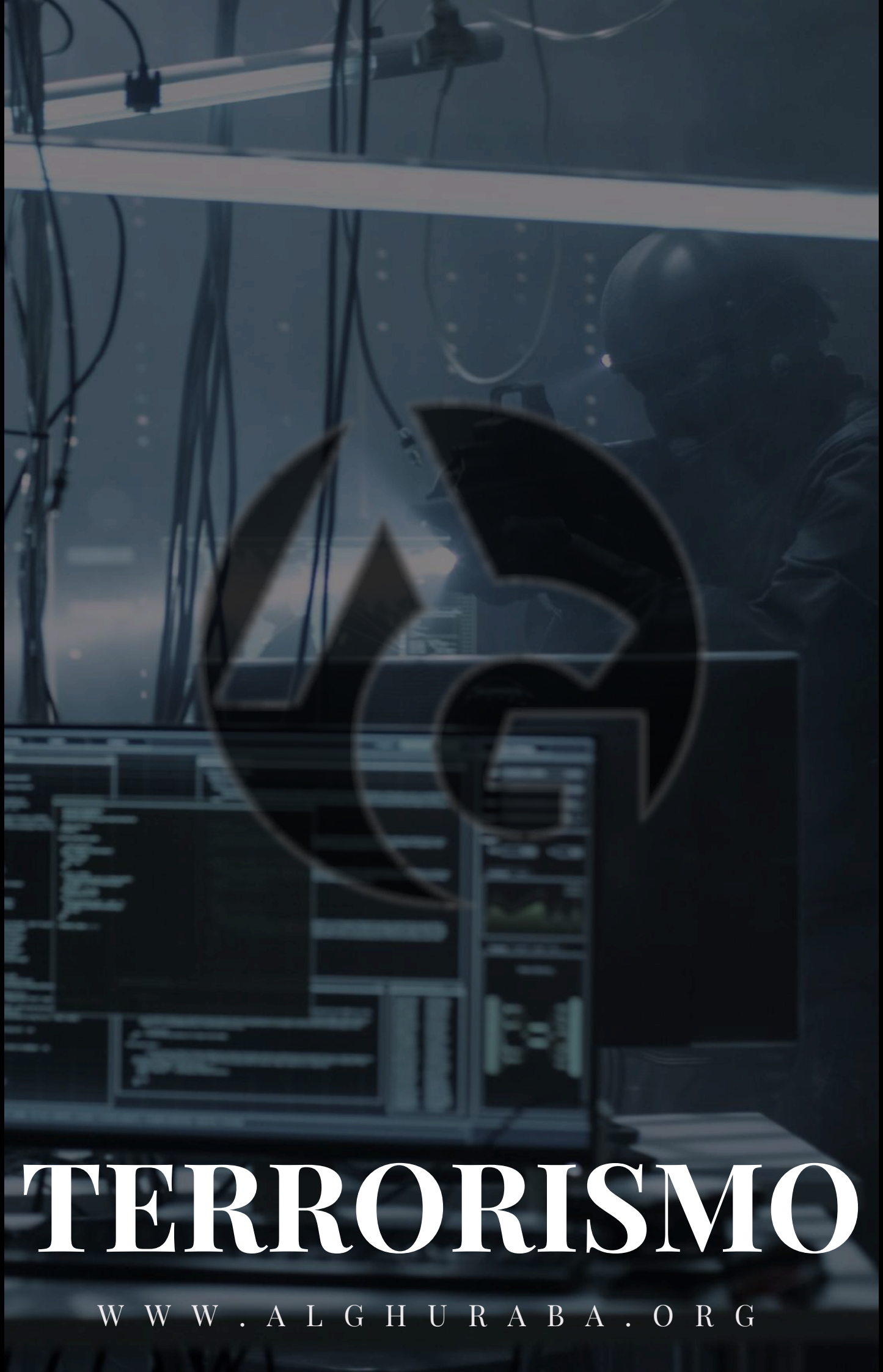

TERRORISMO

WWW.ALGHURABA.ORG

EL TERRORISMO

COMO TÁCTICA ENCUBIERTA DE LA GUERRA HÍBRIDA

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

INTRODUCCIÓN

El terrorismo se ha consolidado como un recurso clave dentro del esquema de la guerra híbrida, una forma de conflicto que combina tácticas convencionales, irregulares, criminales y psicológicas en un marco flexible y simultáneo (Kaiser, A., 2025). Esta estrategia es utilizada tanto por Estados como por actores no estatales para alcanzar objetivos políticos o geoestratégicos, aprovechando su versatilidad y la dificultad de ser contrarrestada de manera clara y efectiva.

En este tipo de enfrentamientos, el terrorismo —entendido como el uso sistemático de la violencia con fines intimidatorios y desestabilizadores— ofrece ventajas decisivas. Actúa como un medio para compensar la desventaja militar directa, generando un impacto desproporcionado a través del miedo, la incertidumbre y la confusión. Asimismo, al operar mediante estructuras encubiertas o con apoyo de intermediarios, complica la identificación de los responsables, entrelazándose con redes ilícitas y estrategias de desinformación (Liddell, B.S.,2019). Estas acciones, además de producir efectos políticos, permiten el acceso a recursos materiales y respaldo logístico mediante canales ilegales o institucionalmente débiles.

Diversos casos han mostrado cómo estas dinámicas se insertan en contextos de confrontación híbrida (Kaiser, A., 2025). Rusia, por ejemplo, ha empleado asesinatos selectivos, atentados fuera de su territorio y campañas de propaganda para intimidar y desestabilizar democracias, combinando estas acciones con ofensivas cibernéticas y manipulaciones informativas (San Martín, H., 2018; Banasik, M., 2024). Grupos como Hezbollah también ofrecen ejemplos ilustrativos, al fusionar capacidades militares regulares con operaciones terroristas y tácticas irregulares, en un modelo híbrido de notable sofisticación (Belliard, J.R., 2025).

