El artículo examina una operación encubierta ocurrida en septiembre de 2024, en la que dispositivos de comunicación de miembros de Hezbolá explotaron de forma sincronizada en Medio Oriente. Analiza el impacto del uso de tecnología y la infiltración en cadenas de suministro sobre las doctrinas y tácticas de actores no estatales en conflictos asimétricos. El estudio emplea una metodología cualitativa basada en análisis de fuentes abiertas. Los resultados evidencian una adaptación doctrinal de Hezbolá y la consolidación de un modelo de guerra encubierta tecnológica.

Tecnología e Inteligencia en Operaciones Encubiertas: Análisis del Caso Mossad–Hezbolá (septiembre 2024)

Technology and Intelligence in Covert Operations: Analysis of the Mossad–Hezbollah Case (September 2024)

This article examines a covert operation conducted in September 2024 in which communication devices used by Hezbollah members exploded in a synchronized manner across the Middle East. It analyzes the impact of technological use and supply chain infiltration on the doctrines and tactics of non-state actors in asymmetric conflicts. The study employs a qualitative methodology based on open-source analysis. The findings reveal Hezbollah's doctrinal adaptation and the consolidation of a model of technologically driven covert warfare.

Palomino, V. (2025). Tecnología e Inteligencia en Operaciones Encubiertas: Análisis del Caso Mossad–Hezbolá (septiembre 2024). Revista *Pensamiento Conjunto,* Año 13, N° 2. pp. 94-99. ISSN° 2707-367X

Fecha de recepción: 18 de agosto de 2025.
Fecha de aceptación: 17 de noviembre de 2025.
Fecha de publicación: 31 de diciembre de 2025.

Teniente Coronel EP
David Palomino Villcas
orcid.org/0009-0005-2062-7649

Magister en Ciencias Militares por la Escuela Superior de Guerra del Ejército; Candidato a Magister en Administración y Gestión Pública por el Centro de Altos Estudios Nacionales; Licenciado en Ciencias Militares por la Escuela Militar de Chorrillos; Curso Superior de Inteligencia Estratégica en la Escuela Nacional de Inteligencia - DINI; Diplomado en el Programa de Inteligencia Estratégica y Operacional en la Escuela Superior Conjunta de las FFAA. Comandó el Batallón contraterrorista N° 334 en el VRAEM; Integrante del V Contingente de la Compañía Perú en la Estabilización de las Naciones Unidas en la República de Haití; Jefe del Departamento de Evaluación y de Calidad Educativa en la Escuela Superior Conjunta de las FFAA; Especialista en la Dirección de Movilización y la Dirección de Política y Planeamiento para la Defensa en el MINDEF.

INTRODUCCIÓN

Las operaciones de inteligencia vienen experimentando cambios significativos durante las últimas décadas, los avances tecnológicos han permitidos a las agencias estatales llevar a cabo misiones encubiertas con mayor precisión, alcance global y efectos letales. En este contexto, el Instituto de Inteligencia y Operaciones Especiales de Israel (Mossad) ha perfeccionado el enfoque de operaciones combinando la manipulación de redes tecnológicas, con la cobertura comercial y la acción encubierta remota a distancia con daños físicos destructivos.

Un ejemplo notable de esta evolución ocurrió entre el 17 y 18 de septiembre de 2024 en Líbano, Siria e Irak, cuando una serie de dispositivos de comunicación personal, principalmente buscapersonas (beepers) y walkie-talkies, estallaron de manera coordinada. Estos equipos, utilizados por miembros del grupo chiíta Hezbolá, habrían sido intervenidos previamente por el Mossad a través de una sofisticada operación de infiltración en la cadena de suministro global. Esta operación se facilitó gracias a un cambio en la doctrina de comunicaciones de Hezbolá, impulsado por las disposiciones de su líder, Hassan Nasrallah, quien buscaba evitar el uso de tecnologías modernas que pudieran ser susceptibles de vigilancia extranjera (BBC, 2024).

Según informes de CBS News (2024), ex agentes del Mossad revelaron que la operación incluyó la creación de empresas ficticias para introducir explosivos en dispositivos fabricados por Gold Apollo, una firma taiwanesa que

PALABRAS CLAVE: INTELIGENCIA ESTRATÉGICA, TECNOLOGÍA, OPERACIONES ENCUBIERTAS, MOSSAD, HEZBOLÁ.
KEYWORDS: STRATEGIC INTELLIGENCE; TECHNOLOGY; COVERT OPERATIONS; MOSSAD; HEZBOLLAH.

