitar la propia integración. Es una labor costosa que necesita de mucha implicación, conocimiento y profesionalización.

Evidentia University
of Behavioral & Forensic Sciences

Master of Science in Criminal Profiling

Profesores del FBI, Policía Nacional Española, Guardia Civil Española, Policía Nacional de Ecuador, Fiscalía de México y los mejores profesores internacionales en la materia.

100% online con clases semanales en vivo.

Tutorización y seguimiento continuo.

Programa en español o inglés. Tú eliges.

www.evidentiauniversity.com

111 E Monument Av. Kissimmee, Florida. USA

CRIMINOLOGÍA

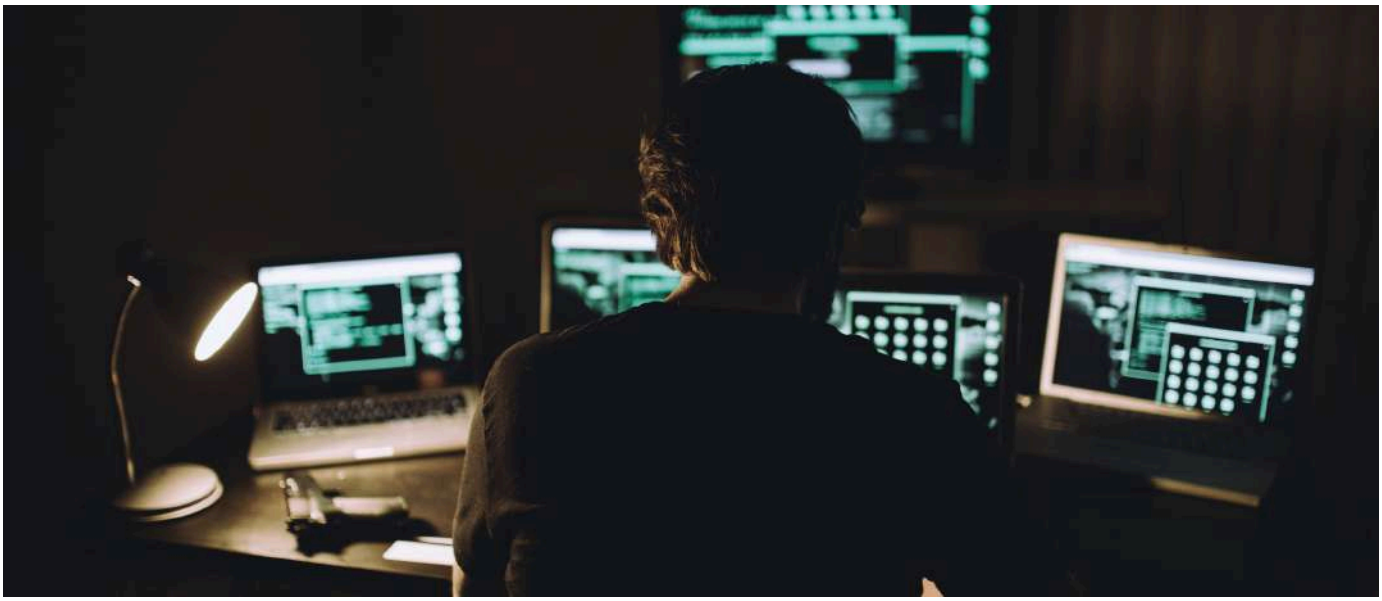
WWW.ALGHURABA.ORG

ORGANIZACIONES CRIMINALES DIGITALES

EVOLUCIÓN, ESTADO DE DESARROLLO E IMPACTO EN AMÉRICA LATINA

Edgardo C. Glavinich.

Director ejecutivo Fundacion Sherman Kent. Delegado CISEG para la República Argentina. Consultor especializado en inteligencia estratégica con experiencia en los sectores público y privado. Docente de posgrado.



INTRODUCCIÓN

El panorama de la seguridad en América Latina ha experimentado transformaciones profundas en la última década, siendo una de las más significativas la emergencia y consolidación de las organizaciones criminales digitales (OCD). Estas entidades representan una evolución cualitativa del crimen organizado tradicional, caracterizada por la integración sistemática de tecnologías digitales en sus estructuras operativas y estrategias de expansión territorial (Lavorgna, 2022). La región latinoamericana ha emergido como un epicentro global para el desarrollo de estas organizaciones, concentrando el 33% de los ataques de ransomware a nivel mundial y procesando transacciones criminales por valor de 40.900 millones de dólares en criptomonedas durante 2024 (Chainalysis, 2025). Esta concentración responde a factores estructurales que incluyen la presencia de organizaciones criminales tradicionales robustas, marcos regulatorios fragmentados y capacidades estatales asimétricas para enfrentar amenazas cibernéticas. El análisis de las OCD en América Latina revela patrones de adaptación que desafían las categorías analíticas tradicionales del crimen organizado. La digitalización ha permitido a estas organizaciones trascender limitaciones geográficas, desarrollar nuevas formas de gobernanza criminal y establecer alianzas transnacionales que erosionan la soberanía estatal de manera sutil pero efectiva (Depetris, 2021).

DEFINICIÓN Y CARACTERÍSTICAS DE LAS ORGANIZACIONES CRIMINALES DIGITALES

Las organizaciones criminales digitales se definen como estructuras criminales complejas que integran tecnologías digitales de manera sistemática en sus operaciones centrales, distinguiéndose de las organizaciones criminales tradicionales que simplemente utilizan herramientas digitales de forma ocasional (Lessing, 2020). Esta definición captura tres dimensiones críticas: la integración tecnológica sistemática, la transformación de los modelos operativos y la emergencia de nuevas formas de gobernanza criminal.

La literatura académica ha identificado tres tipologías principales de OCD. Las organizaciones puramente virtuales que operan exclusivamente en espacios digitales, dedicándose a actividades como el ransomware y el fraude cibernético. Las organizaciones híbridas combinan operaciones físicas y digitales, manteniendo estructuras territoriales mientras incorporan capacidades digitales. Las organizaciones tradicionales digitalizadas que mantienen sus estructuras básicas pero han adoptado tecnologías digitales para modernizar sus operaciones (Lavorgna, 2023).

Transformación del Poder Criminal en el Contexto Digital

La digitalización ha alterado fundamentalmente las dinámicas del poder criminal, creando nuevas formas de autoridad y control que operan tanto en espacios físicos como virtuales. Las OCD desarrollan lo que podemos denominar "soberanía digital criminal", ejerciendo control sobre territorios virtuales y estableciendo normas de comportamiento en mercados ilegales digitales (Skarbek, 2021). La teoría de redes criminales proporciona un marco analítico útil para comprender estas transformaciones. Las OCD operan como redes descentralizadas que pueden reconfigurarse dinámicamente en respuesta a presiones externas, manteniendo la funcionalidad operativa incluso cuando componentes específicos son neutralizados. Esta capacidad representa una evolución cualitativa respecto a las organizaciones jerárquicas tradicionales.

METODOLOGÍA

Este estudio adopta un enfoque de análisis comparativo de casos múltiples, combinando técnicas cuantitativas y cualitativas para examinar la evolución de las OCD en América Latina. La selección de casos se basó en criterios de representatividad regional y disponibilidad de datos verificables. Se analizaron tres casos principales: el Primeiro Comando da Capital (PCC) de Brasil, el Cartel Jalisco Nueva Generación (CJNG) de México y redes criminales transnacionales que operan en el Cono Sur.

Los datos se obtuvieron mediante análisis de fuentes abiertas, incluyendo reportes de investigación periodística, documentos judiciales públicos e informes de organismos internacionales. Los datos secundarios provienen de bases de datos especializadas en criptomonedas y reportes de ciberseguridad. El análisis se estructuró en tres fases temporales: 2020-2021 (emergencia y adaptación), 2022-2023 (consolidación y expansión) y 2024 (maduración y sofisticación).

Evolución y estado de desarrollo de las OCD en América Latina. Fase de Emergencia y Adaptación (2020-2021)

La primera fase de desarrollo coincidió con la pandemia de COVID-19, que aceleró la digitalización de múltiples sectores, incluyendo las actividades criminales. Las organizaciones criminales tradicionales enfrentaron disrupciones significativas en sus operaciones físicas, catalizando procesos de adaptación tecnológica acelerada.

El PCC ejemplifica esta transformación temprana. La organización estableció empresas especializadas en lavado de dinero, procesando 500 millones de reales brasileños a través de canales digitales durante 2020-2021, representando un incremento del 340% respecto al período anterior (Ministerio Público Federal de Brasil, 2021).

Los cárteles mexicanos experimentaron transformaciones similares. El CJNG estableció alianzas con redes chinas de lavado de dinero, procesando entre 15 y 40 millones de dólares mensuales a través de exchanges de criptomonedas. Esta alianza transnacional representa un salto cualitativo en la sofisticación operativa, combinando infraestructura territorial mexicana con expertise tecnológica asiática (DEA, 2021).

Fase de Consolidación y Expansión (2022-2023)

La segunda fase se caracterizó por la consolidación de capacidades digitales y la expansión territorial. Las organizaciones desarrollaron estructuras operativas más complejas y establecieron presencia en múltiples países de la región.

El PCC expandió sus operaciones internacionales, estableciendo células en Argentina, Uruguay, Paraguay y Bolivia. La organización utilizó tecnologías de comunicación encriptada para coordinar operaciones transnacionales, manteniendo un nivel de integración operativa que replica estructuras corporativas multinacionales. El análisis de comunicaciones interceptadas revela protocolos de seguridad digital que incluyen rotación de plataformas cada 48 horas y uso de criptomonedas para transacciones superiores a 10,000 dólares (Insight Crime, 2023).

Los cárteles mexicanos desarrollaron capacidades diferenciadas. El Cartel de Sinaloa se especializó en operaciones de lavado mediante stablecoins, aprovechando la menor volatilidad para facilitar transacciones de gran volumen. El CJNG se focalizó en el desarrollo de infraestructura de ransomware as a service, generando ingresos adicionales mediante la provisión de servicios criminales (NBC News, 2024).

Fase de Maduración y Sofisticación (2024)

La fase actual se caracteriza por la maduración tecnológica y la sofisticación operativa. Las organizaciones han desarrollado capacidades que rivalizan con las de algunos Estados, incluyendo inteligencia artificial para operaciones automatizadas y sistemas de comunicación resistentes a la interceptación.

El caso más emblemático es la acusación israelí contra el PCC por transferir 82 millones de dólares en criptomonedas a organizaciones terroristas. Esta acusación ilustra el nivel de sofisticación alcanzado y la capacidad para operar en mercados globales de servicios criminales (Gazeta do Povo, 2024).

Las métricas confirman esta evolución: América Latina representa el 22% del volumen global de transacciones criminales en criptomonedas, con un crecimiento del 156% respecto al año anterior. Esta cifra refleja no solo el volumen de actividad, sino también la sofisticación de las técnicas empleadas (Chainalysis, 2025).