El impacto de estas es profundo: erosionan la gobernabilidad, minan la confianza en las instituciones y dificultan la capacidad del Estado para responder ante amenazas difusas y multidimensionales (Liddell, B.S.,2019). Lejos de ser un fenómeno aislado, el terrorismo potencia otras formas de agresión, actuando de forma coordinada y compleja en múltiples frentes.

LA GUERRA HÍBRIDA

La guerra híbrida es una forma contemporánea de conflicto que se caracteriza por la combinación de medios militares convencionales con herramientas no tradicionales, como los ciberataques, las operaciones de influencia, el sabotaje y la presión económica (Gavaldà, I., 2024; Zapata, M., 2024; Kaiser, A., 2025). Su rasgo distintivo es la ambigüedad: no se manifiesta a través de declaraciones formales de guerra ni mediante enfrentamientos abiertos, sino mediante acciones encubiertas y el uso estratégico de la manipulación de la percepción pública (Fernando, L., 2024).

En este tipo de escenario, las acciones suelen ser delegadas a terceros, como milicias, mercenarios, insurgentes o grupos terroristas. El uso de tecnologías digitales permite alterar procesos políticos, polarizar a las sociedades y aumentar la vulnerabilidad interna de los Estados.

El epicentro del conflicto, por tanto, ya no está en el campo de batalla, sino en sectores neurálgicos de la sociedad: la opinión pública, la cohesión social y la estabilidad institucional.

Esta modalidad bélica representa un serio desafío para la seguridad internacional, ya que diluye las fronteras entre la paz y el conflicto. Obliga a los Estados a prepararse para amenazas que pueden afectar infraestructuras críticas, sistemas políticos e incluso la cohesión social, muchas veces sin que se dispare una sola bala.

ESTRATEGIAS Y TÁCTICAS TERRORISTAS EN LA GUERRA HÍBRIDA

Como componente táctico de las guerras híbridas, el terrorismo busca socavar la estabilidad del adversario actuando sobre su tejido social y político (Zapata, M., 2024, Kaiser, A., 2025).