92

subcontrató la producción a una empresa húngara presuntamente infiltrada. Como resultado, el ataque dejó al menos 42 muertes y más de 2,800 heridos, provocando una fuerte condena internacional, incluyendo declaraciones del Alto Comisionado de Derechos Humanos de la ONU, quien calificó la acción como un posible crimen de guerra.

Este artículo tiene como objetivo examinar el incidente desde la perspectiva de la inteligencia estratégica y operacional, con un enfoque especial en las doctrinas y tácticas del adversario. Se busca responder a la siguiente pregunta: ¿cómo reconfigura el uso de tecnología en operaciones encubiertas, como la del Mossad contra Hezbolá, las doctrinas y tácticas de actores no estatales en conflictos asimétricos?

MÉTODO.

Para este artículo se utilizó el método cualitativo con un diseño descriptivo-analítico, considerando el análisis de documentos de fuentes accesibles y verificables. La investigación se basa principalmente en la recolección y revisión de artículos periodísticos publicados entre setiembre y diciembre de 2024 por medios internacionales como la BBC News, The New York Times y CBS News, declaraciones de organismos oficiales, como el de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.

La metodología empleada fue el análisis de contenido, enfocado en identificar patrones tácticos, doctrinas operativas y modos de infiltración tecnológica atribuidos al Mossad, así como las respuestas doctrinales y operativas del grupo Hezbolá. La investigación se llevó a cabo desde una perspectiva inductiva, interpretando los acontecimientos suscitados a partir de fuentes indirectas, es decir, sin intervención experimental ni acceso a documentación clasificada.

Se dio prioridad a la información actual, eligiendo solo fuentes verificables publicadas en el periodo inmediato a los hechos. Además, se respetaron principios éticos de investigación, trabajando exclusivamente con información pública, pero evitando a la vez reproducir contenidos sensibles o no confiables. El enfoque empleado es apropiado para la enseñanza de operaciones de inteligencia operacional, en las que la comprensión de las tácticas del adversario se basa en análisis exploratorios, dada la naturaleza reservada de los agentes involucrados.

RESULTADOS.

El análisis cualitativo de fuentes abiertas permitió identificar una serie de hallazgos significativos en relación con la operación encubierta atribuida al Mossad durante los días 17 y 18 de septiembre de 2024. Estos resultados se presentan en cinco dimensiones analíticas que reflejan tanto las tácticas operacionales como las implicaciones doctrinales del caso:

1. Reconfiguración doctrinal de las comunicaciones en Hezbolá.
   En respuesta al riesgo de vigilancia digital, la dirigencia de Hezbolá restringió el uso de teléfonos inteligentes y plataformas digitales, adoptando tecnologías consideradas menos vulnerables, como los beepers o pagers, traducido al español como buscapersonas y los walkie-talkies (BBC, 2024). Esta medida refleja una lógica doctrinal orientada a la descentralización operativa y la reducción del perfil electrónico de sus miembros, aunque sin prever los nuevos riesgos tecnológicos derivados de esa transición.
2. Infiltración técnica en la cadena de suministro global.
   El Mossad identificó este cambio táctico y articuló una operación de infiltración y manipulación tecnológica en la cadena de suministro internacional. Según informes de prensa, se establecieron empresas ficticias para intervenir la producción de dispositivos electrónicos en una firma húngara subcontratada por la fabricante taiwanesa, Gold Apollo. Esta infiltración permitió insertar explosivos sin ser detectados en los procesos de adquisición o distribución (The New York Times, citado en BBC, 2024).
3. Ejecución sincronizada de una operación letal.
   La activación coordinada de los dispositivos alterados se llevó a cabo los días 17 y 18 de septiembre de 2024 en múltiples localizaciones de Líbano, Siria e Irak. Las detonaciones resultaron

en al menos 42 muertos y miles de heridos, de acuerdo con fuentes oficiales libanesas (BBC Mundo, 2024). La simultaneidad y precisión de las explosiones sugiere un alto nivel de planificación estratégica y dominio del entorno operativo a distancia, esto representa un nuevo adelanto en la guerra donde dispositivos de comunicación personal se convierten en armas.