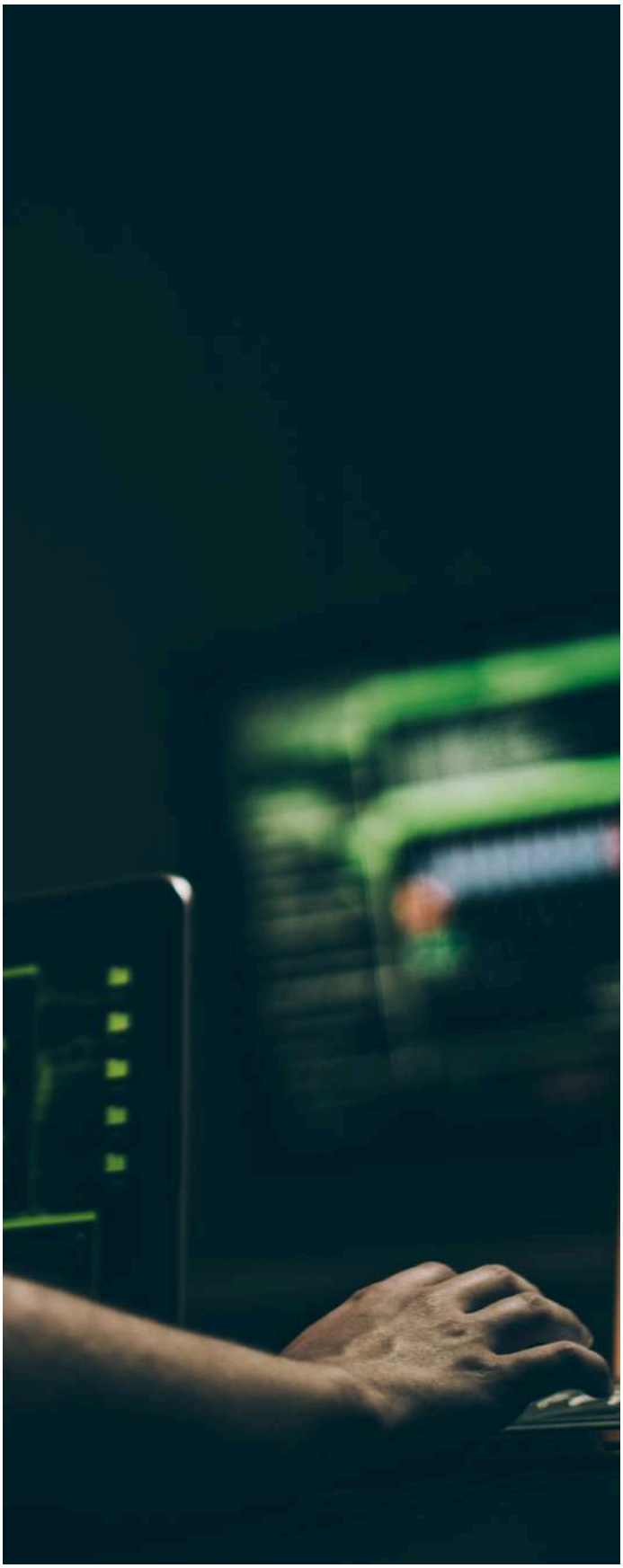
Impacto en la Seguridad Regional. Erosión de la Soberanía Estatal

. as OCD han generado formas novedosas de erosión de la soberanía estatal que operan de manera sutil pero efectiva. A

diferencia de las organizaciones tradicionales que desafían abiertamente la autoridad estatal, las OCD desarrollan espacios de gobernanza paralela que coexisten con las estructuras estatales formales.

En Brasil, el PCC ha establecido un sistema de justicia privada que opera en favelas y prisiones, utilizando aplicaciones de mensajería encriptada para coordinar decisiones judiciales que afectan a miles de personas. Este sistema paralelo procesa disputas comerciales, regula mercados ilegales y administra sanciones, operando como un Estado dentro del Estado (Feltran, 2022).

El impacto trasciende las fronteras nacionales. El análisis de redes criminales transnacionales revela que las OCD han desarrollado capacidades para influir en procesos políticos de múltiples países simultáneamente, utilizando criptomonedas para ocultar el origen de fondos destinados a campañas políticas.



Transformación de las Dinámicas de Violencia

La digitalización ha transformado las dinámicas de violencia criminal, creando nuevas formas de coerción que operan tanto en espacios físicos como virtuales. Las OCD han desarrollado capacidades de "violencia híbrida" que combinan amenazas físicas tradicionales con ataques cibernéticos y chantaje digital. El fenómeno del "narcociberterrorismo" ilustra esta evolución. Los cárteles mexicanos han utilizado ataques DDoS contra infraestructura crítica para presionar a autoridades locales, combinando estos ataques con amenazas físicas para maximizar el impacto psicológico (Americas Quarterly, 2023).

Impacto Económico y Financiero

El impacto económico de las OCD ha alcanzado dimensiones macroeconómicas significativas. Las estimaciones sugieren que las actividades criminales digitales representan entre el 3% y el 5% del PIB regional, con concentraciones particularmente altas en Brasil, México y Colombia.

El lavado de dinero a través de criptomonedas ha creado distorsiones en los mercados financieros regionales. El análisis identificó que el 67% de las transacciones de Bitcoin en América Latina durante 2024 estuvieron vinculadas a actividades ilícitas, comparado con el 23% en América del Norte. Esta concentración ha generado volatilidad artificial y dificultado la adopción legítima de estas tecnologías.

RESPUESTAS ESTATALES Y COOPERACIÓN INTERNACIONAL

Adaptación de las capacidades estatales

Los Estados latinoamericanos han implementado respuestas diferenciadas para enfrentar las OCD. Brasil ha desarrollado un enfoque más integral, estableciendo el Sistema Integrado de Investigación de Criptomonedas (SIIC) que conecta múltiples agencias para el rastreo de transacciones criminales.

El SIIC ha facilitado la desarticulación de 23 organizaciones criminales digitales entre 2022 y 2024, incautando criptomonedas por valor de 1.2 mil millones de reales. Sin embargo, las organizaciones desarticuladas se reconstituyen en promedio en un periodo aproximado de 8 meses, sugiriendo que las respuestas actuales son insuficientes para disrupciones permanentes (Ministerio de Justicia de Brasil, 2024).

México ha adoptado un enfoque centrado en la cooperación internacional, estableciendo unidades especializadas que operan en coordinación con agencias estadounidenses y canadienses. La Fiscalía Especializada en Ciberdelincuencia ha desarrollado capacidades para investigaciones transnacionales que incluyen rastreo de criptomonedas y análisis de comunicaciones encriptadas.

Iniciativas de cooperación regional

La cooperación regional ha emergido como un componente crítico de las respuestas estatales. La Organización de Estados Americanos ha establecido el Programa Hemisférico de Ciberseguridad, que incluye componentes específicos para el combate a las OCD.

El programa ha facilitado la armonización de marcos legales en 18 países de la región, estableciendo definiciones comunes de delitos digitales y procedimientos estandarizados para la cooperación. Sin embargo, la implementación ha sido desigual, con diferencias significativas en las capacidades técnicas entre países.

DESAFÍOS Y LIMITACIONES

Asimetrías tecnológicas y de recursos

Las respuestas estatales enfrentan asimetrías significativas en recursos tecnológicos y capacidades humanas. Las OCD operan con presupuestos que superan los de las agencias estatales especializadas, permitiéndoles contratar talento técnico de alto nivel y acceder a tecnologías de vanguardia.

El PCC destina aproximadamente 200 millones de dólares anuales a tecnología y ciberseguridad, mientras que la Polícia Federal

brasileña asigna 45 millones de dólares a capacidades similares. Esta diferencia se traduce en ventajas operativas tangibles para las organizaciones criminales.

Fragmentación regulatoria y jurídica

La fragmentación de marcos regulatorios representa un desafío estructural. Las OCD explotan inconsistencias en las definiciones legales y diferencias en los procedimientos de investigación para eludir la persecución penal.

El caso de las criptomonedas ilustra esta fragmentación. Mientras algunos países han adoptado marcos regulatorios permisivos, otros han implementado regulaciones restrictivas que pueden limitar las investigaciones transnacionales. Esta heterogeneidad crea espacios de impunidad que las OCD explotan sistemáticamente.

Perspectivas futuras y tendencias emergentes

Integración de inteligencia artificial

La integración de inteligencia artificial representa una tendencia emergente que podría transformar fundamentalmente la naturaleza de las OCD. Las organizaciones más sofisticadas están experimentando con sistemas de IA para automatizar operaciones de lavado de dinero, optimizar rutas de tráfico y personalizar estrategias de corrupción.

Evolución hacia Organizaciones Autónomas Descentralizadas

La tendencia más disruptiva es la evolución hacia Organizaciones Autónomas Descentralizadas Criminales que operan mediante smart contracts. Estas organizaciones podrían funcionar sin liderazgo centralizado, distribuyendo automáticamente ganancias y ejecutando contratos criminales sin intervención humana.

Los primeros prototipos han emergido en mercados de drogas sintéticas, donde smart contracts administran la cadena de suministro desde la producción hasta la distribución. Esta automatización podría hacer que las organizaciones criminales sean virtualmente imposibles de desarticular mediante métodos tradicionales.

CONCLUSIONES

El análisis de las organizaciones criminales digitales en América Latina revela una transformación fundamental en la naturaleza del crimen organizado contemporáneo. Las OCD han evolucionado desde adaptaciones tecnológicas superficiales hasta entidades sofisticadas que rivalizan con las capacidades estatales en múltiples dimensiones.

La evidencia demuestra que las OCD han desarrollado capacidades que trascienden las categorías analíticas tradicionales del crimen organizado. La integración sistemática de tecnologías digitales ha permitido a estas organizaciones trascender limitaciones geográficas, desarrollar nuevas formas de gobernanza criminal y establecer presencia en múltiples países simultáneamente.

El impacto de las OCD en América Latina ha alcanzado dimensiones macroeconómicas y geopolíticas significativas. Los 40.900 millones de dólares procesados en transacciones criminales digitales durante 2024 representan no solo una cifra económica, sino también un indicador de la capacidad de estas organizaciones para influir en mercados financieros y procesos políticos.

Las respuestas estatales han mostrado capacidades de adaptación, pero también limitaciones estructurales significativas. La experiencia brasileña ilustra tanto las posibilidades como las limitaciones de las respuestas tecnológicas, mientras que la reconstitución promedio en 8 meses sugiere que las respuestas actuales son insuficientes para disrupciones permanentes.

La cooperación regional ha emergido como un componente crítico, pero enfrenta desafíos estructurales que limitan su efectividad. Las asimetrías en capacidades técnicas, la fragmentación regulatoria y las limitaciones en los mecanismos de cooperación internacional crean espacios de impunidad que las OCD explotan sistemáticamente.

Las tendencias emergentes sugieren que la sofisticación de las OCD continuará acelerándose, con implicaciones particulares para la integración de inteligencia artificial y la evolución hacia organizaciones autónomas descentralizadas. Estas tendencias representan desafíos cualitativamente diferentes que requerirán enfoques innovadores.

El caso de América Latina demuestra que las OCD no son simplemente una evolución tecnológica del crimen organizado, sino una transformación fundamental que requiere marcos analíticos y respuestas políticas igualmente transformadoras. La región se ha convertido en un laboratorio crítico para comprender estos fenómenos, con implicaciones que trascienden las fronteras regionales.