Mediante acciones encubiertas, ataques indirectos y el uso de intermediarios, se evita la atribución directa, lo que reduce las posibilidades de represalias claras (Liddell, B.S.,2019). Al mismo tiempo, se emplean medidas de presión económica y social, como la manipulación de recursos críticos o la difusión de mensajes hostiles que generan un clima de inseguridad.

En este contexto, los grupos terroristas encuentran un terreno fértil para operar, ya que pueden influir en el desarrollo de los conflictos sin exponerse a un enfrentamiento directo (Baqués, J., 2021).

Entre las tácticas más utilizadas se encuentran los atentados contra civiles y símbolos culturales, los secuestros, asesinatos selectivos y ataques suicidas (Fernando, L., 2024).

Estas acciones, diseñadas para maximizar el impacto emocional y político, se potencian con el uso de tecnología avanzada —como drones, ciberarmas y sistemas de vigilancia—, así como con la instrumentalización de fenómenos como las migraciones masivas, que pueden convertirse en herramientas de presión geopolítica (Fernando, L., 2024; Gavaldà, I., 2024).

A modo de complemento a estas tácticas, la manipulación informativa se consolida como un elemento central en estas estrategias (Liddell, B.S.,2019). A través de la difusión de noticias falsas, el uso de trolls digitales, deepfakes e inteligencia artificial, se socava la cohesión interna de los Estados y se debilita su capacidad de respuesta (Fernando, L., 2024).
Estas técnicas buscan fracturar el consenso social, erosionar la legitimidad de las autoridades y alimentar divisiones ideológicas o identitarias. Las redes sociales amplifican este fenómeno al facilitar la rápida y masiva circulación de narrativas manipuladas.

Diversos episodios recientes han mostrado cómo estas técnicas se han aplicado con éxito: desde ciberataques en Europa hasta interferencias en procesos electorales en el Este europeo (Gavaldà, I., 2024).
En conflictos como los de Ucrania, el Magreb o Medio Oriente, la convergencia entre terrorismo, crimen organizado y manipulación política ha dado lugar a escenarios especialmente complejos, donde los ataques no siempre tienen una autoría clara ni un frente visible (Caride, E., 2024).

TERRORISMO BLANDO EN LA GUERRA HÍBRIDA

El terrorismo blando hace referencia a formas de violencia o presión que, aunque no alcanzan el nivel de ataques armados directos, buscan influir, intimidar o desestabilizar a una sociedad mediante métodos menos letales, como la desinformación, la manipulación mediática, el ciberacoso o la coacción moral (Gavaldà, I., 2024).

En el contexto de la guerra híbrida, estas tácticas se combinan con estrategias tanto convencionales como irregulares —como el terrorismo clásico, la ciberguerra, las operaciones de influencia — con el objetivo de explotar vulnerabilidades políticas, económicas, tecnológicas y sociales, sin necesidad de recurrir a la violencia abierta (Liddell, B.S.,2019; Zapata, M., 2024; Kaiser, A., 2025). La finalidad es debilitar al adversario y erosionar su cohesión interna, operando dentro de ese espacio ambiguo aparentemente de paz (Korybko, A., 2015). En este escenario, las redes sociales desempeñan un papel fundamental, ya que permiten difundir desinformación y propaganda de forma masiva y veloz, influir en la opinión pública y minar la confianza en las instituciones. Estas plataformas tienen la capacidad de viralizar contenidos maliciosos, manipular narrativas y polarizar a la sociedad, aprovechando algoritmos que refuerzan los sesgos de los usuarios. Además, facilitan la coordinación de campañas de presión, protestas o apoyos, y exponen vulnerabilidades tanto de actores estatales como no estatales.

Así, las redes sociales se han convertido en una herramienta poderosa dentro de la guerra híbrida, integrándose con otras tácticas militares y no convencionales (Kaiser, A., 2025).