4. Consecuencias estratégicas y geopolíticas inmediatas.

   El incidente provocó una reacción diplomática adversa, con condenas internacionales encabezadas por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos, quien calificó la acción como un posible crimen de guerra (BBC News, 2024). Aunque el gobierno israelí, fiel a su doctrina de ambigüedad estratégica, evitó pronunciarse oficialmente, la respuesta de Hezbolá incluyó amenazas de represalias y reforzó sus mecanismos de contrainteligencia.

5. Validación indirecta de las capacidades encubiertas del Mossad.

   La operación evidencia la capacidad del Mossad para identificar las brechas de seguridad de su adversario, operar encubiertamente en sistemas comerciales globales, y realizar ataques letales sin despliegue militar convencional. Este caso fortalece su perfil como agencia especializada en guerra encubierta con una dimensión tecnológica avanzada, marcando un precedente en la integración de inteligencia humana, ingeniería logística internacional y acción letal remota.

DISCUSIÓN.

Los resultados del presente estudio ayudan a interpretar la operación encubierta atribuida al Mossad en septiembre de 2024 como un ejemplo representativo de guerra asimétrica tecnológica, donde la inteligencia estratégica se entrelaza con una comprensión profunda de la doctrina operativa del adversario. La decisión de manipular los dispositivos de comunicación adquiridos por Hezbolá, aprovechando su cambio táctico hacia tecnologías analógicas como estrategia de seguridad, evidencia un alto grado de adaptabilidad, infiltración y dominio del ciclo de inteligencia israelí.

Al compararse con otros estudios sobre la actuación del Mossad en operaciones similares —como el asesinato de científicos nucleares iraníes mediante explosivos activados a distancia (Bergman, 2018)— se observa una continuidad en el uso de tecnología de precisión, empresas pantalla y ataques sin presencia directa. Sin embargo, el caso de los beepers representa una evolución táctica relevante: en lugar de insertar dispositivos en individuos o vehículos, el ataque se centró en los aparatos de comunicación, es decir, en la propia capacidad operativa del adversario. Esta táctica incrementa el impacto psicológico y degrada la cohesión dentro de la organización del Hezbolá al hacer que sus propios medios electrónicos se conviertan en amenazas.

Las implicancias estratégicas del caso son múltiples. Por un lado, demuestra que la guerra encubierta moderna no requiere ya del despliegue convencional ni del uso de armas visibles para lograr efectos letales y desestabilizadores. Por otro, plantea desafíos éticos y legales en torno al uso de medios no militares —beepers y walkie-talkies— como ruta de ataque, en lo que podría constituir una violación del derecho internacional humanitario, tal como lo expresó el Alto Comisionado de las Naciones Unidas para los Derechos Humanos Volker Türk.

Desde el punto de vista doctrinal, la operación también revela una vulnerabilidad estructural de Hezbolá: su inclinación a adoptar soluciones tecnológicas como una estrategia de seguridad consideradas “bajas en riesgo”, motivada por preocupaciones sobre la vulnerabilidad de los teléfonos móviles a la vigilancia israelí, pero sin un adecuado control sobre la cadena de suministro. Esta vulnerabilidad táctica fue muy bien aprovechada por el Mossad con un nivel de sofisticación que supera todas las prácticas documentadas en conflictos previos en la región. La capacidad israelí para anticiparse a las doctrinas de sus adversarios y aprovecharlas mediante ingeniería encubierta se confirma una vez más como un pilar fundamental de su arquitectura de defensa y disuasión.

En cuanto a las limitaciones del estudio, es preciso resaltar que la naturaleza encubierta de todas las operaciones de inteligencia impide el acceso

directo a fuentes primarias o a confirmaciones oficiales. Es por ello que la investigación se basó en fuentes abiertas, lo que, si bien permite una aproximación verosímil, también restringe la profundidad analítica y la validación empírica. Además, las posibles manipulaciones mediáticas o intereses políticos de las fuentes utilizadas constituyen un riesgo metodológico inevitable.

Finalmente, esta investigación abre varias líneas futuras de indagación. Se sugiere profundizar en el análisis de la guerra tecnológica encubierta en el ciberespacio y la cadena de suministro, así como en las estrategias de contrainteligencia de actores no estatales como Hezbolá frente a amenazas de este tipo. Asimismo, es necesario estar al tanto a las nuevas propuestas normativas internacionales que como consecuencia de lo sucedido quieran regular el uso de tecnología de doble aplicación (civil-militar) en conflictos asimétricos, dada su creciente utilización con fines letales y considerando los efectos colaterales.