La evidencia presentada sugiere que el futuro de la seguridad en América Latina dependerá de la capacidad de los Estados para desarrollar respuestas que igualen la sofisticación y agilidad de las OCD. Este desafío requiere inversiones significativas en capacidades tecnológicas, marcos regulatorios adaptativos y mecanismos de cooperación internacional que puedan operar a la velocidad de las amenazas digitales.

REFERENCIAS

Americas Quarterly. (2023). The dramatic cyberattack that put Latin America on alert. *Americas Quarterly*, 17(2), 34-41.

Chainalysis. (2025). *2025 Crypto Crime Report: Regional analysis Latin America*. Chainalysis Research.

Depetris, J. A. (2021). Organizaciones criminales digitales: conocerlas para enfrentar su desafío. *Revista del CLAD Reforma y Democracia*, 79, 117-154.

Drug Enforcement Administration. (2021). *Mexican cartel cryptocurrency operations: Intelligence assessment*. DEA Intelligence Division.

Feltran, G. (2022). *El gobierno que viene: el crimen como política en las periferias de São Paulo*. Siglo XXI Editores.

REFERENCIAS

Gazeta do Povo. (2024, marzo 15). Governo de Israel acusa PCC de usar banco digital e criptomoedas para financiar terrorismo. *Gazeta do Povo*. https://www.gazetadopovo.com.br/

Insight Crime. (2023). *PCC: The evolution of Brazil's largest criminal organization*. InSight Crime Research.

Lavorgna, A. (2022). The digital transformation of organized crime: Conceptual framework and empirical evidence. *European Journal of Criminology*, 19(4), 456-478.

Lavorgna, A. (2023). Digital organized crime spectrum: Theoretical developments and empirical applications. *Trends in Organized Crime*, 26(2), 189-210.

Lessing, B. (2020). Conceptualizing criminal governance. *Perspectives on Politics*, 18(3), 854-873.

Ministerio de Justicia de Brasil. (2024). *Evaluación de efectividad en el combate a organizaciones criminales digitales*. MJ Brasil.

Ministerio Público Federal de Brasil. (2021). *Operação Archimedes: Investigação sobre lavagem de dinheiro digital*. MPF Brasil.

NBC News. (2024, junio 20). Marijuana and Mexican cartels: Inside the stunning rise of Chinese money launderers. *NBC News*. https://www.nbcnews.com/

Skarbek, D. (2021). Governance and social order in criminal organizations. *Annual Review of Law and Social Science*, 17, 357-374.

TRIBUNA DE OPINIÓN

WWW.ALGHURABA.ORG

BANALIZACIÓN

DEL CONCEPTO TERRORISMO

Jordi Escofet.

Delegado de CISEG. Analista terrorismo de etiología yihadista

En la actualidad estamos observando que el uso del lenguaje se ha convertido en un arma y en muchos casos de intento de destrucción y deslegitimación por parte de la política nacional. En este concepto podemos ver como mediante un guion orquestado, denominar al adversario político y social con palabras que anteriormente eran consideradas como forma de escarnio público, ahora se han convertido en una muleta conversacional más, siendo un honor para unos recibirla y un honor para los otros poder etiquetar a un sector social.

En este caso, nos basaremos en el actual uso del concepto y de la palabra “terrorismo” que en las ultimas semanas se está usando mucho para etiquetar cualquier acción que ocurre en nuestra geografía, como por ejemplo: a) terrorismo racial o racista para englobar lo ocurrido en Torre-Pacheco (Murcia), que incluye u total de 63000 resultados en Yahoo; b) Terrorismo patriarcal, con una media de 50000 resultados en Yahoo; c) Terrorismo machista, con una media de 50.000 resultados en buscador Yahoo.

Como podemos observar, y ahora analizaremos cual es la definición aceptada de terrorismo en España, podemos ver como el mal uso de la terminología podría ser una herramienta más de blanquear una lacra social vivida en nuestro país, inicialmente durante la época activa de ETA y llegando a nuestros días con el terrorismo de etiología Yihadista.

Según el CP español, en el artículo 573:

1. Se considerarán delito de terrorismo la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías, cuando se llevaran a cabo con cualquiera de las siguientes finalidades:

1.ª Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

2.ª Alterar gravemente la paz pública.

3.ª Desestabilizar gravemente el funcionamiento de una organización internacional.

4.ª Provocar un estado de terror en la población o en una parte de ella.

2. Se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior.

3. Asimismo, tendrán la consideración de delitos de terrorismo el resto de los delitos tipificados en este Capítulo.

Podemos observar como en la aplicación del artículo 573, los supuestos anteriores de “terrorismo” no tendrían cabida legal para ser denominado de esta manera, por lo cual podemos extraer que se usa como factor de polarización y se sustenta debido a la frugalidad del concepto terrorismo ya que no existe una definición clara en nuestro entorno.

De esta forma, todo el poder global que puede tener una palabra y su alcance, todo el significado transversal queda parcialmente denostado y diluido en una sociedad que no tiene férreas convicciones y que, por suerte, la juventud actual, no ha tenido que convivir con la lacra terrorista de tener que mirar debajo del coche o al cruzar la esquina. Los que antaño señalaban mediante artículos de prensa, y los ejecutores, ejecutaban, nos quieren dar lecciones de lo que es bueno y lo que no. Esos, son los necesarios para que los jóvenes que nunca vivieron eso, mediante la estrategia blanqueante del lenguaje, les estén aupando al poder, aún más si cabe.

Uso Político y Retórico:

·Descalificación de oponentes: Es una de las formas más comunes en nuestra sociedad. Este término se utiliza para estigmatizar y criminalizar a los adversarios políticos, incluso cuando no cumplen con la definición de terrorismo). Esto busca deslegitimar cualquier forma de disidencia o crítica hacia todo lo que molesta las maniobras del poder.

·"Todo es terrorismo": Se aplica a toda una amplia gama de actos violentos o disruptivos que, si bien pueden ser delitos graves, carecen de toda motivación política de generar terror, que pueda ser confundido con los límites del terrorismo.

En definitiva, la banalización del concepto de terrorismo es un fenómeno preocupante que debilita la capacidad de las sociedades para comprender, analizar y responder adecuadamente a esta grave amenaza, al tiempo que puede ser utilizada como una herramienta para la represión política y la polarización.

Ambigüedad y Falta de Consenso en la Definición:

·La ausencia de una definición universalmente aceptada, y en nuestro caso, tanto nacional como europea del concepto de terrorismo facilita su manipulación según intereses particulares de cada Estado. Siendo en muchos de ellos un cajón de sastre para controlar la disidencia.

·Esto permite que las "figuras públicas etiqueten cualquier tipo de acto violento realizado por la oposición ideológica de cualquier tipo de organización" sin discriminación, buscando la deslegitimación de esta y el descrédito del adversario.

El progresismo era hacerse fotos con terroristas patrios. El progresismo era llamar terrorismo a todo lo que no nos gusta. El progresismo era blanquear el relato del terror para darle cabida en tu proyecto político.

Dificultad en la Lucha Efectiva:

·Si no se define claramente qué es terrorismo, no podremos aplicar las estrategias adecuadas para combatirlo, y estas pueden volverse ineficaces, ya que se dispersan recursos en la persecución de actos que no encajan en la verdadera naturaleza del fenómeno.

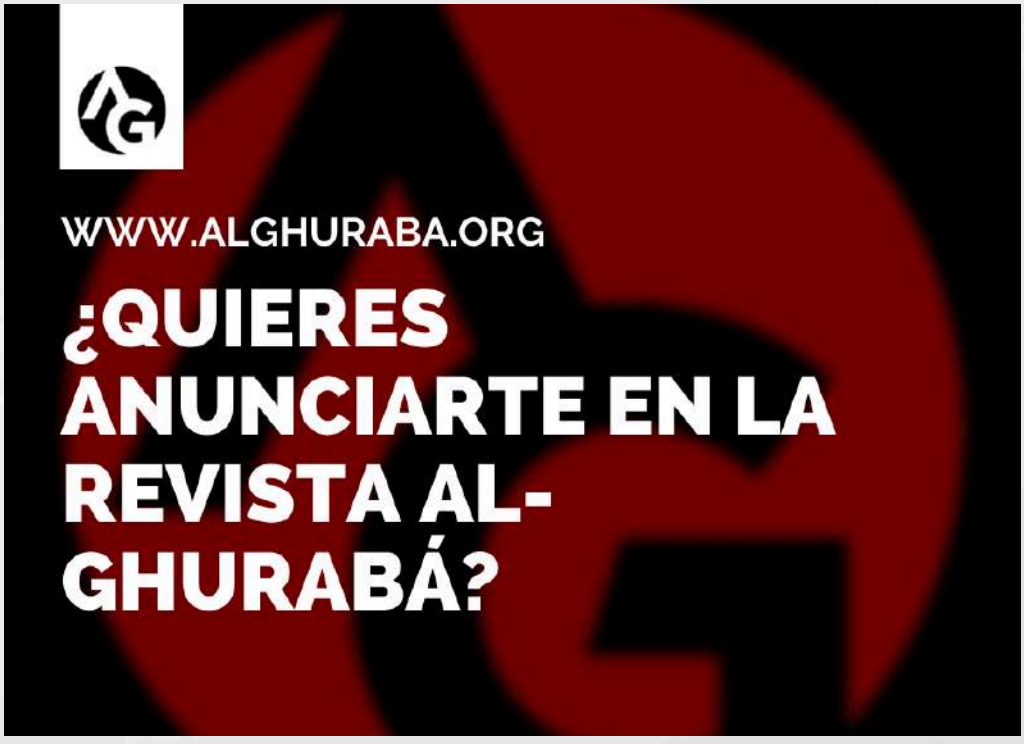
Recuerden que: SI TODO ES TERRORISMO, NADA ES TERRORISMO y si nada es TERRORISMO vuelven a ganar el relato.