ACCIONES TERRORISTAS EN SITUACIONES DE GUERRA HÍBRIDA

Un caso emblemático de guerra híbrida en el que se ha utilizado el terrorismo es el conflicto entre Israel y Hezbolá en 2006 (Zapata, M., 2024; Kaiser, A., 2025). En este enfrentamiento, Hezbolá —organización catalogada como terrorista por diversos países y organismos internacionales— combinó tácticas militares convencionales, como el uso de misiles de corto y medio alcance, con métodos no convencionales (Korybko, A., 2015; Belliard, J.R., 2025).

Estos incluyeron la movilización de milicianos entrenados en combate urbano, la ejecución de ataques sorpresa contra objetivos civiles y militares, el uso sistemático de propaganda mediática y la recepción de apoyo logístico y financiero tanto de actores estatales como de redes no estatales (Fernando, L., 2024). Esta fusión de técnicas y recursos desdibujó la frontera tradicional entre la guerra regular y el terrorismo, complicando la respuesta militar y diplomática de Israel, y generando una nueva dinámica en los conflictos asimétricos contemporáneos.

Otro ejemplo significativo de la aplicación del terrorismo dentro de una estrategia híbrida es la campaña global desarrollada por el autodenominado Estado Islámico (ISIS) (Kaiser, A., 2025). Esta organización no solo llevó a cabo atentados terroristas en distintos continentes, sino que también desplegó una potente maquinaria de propaganda digital para reclutar combatientes, difundir ideología extremista y generar miedo a escala global (Korybko, A., 2015). Además, realizó operaciones militares irregulares, ocupando territorios en Siria e Irak, imponiendo gobiernos locales y cobrando impuestos, lo que demostró una sofisticación estratégica inusual en grupos terroristas (Korybko, A., 2015). La combinación de estas herramientas le permitió al ISIS actuar simultáneamente como grupo terrorista, ejército insurgente y actor político en el tablero internacional, desafiando el orden estatal y sembrando caos en regiones enteras (Korybko, A., 2015).

Rusia, por su parte, ha sido acusada reiteradamente de utilizar tácticas propias de la guerra híbrida con componentes claramente terroristas (San Martín, H., 2018; Banasik, M., 2024; Kaiser, A., 2025). Entre estas se incluyen los asesinatos selectivos de opositores y exagentes en territorio extranjero, el apoyo encubierto a organizaciones extremistas con intereses alineados, y la ejecución de ataques deliberados contra objetivos civiles durante sus intervenciones militares (Fernando, L., 2024).

Estas acciones forman parte de una estrategia más amplia dirigida a desestabilizar democracias, debilitar instituciones internacionales y expandir su influencia geopolítica. La ambigüedad de estas tácticas, combinada con su negación sistemática por parte del Kremlin, dificulta la atribución directa y complica las respuestas diplomáticas y legales de los países afectados.

Un caso paradigmático de este tipo de conflicto híbrido es la guerra en Ucrania, iniciada en 2014 tras la anexión de Crimea por parte de Rusia (San Martín, H., 2018; Caride, E., 2024). Este conflicto ha involucrado tanto fuerzas regulares como grupos paramilitares y separatistas prorrusos, operaciones de desinformación masiva, ciberataques a infraestructuras críticas, campañas de propaganda en redes sociales y una presencia militar encubierta negada oficialmente por Moscú (Gavaldà, I., 2024). La complejidad y persistencia del conflicto lo convierten en uno de los ejemplos más claros de cómo se despliega una guerra híbrida en múltiples dimensiones —militar, informativa, económica y psicosocial— para desestabilizar a un Estado soberano (Kaiser, A., 2025).