REFERENCIAS

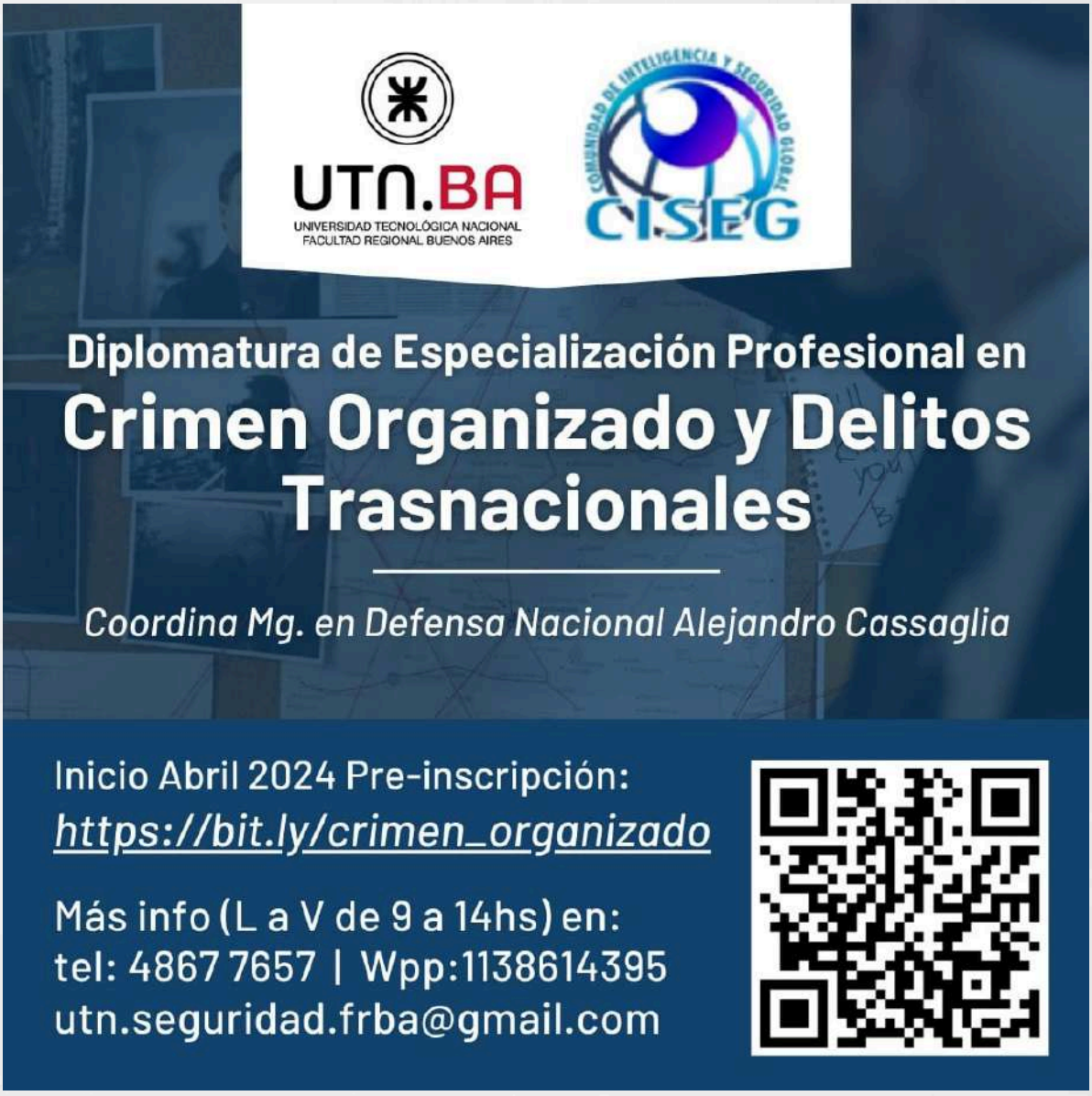
MARTÍNEZ, J., 2025. Terrorismo racista. Display Connectors
SL [en línea]. 17 julio 2025. Disponible en: https://www.publico.es/opinion/columnas/terrorismo-racista.html.

CONCEPTOSJURIDICOS.COM, 2023. Artículo 573 del Código Penal. Conceptos Jurídicos [en línea]. Disponible en: https://www.conceptosjuridicos.com/codigo-penal-articulo-573/.

AGENDA



¿Quieres promocionar tu próximo evento? Contacta con alghuraba@intelciseg.com



DIPLOMATURA DE ESPECIALIZACIÓN PROFESIONAL

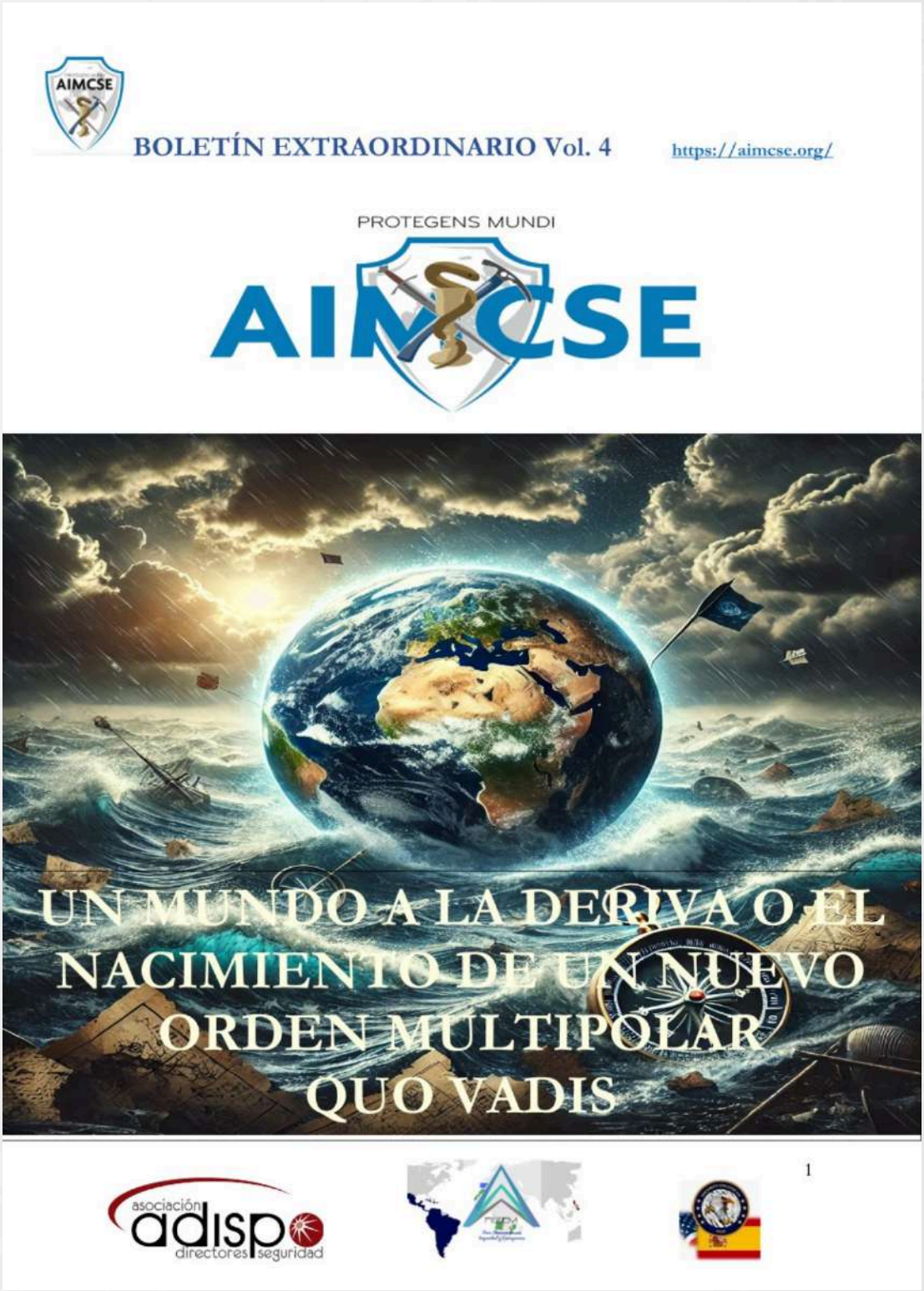
en

CRIMEN ORGANIZADO Y DELITOS TRASNACIONALES

Info: utn.seguridad.frba@gmail.com
LINK: https://bit.ly/crimen_organizado

DIPLOMADO INTERNACIONAL TERRORISMO DE ETIOLOGÍA YIHADISTA

Info: info@intelciseg.com



BOLETÍN PROTEGENS MUNDI

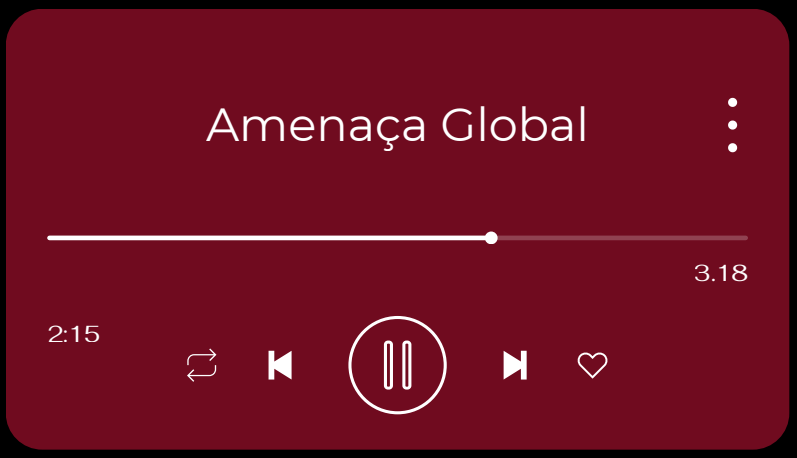
Info: https://aimcse.org

Hemeroteca

Todos los números de
Al-Ghurabá a un golpe de click

AMENAÇA GLOBAL

un programa de Radio 4



¡ESCÚCHANOS!

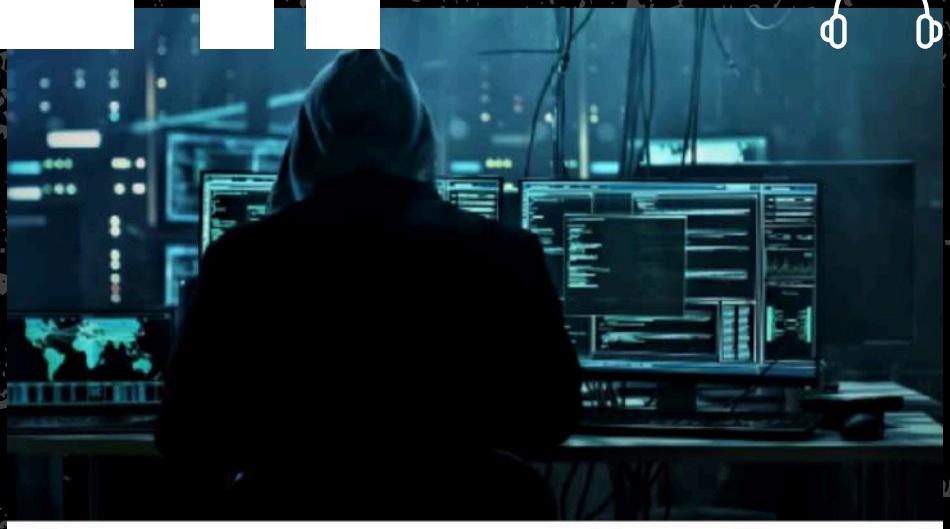
ACCEDE A TODOS LOS PODCAST

AMENAÇA GLOBAL

AMENAÇA GLOBAL

PROGRAMA 1

CRIMINOLOGÍA Y SEGURIDAD



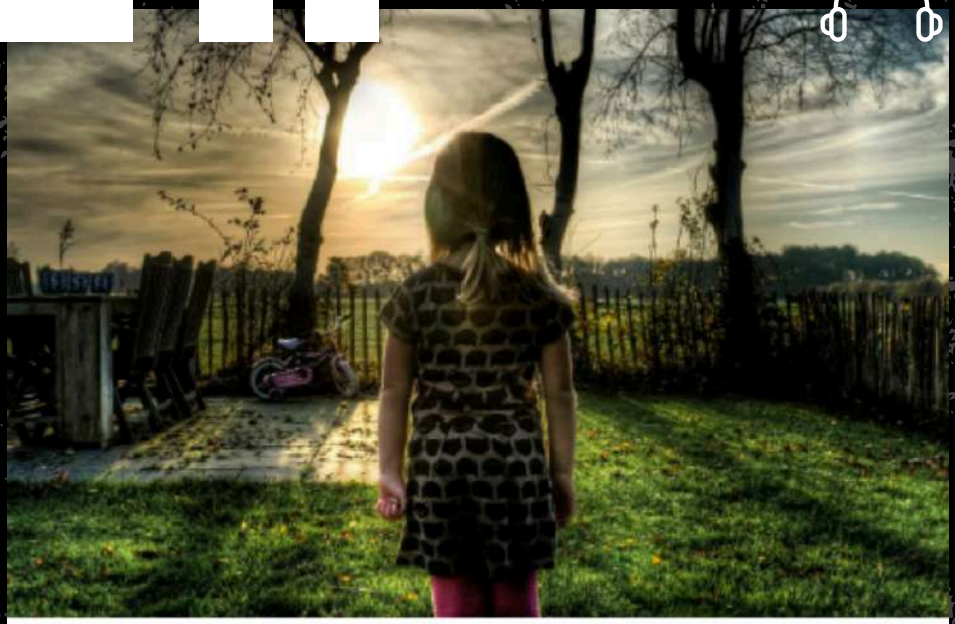
Amenaça Global - Ciberseguretat, amb Vicente Aguilera, ciber-analista

Treballem i estudiem a través del portàtil, tenim oci, serveis, relacions, però: és tan innocent i maco com sembla?

rtve RTVE.es / Feb 11, 2022

PROGRAMA 2

CRIMINOLOGÍA Y SEGURIDAD



Amenaça Global - Segrest de menors, amb Xavier Llaveries, criminòleg i Mosso d'Esquadra

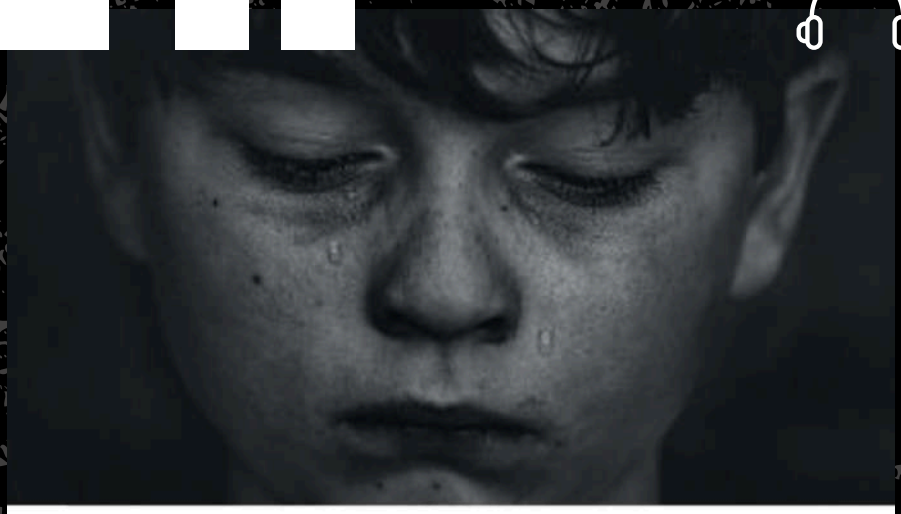
Emisión del programa Amenaça Global titulado Segrest de menors amb Xavier Llaveries, criminòleg i Mosso. Todos los contenidos de RNE los tienes aquí, en RTVE...

rtve RTVE.es / Feb 11, 2022

AMENAÇA GLOBAL

PROGRAMA 3

CRIMINOLOGÍA Y SEGURIDAD



Pornografia infantil

Pornografia Infantil amb Miguel Ángel Soria, doctor en Psicología y profesor de Psicología Jurídica, Criminal y Criminología Avanzada en la Universidad de Barcelona...

rtve RTVE.es / 25 feb

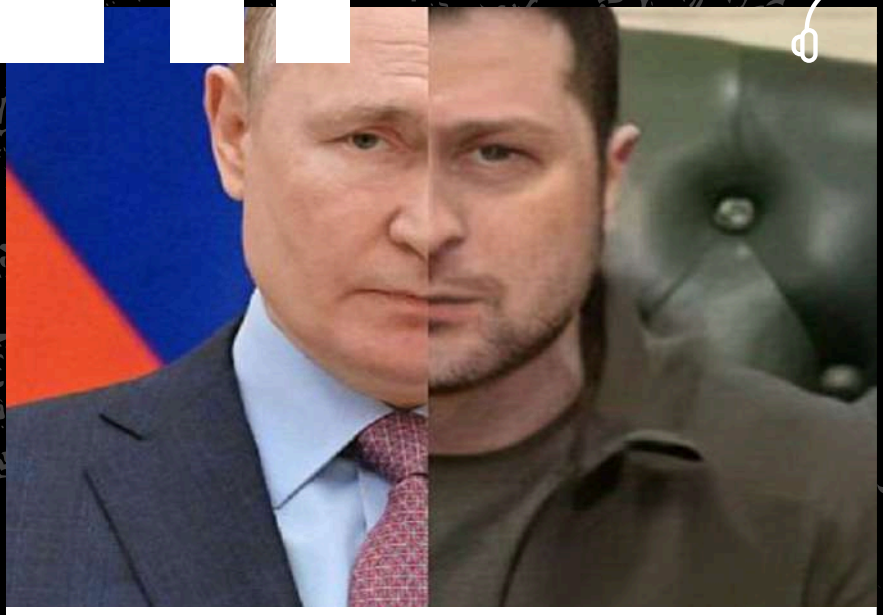
PROGRAMA 4

CRIMINOLOGÍA Y SEGURIDAD

AMENAÇA GLOBAL

PROGRAMA 5

CRIMINOLOGÍA Y SEGURIDAD



Rússia i Ucraïna, un crit, dues trinxeres

Rússia i Ucraïna, un crit, dues trinxeres, amb Jesus M. Pérez, analista de seguretat i defensa. Ha escrit per vàri...

RTVE.es / 5 abr

PROGRAMA 6

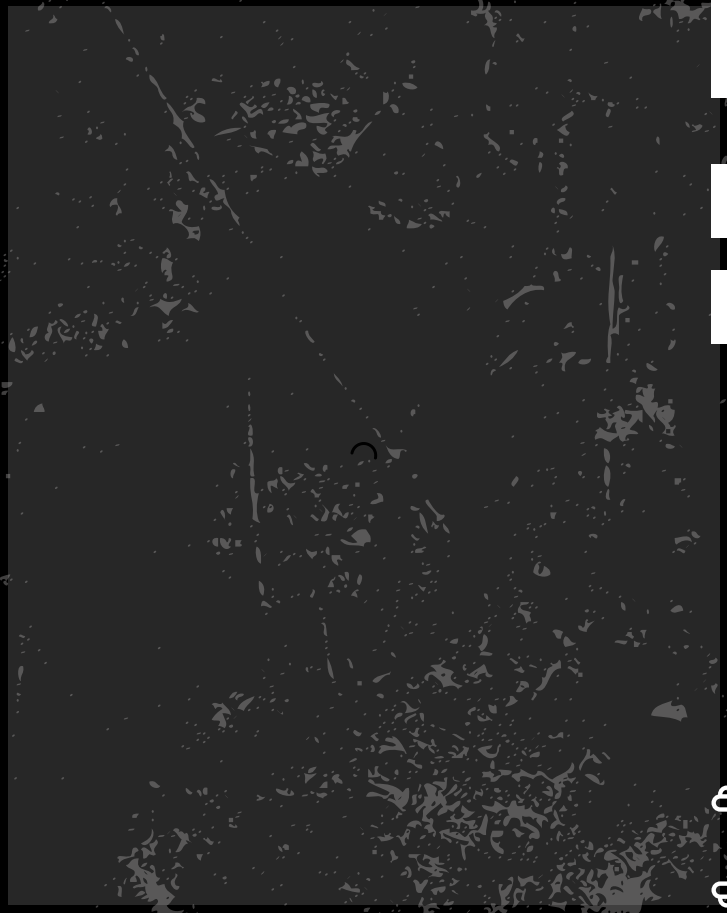
CRIMINOLOGÍA Y SEGURIDAD

Amenaça Global - Homicides: què hi ha darrera de l'homicidi?

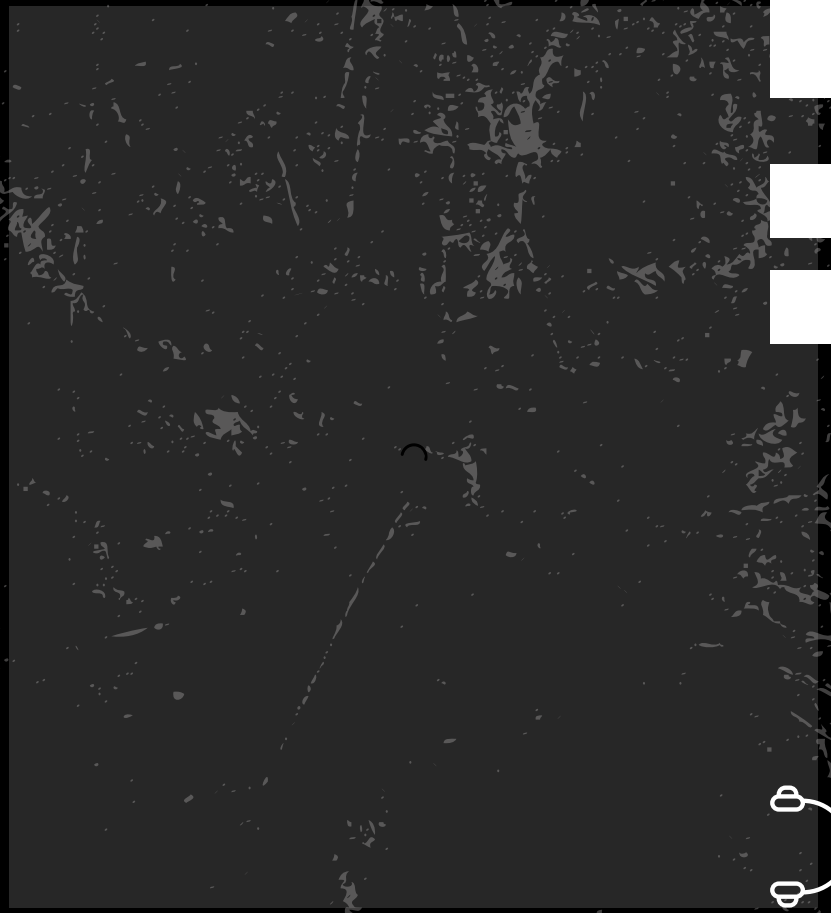
Què sabem sobre les víctimes? Realment tenim assassins serials al nostre país o més aviat són homicidis únics?