Otro ejemplo reciente fue la crisis migratoria entre Bielorrusia y la Unión Europea en 2021 (San Martín, H., 2018; Banasik, M., 2024). Diversos analistas y organismos internacionales interpretaron este fenómeno como un ataque híbrido, ya que el régimen bielorruso habría facilitado el paso de migrantes hacia las fronteras de países como Polonia y Lituania con la intención de provocar una crisis humanitaria y presionar políticamente a la Unión Europea. Este uso instrumental de la migración como arma política refleja cómo, en el contexto de la guerra híbrida, se emplean medios no militares para alcanzar objetivos estratégicos, erosionando la estabilidad social y la cohesión interna de los Estados atacados (Kaiser, A., 2025).

En conjunto, estos casos demuestran que el terrorismo, lejos de actuar aisladamente, puede formar parte de una arquitectura estratégica más amplia. Cuando se inserta en el marco de la guerra híbrida, se convierte en una herramienta de alta eficacia para alcanzar metas políticas, desestabilizar adversarios y alterar el equilibrio global sin necesidad de una guerra convencional abierta (Kaiser, A., 2025). Esto plantea enormes desafíos para los Estados, que deben adaptarse a un entorno de seguridad cada vez más difuso, donde las amenazas no siempre provienen de ejércitos regulares, sino de una combinación de actores y métodos interconectados.

MEDIDAS PREVENTIVAS CONTRA EL TERRORISMO EN LAS GUERRAS HÍBRIDAS

Las acciones contra el terrorismo como herramienta en la guerra híbrida requieren un enfoque integral y adaptado a las características no convencionales de este tipo de conflicto ((Ministerio de Defensa, 2020; Zapata, M., 2024).
Es necesario implementar políticas de ciberdefensa robustas para proteger infraestructuras críticas y prevenir ciberataques que los grupos terroristas puedan aprovechar. Esto implica monitorear constantemente las redes digitales, proteger datos sensibles y actuar rápidamente ante incidentes de ciberseguridad (Gavaldà, I., 2024).

Además, es esencial desarrollar estrategias para contrarrestar la desinformación y la propaganda terrorista en las redes

sociales y otros medios (Liddell, B.S.,2019). Estas medidas pueden incluir la creación de campañas que desmientan los relatos "fake" y distorsiones, promoviendo información veraz y confiable que desafíe los discursos manipulados. También, los gobiernos y plataformas digitales deben colaborar para evitar que las redes sociales se conviertan en vehículos de radicalización, reclutamiento y coordinación de actividades terroristas. Esto puede implicar la identificación y eliminación de contenido relacionado con el terrorismo, la detección de cuentas falsas y la vigilancia de posibles actividades extremistas.

El terrorismo en la guerra híbrida tiene una dimensión transnacional, por lo que la cooperación internacional es fundamental (Kaiser, A., 2025). Los países deben compartir inteligencia, coordinar esfuerzos de seguridad y colaborar en la persecución de terroristas tanto en línea como fuera de línea. Además, es necesario trabajar conjuntamente para prevenir el financiamiento del terrorismo, que a menudo se oculta en actividades legítimas.

Fomentar la cohesión social y la resistencia frente a la polarización es otro aspecto clave. La promoción de la inclusión, el entendimiento intercultural y la lucha contra la discriminación puede reducir las oportunidades de los grupos terroristas para sembrar discordia y crear tensiones dentro de las sociedades. La protección de las instituciones democráticas también es crucial, ya que los grupos terroristas pueden atacar sistemas clave como el judicial, los medios de comunicación o las fuerzas de seguridad (Ministerio de Defensa, 2020). Garantizar la integridad de estas instituciones es esencial para evitar que los terroristas socaven la estabilidad política y social.

La recopilación y el análisis de inteligencia son fundamentales para prevenir y neutralizar las actividades terroristas. Las operaciones encubiertas, como el sabotaje de comunicaciones o la infiltración de redes terroristas, son esenciales para desbaratar amenazas antes de que se materialicen. Asimismo, es necesario implementar programas educativos que fomenten el pensamiento crítico y la resistencia a la manipulación ideológica, especialmente en escuelas, universidades y comunidades, para educar sobre los riesgos del terrorismo en la guerra híbrida (Kaiser, A., 2025).