AMENAÇA GLOBAL

PROGRAMA 8
CRIMINOLOGÍA Y SEGURIDAD



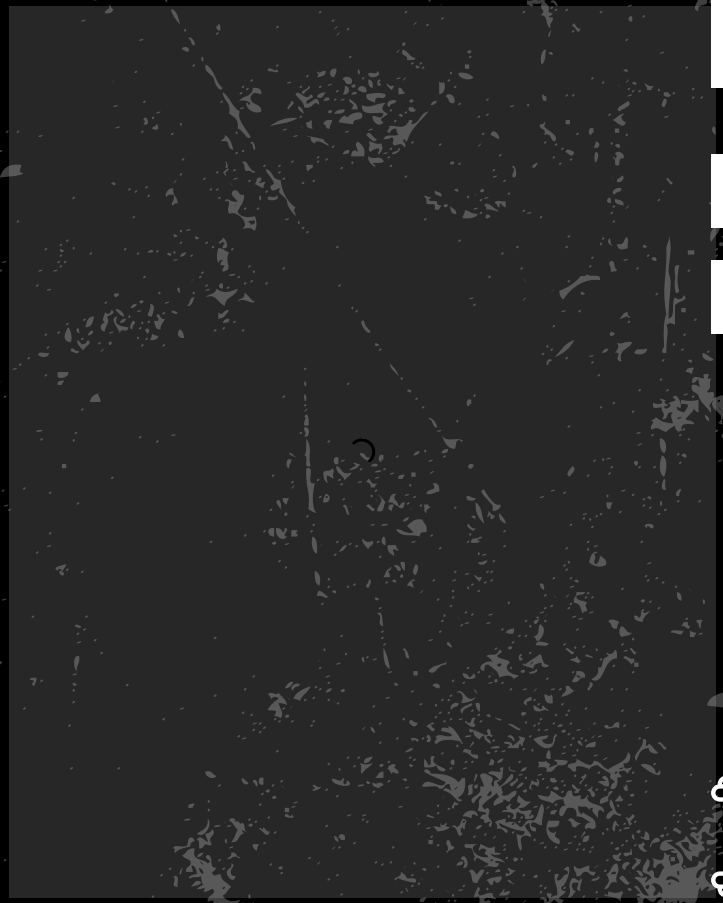
PROGRAMA 7
CRIMINOLOGÍA Y SEGURIDAD



AMENAÇA GLOBAL

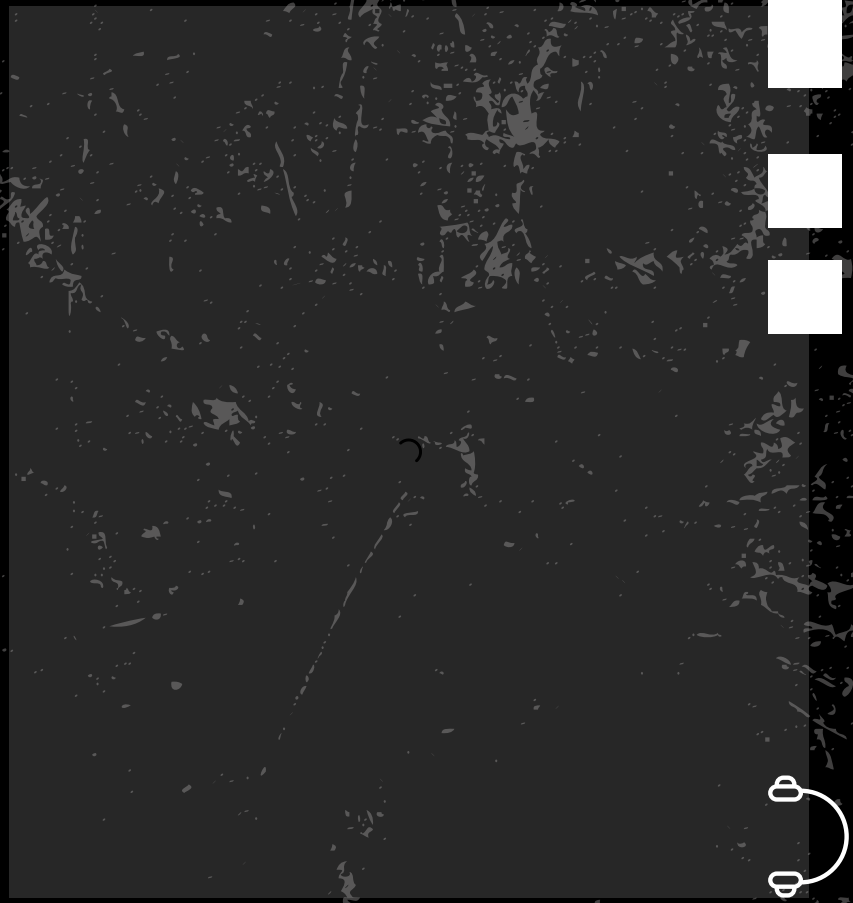
PROGRAMA 10

CRIMINOLOGÍA Y SEGURIDAD



PROGRAMA 9

CRIMINOLOGÍA Y SEGURIDAD



AMENAÇA GLOBAL

PROGRAMA 11

CRIMINOLOGÍA Y SEGURIDAD

Amenaça Global - Confiem en la policia?

Quins models policials tenen una bona rebuda social?

rtve RTVE.es / Jul 26, 2022

PROGRAMA 12

CRIMINOLOGÍA Y SEGURIDAD

AMENAÇA GLOBAL

PROGRAMA 14

CRIMINOLOGÍA Y SEGURIDAD

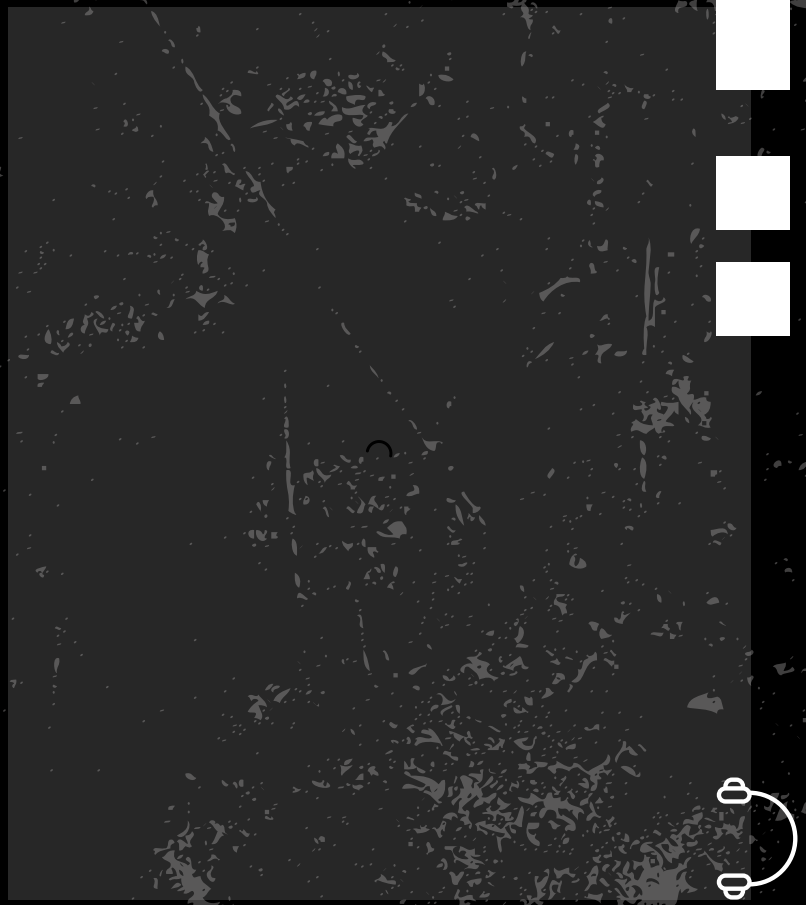
PROGRAMA 13

CRIMINOLOGÍA Y SEGURIDAD

AMENAÇA GLOBAL

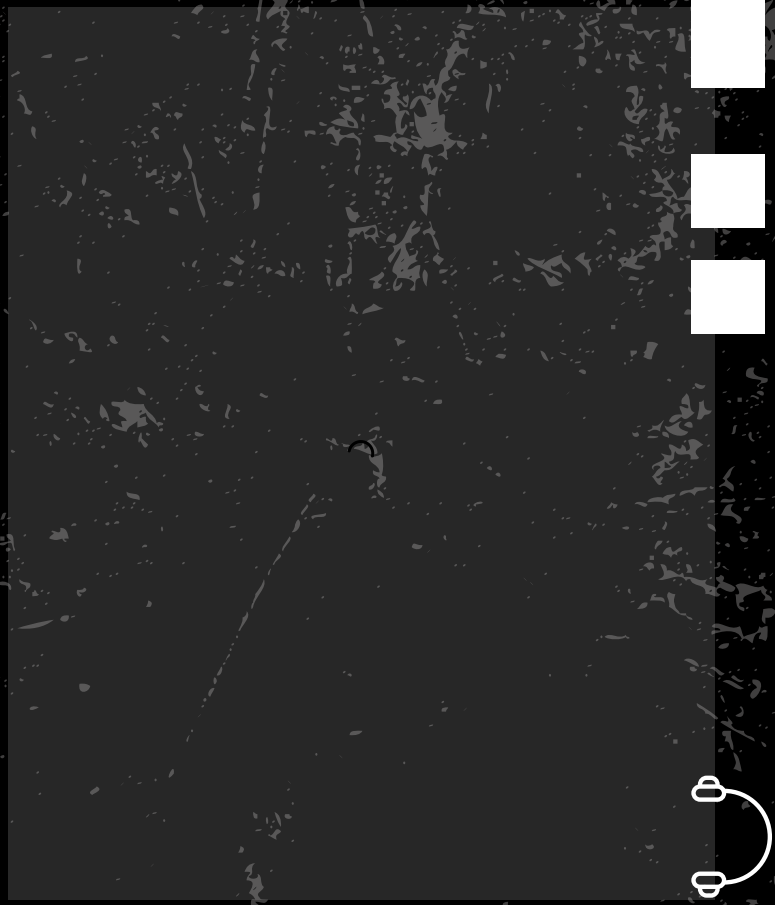
PROGRAMA 16

CRIMINOLOGÍA Y SEGURIDAD



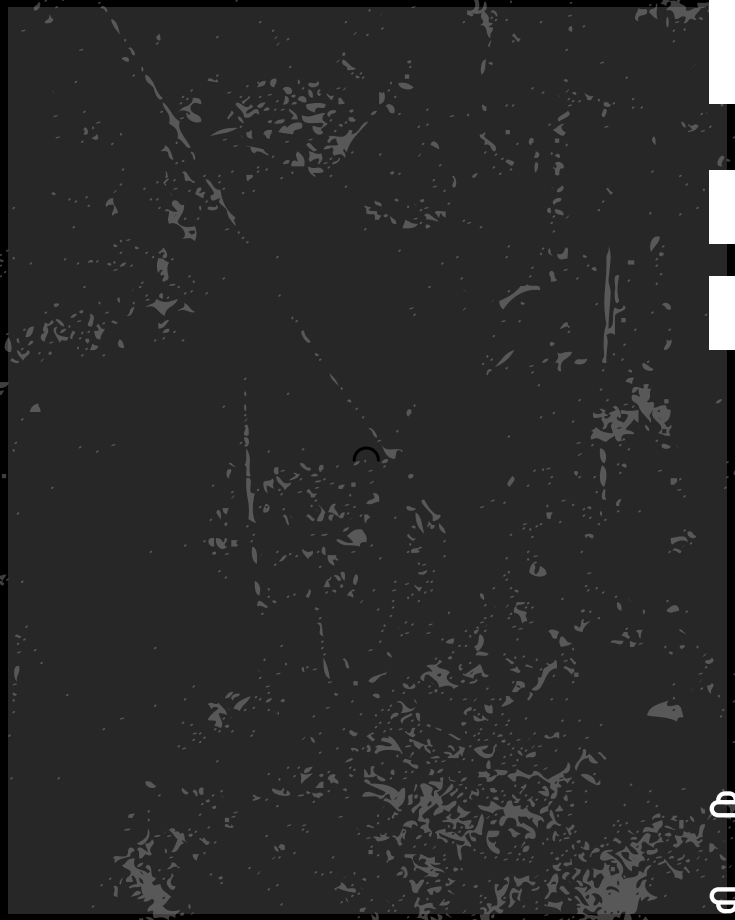
PROGRAMA 15

CRIMINOLOGÍA Y SEGURIDAD

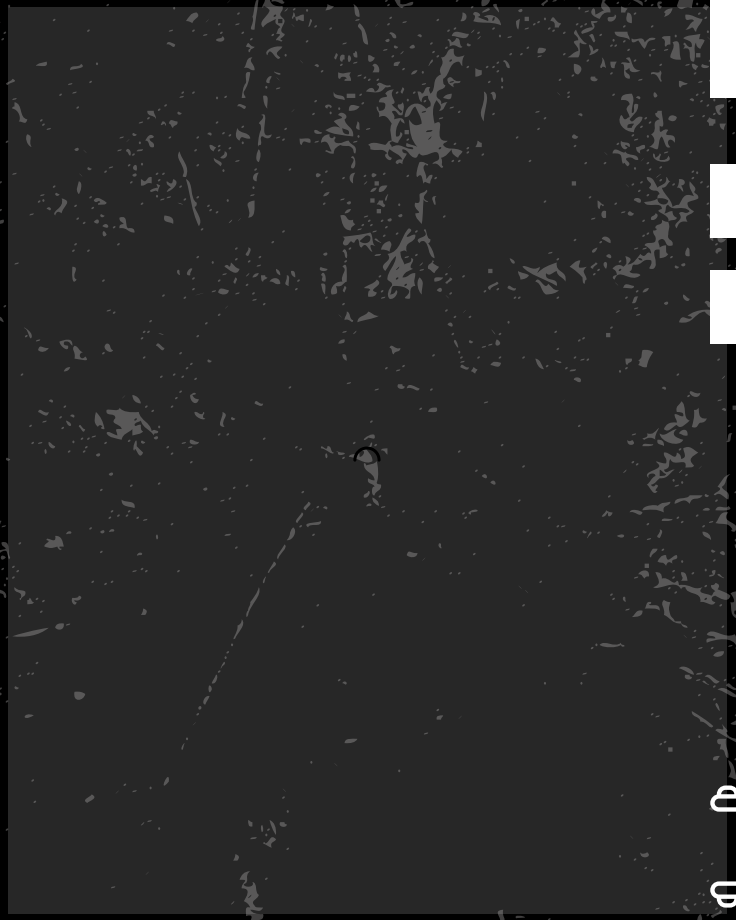


AMENAÇA GLOBAL

PROGRAMA 18
CRIMINOLOGÍA Y SEGURIDAD



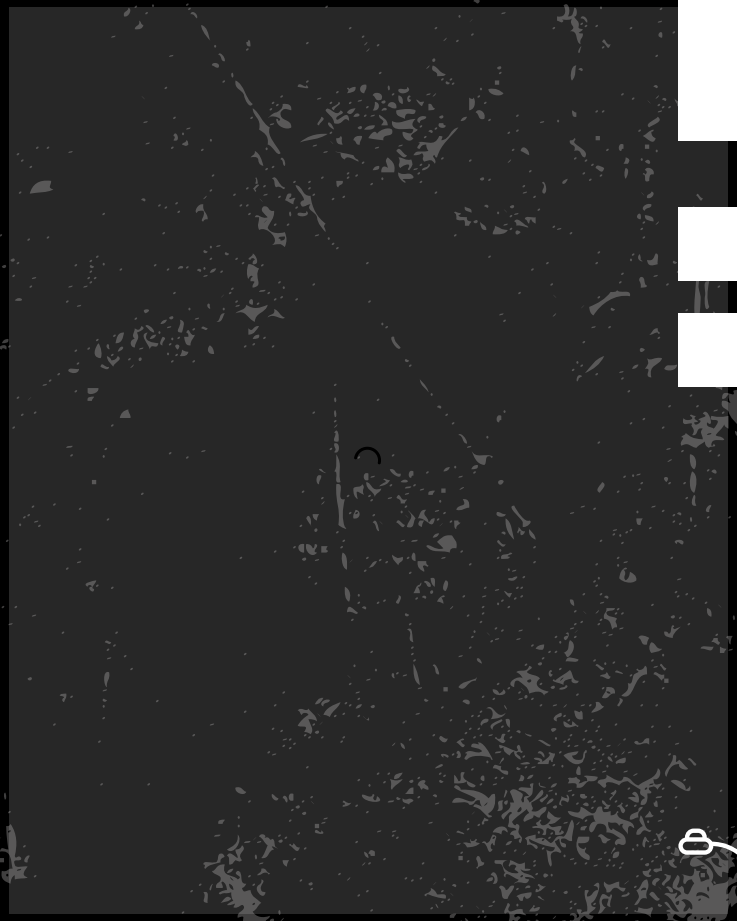
PROGRAMA 17
CRIMINOLOGÍA Y SEGURIDAD



AMENAÇA GLOBAL

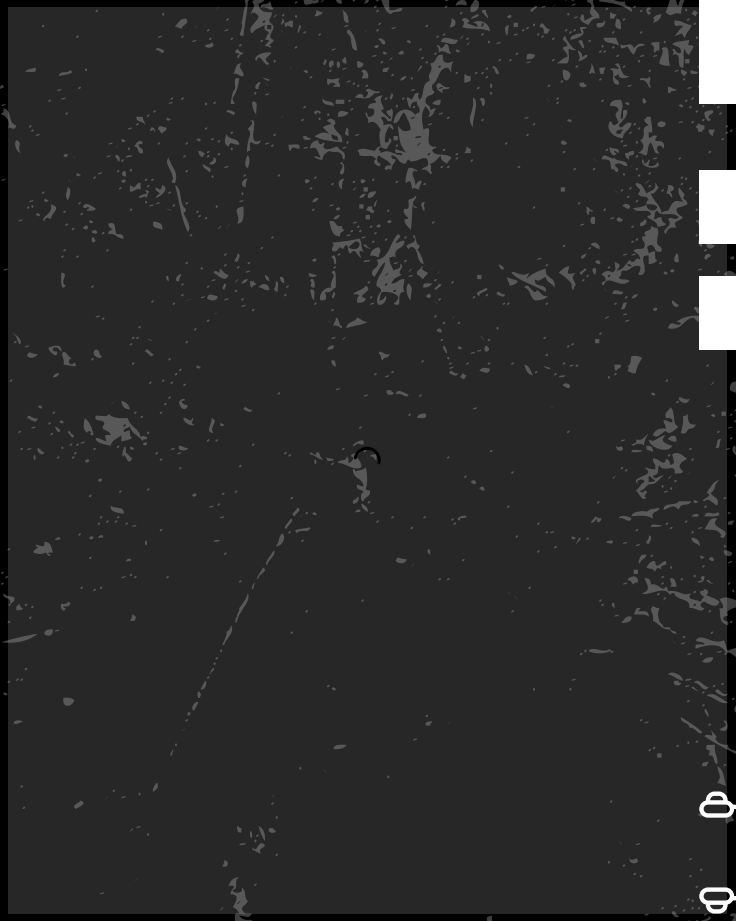
PROGRAMA 20

CRIMINOLOGÍA Y SEGURIDAD



PROGRAMA 19

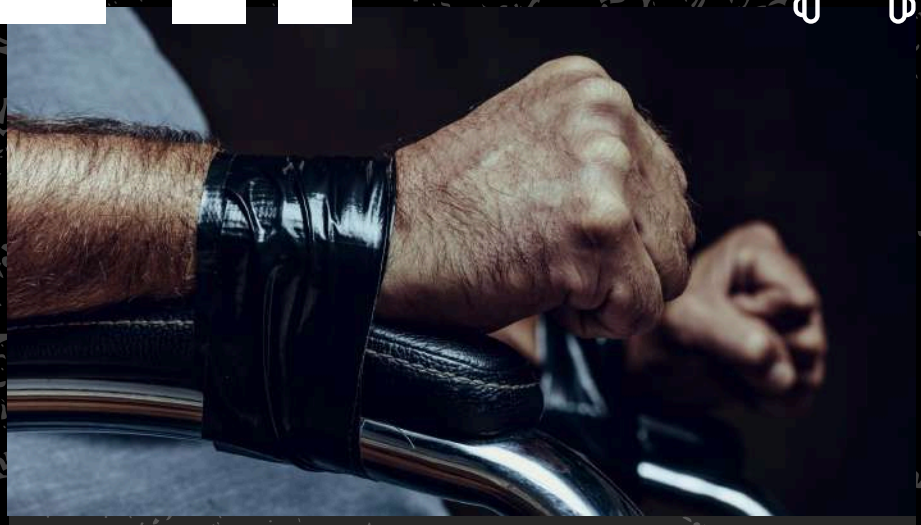
CRIMINOLOGÍA Y SEGURIDAD



AMENAÇA GLOBAL

PROGRAMA 21

CRIMINOLOGÍA Y SEGURIDAD



PROGRAMA 22

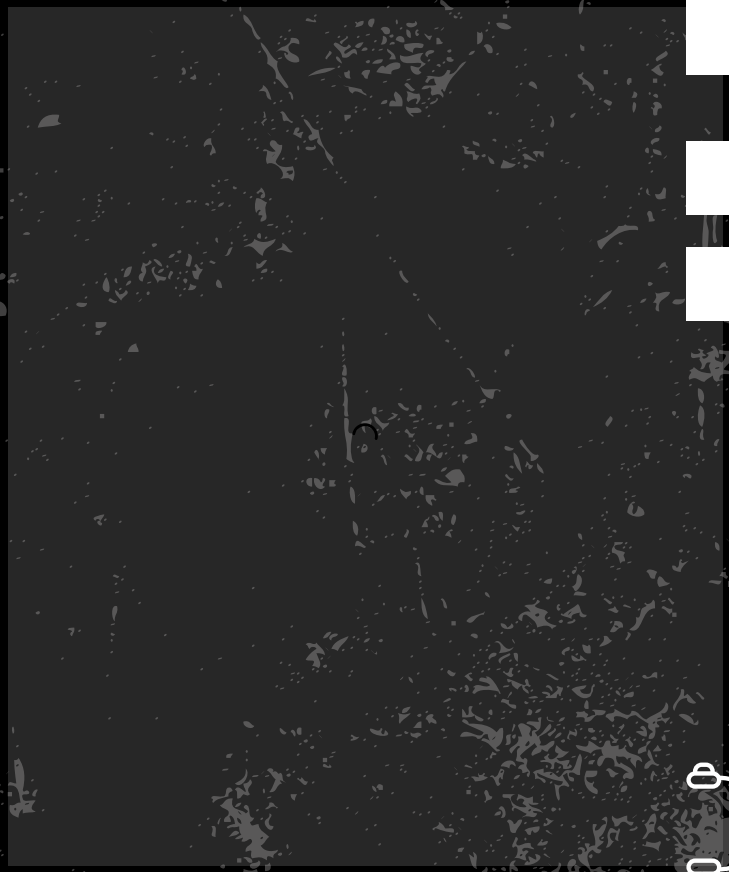
CRIMINOLOGÍA Y SEGURIDAD