La combinación de las estrategias citadas es la clave para mitigar el impacto del terrorismo y neutralizar las tácticas empleadas en los conflictos híbridos (Ministerio de Defensa, 2020).

CONCLUSIONES

El terrorismo, dentro del contexto de la guerra híbrida, se ha consolidado como una herramienta potente y compleja, capaz de desestabilizar tanto a nivel local como global (Kaiser, A., 2025). Aprovechando la ambigüedad y la capacidad de adaptación de este tipo de conflicto, el terrorismo opera en lo que se conoce como la "zona gris", un espacio ambiguo entre la paz y la guerra abierta (Baqués, J., 2021).

En este entorno, se emplea estratégicamente para socavar la cohesión interna de los Estados, desestabilizar sociedades y alterar el equilibrio de poder sin necesidad de un enfrentamiento militar convencional. Las tácticas terroristas, que incluyen ataques indiscriminados, desinformación, ciberataques y coacción psicológica, no solo provocan respuestas emocionales y políticas inmediatas, sino que también generan una incertidumbre prolongada (Gavaldà, I., 2024).

Estas acciones, combinadas con otras formas de guerra híbrida, dificultan la atribución de responsabilidades, permitiendo a los actores, tanto estatales como no estatales, operar sin las restricciones legales y políticas que acompañan a los conflictos tra-

-dicionales. La guerra híbrida, al integrar el terrorismo como pieza clave en su estrategia, presenta enormes desafíos para la seguridad internacional (Zapata, M., 2024). Estos conflictos desdibujan las fronteras entre la paz y la guerra, y obligan a los Estados a repensar sus enfoques de defensa y respuesta (Gavaldà, I., 2024). Además, es crucial fortalecer la cooperación internacional para abordar las amenazas transnacionales en el marco de esta guerra híbrida, compartiendo inteligencia y recursos para prevenir y neutralizar las actividades terroristas.

En definitiva, el terrorismo no solo representa una amenaza física, sino también psicológica y social, cuyos efectos trascienden los ataques inmediatos. Su inclusión en las dinámicas de la guerra híbrida exige respuestas integrales y adaptativas, que combinen ciberseguridad, medidas diplomáticas y el fortalecimiento de la cohesión social (Gavaldà, I., 2024).
Tanto la guerra híbrida como el terrorismo están redefiniendo la naturaleza de los conflictos contemporáneos, por lo que es esencial adoptar un enfoque multifacético para enfrentarlos y mitigar su impacto.

REFERENCIAS

Banasik, M. (2024). Seguridad y guerra híbrida: Nuevo paradigma de rivalidad de la Federación Rusa en la arena internacional. Ediciones Nuestro Conocimiento.

Baqués, J. (2021). De las guerras híbridas a la zona gris: la metamorfosis de los conflictos en el siglo XXI. UNED.

Belliard, J.R. (2025). Hezbollah-Israël: Une guerre sans limites. Nouveau monde Editions.

Caride, E. (2024). Controlar Ucrania: La guerra híbrida y las operaciones no convencionales rusas en la guerra de Ucrania. ndependently published.

Fernando, L. (2024). Nuevas guerras: Híbridas, cibernéticas y asimétricas. Independently published.

Gavaldà, I. (2024). La Cibertecnología como arma en la Guerra Híbrida. McGraw Hill.

Kaiser, A. (2025). Detrás de la máscara de la paz: La guerra híbrida: La guerra por otros medios contra la civilización occidental. IP.

Korybko, A. (2015). Guerras híbridas. De las revoluciones de colores a los golpes. Institute for Strategic Studies and Predictions.

Liddell, B.S. (2019). Estrategia. Arzalia.

Ministerio de Defensa. (2020). Amenaza híbrida La guerra imprevisible. Cátedra Miguel de Cervantes.

San Martín, H. (2018). La guerra híbrida rusa sobre occidente. Page. P.

Zapata, M. (2024). Amenazas híbridas. El nuevo tipo de guerra de la Sociedad Digital. Independently published.