Amenaça Global - Víctimes de la yihad negra del Daesh

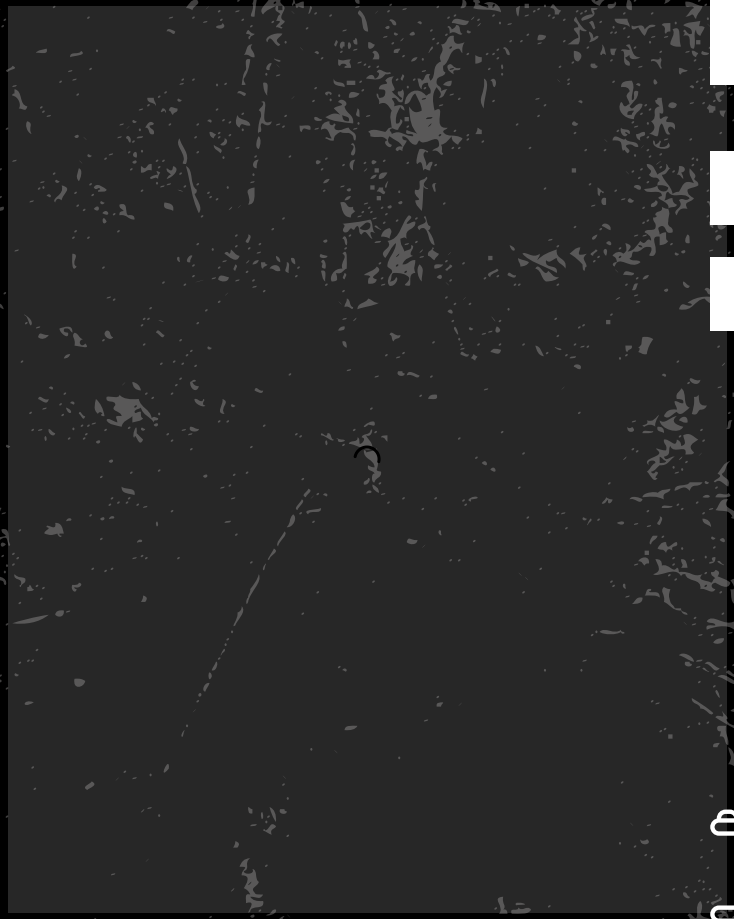
Emisión del programa Amenaça Global titulado Víctimes de la yihad negra del Daesh. Todos los contenidos de RNE los tienes aquí, en RTVE Play

AMENAÇA GLOBAL

PROGRAMA 24
CRIMINOLOGÍA Y SEGURIDAD

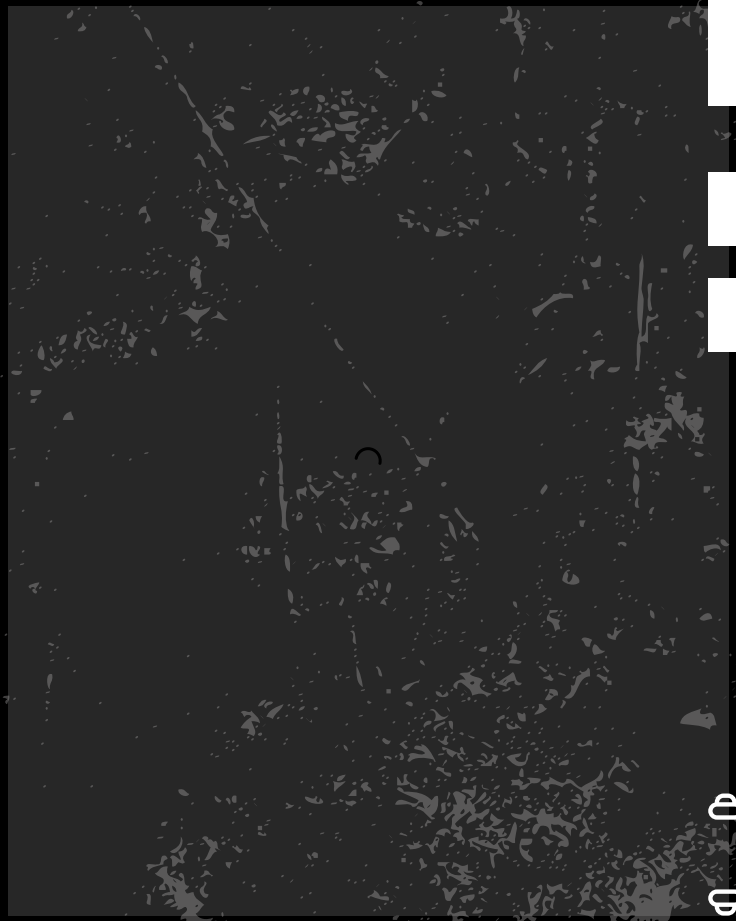


PROGRAMA 23
CRIMINOLOGÍA Y SEGURIDAD

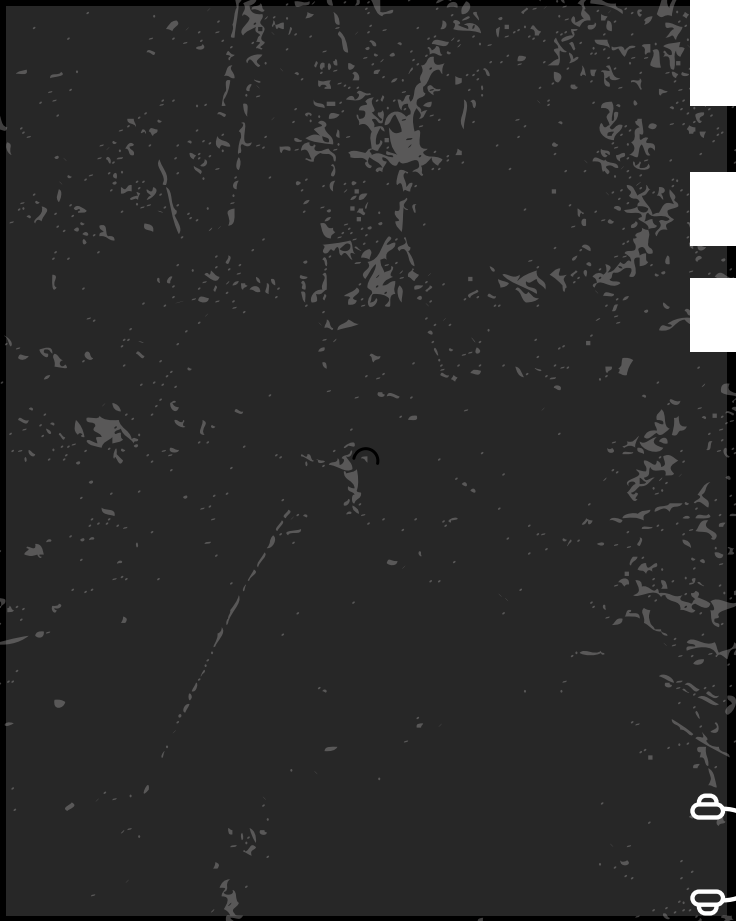


AMENAÇA GLOBAL

PROGRAMA 26
CRIMINOLOGÍA Y SEGURIDAD



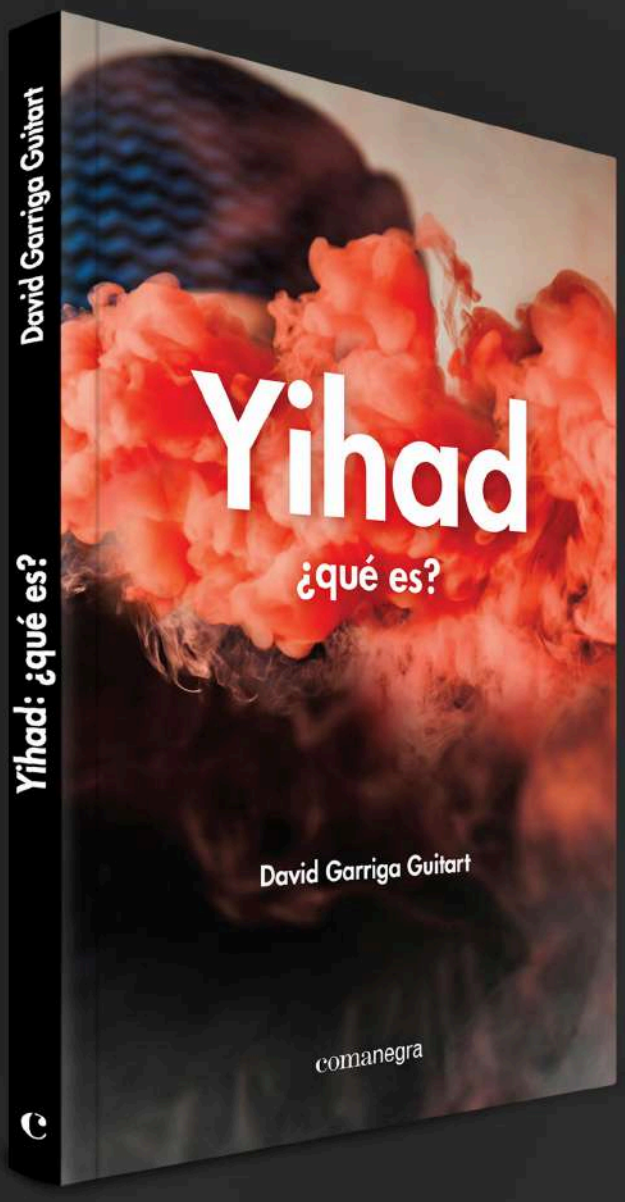
PROGRAMA 25
CRIMINOLOGÍA Y SEGURIDAD



YIHAD, ¿QUÉ ES?

David Garriga Guitart

UNA GUÍA PARA ENTENDER QUÉ ES EL YIHADISMO.



cómpralo con un 5% de descuento en:
www.comanegra.com

*Código de descuento: YHD-17

comanegra

Revista indexada en Revistas Científicas de América Latina,el Caribe, España y Portugal (LATINDEX)

www.alghuraba.org

Comunidad de Inteligencia y Seguridad Global

AL-GHURABÁ

COLABORADORES