CONCLUSIONES.

1. Reconfiguración táctica mediante ingeniería encubierta: El Mossad logró explotar una vulnerabilidad como consecuencia de un cambio doctrinal de Hezbolá hacia tecnologías analógicas. Esto confirma la capacidad de las agencias estatales para anticiparse y redirigir doctrinas del enemigo mediante infiltración tecnológica.
2. Innovación operacional sin despliegue militar: La operación validó un modelo de guerra encubierta basado en el uso de tecnología civil manipulada de forma remota, eliminando la necesidad de presencia física o empleo de armamento convencional, y maximizó la letalidad con bajo costo estratégico.
3. Desestabilización de la cohesión operativa adversaria: La destrucción de los medios de comunicación internos dejó un impacto psicológico profundo en Hezbolá, erosionando la confianza en sus propios sistemas de comando y control.
4. Consecuencias geopolíticas y legales emergentes: El incidente desencadenó una ola de condenas internacionales. La calificación de la operación como posible crimen de guerra abre un debate sobre el marco legal aplicable al uso de la tecnología civil como medio letal.
5. Confirmación de una doctrina israelí de guerra tecnológica: El caso corrobora una línea de continuidad en la estrategia del Mossad, evidenciada en operaciones previas como los asesinatos selectivos en Irán, ahora trasladada a una dimensión de sabotaje logístico y tecnológico más difusa y remota.

LIMITACIONES.

Este estudio se basa exclusivamente en fuentes abiertas, lo que restringe el acceso a información clasificada o de primera mano sobre los procesos operativos del Mossad y la respuesta de Hezbolá. Si bien se ha priorizado la triangulación de datos con estándares internacionales de verificación, fuentes oficiales citadas por The New York Times y otros medios, persiste un margen de incertidumbre debido al carácter reservado de las operaciones encubiertas y la posición del Gobierno israelí de no confirmar ni desmentir la autoría de estas operaciones. Asimismo, el análisis se centró principalmente en la dimensión tecnológica y doctrinal, dejando de lado variables geopolíticas y psicológicas que podrían enriquecer la comprensión integral del caso.

RECOMENDACIONES.

1. Profundizar en el análisis de la respuesta doctrinal de Hezbolá frente a la amenaza tecnológica, incorporando fuentes locales o regionales con conocimiento contextual del movimiento.

2. Analizar lo sucedido como un modelo potencialmente aplicable y adaptable por países vecinos como parte de sus estrategias ofensivas/preventivas.

3. Fomentar estudios comparativos con otros casos reales de sabotaje tecnológico (por ejemplo, Stunet o Pegasus) para evaluar patrones comunes en la doctrina israelí y sus efectos disuasivos.

4. Incorporar enfoques interdisciplinarios, que integren la ética aplicada, el derecho internacional y los estudios de seguridad, a fin de lograr un impacto relevante en el ámbito académico y político.

5. Promover el desarrollo de contramedidas técnicas y protocolos de resiliencia para actores estatales y no estatales expuestos a sabotajes logísticos en sus cadenas de suministros.

REFERENCIAS.

Bergman, R. (2018). Rise and Kill First: The Secret History of Israel's Targeted Assassinations [Levántate y mata primero: la historia secreta de los asesinatos selectivos de Israel].

Van Cleave, M. (2007). Counterintelligence and National Strategy [Contrainteligencia y estrategia nacional]. The School for National Security Executive Education (SNSEE) is the newest of the five graduate institutions at the National Defense University (NDU). file:///D:/PERSONAL/Downloads/481685.pdf

Modinger, J. H. (2024, marzo-abril). Spies, Lies, and Algorithms: The History and Future of American Intelligence [Reseña de: A. Zegart, Spies, Lies, and Algorithms]. Military Review, 139–144. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2024/Spies-Lies-Algorithms/

BBC News. (2024, 18 de setiembre). "Las explosiones de los beepers son un golpe devastador para la moral y la capacidad de Hezbolá" ["The explosions of the beepers are a devastating blow to Hezbollah's morale and capacity"]. BBC. https://www.bbc.com/mundo/articles/c4grxylrm0go

BBC News. (2024, 18 de setiembre). "Qué son los beepers y por qué esta tecnología de hace décadas sigue siendo utilizada por Hezbolá" ["What are beepers and why is this decades-old technology still used by Hezbollah?"]. BBC. https://www.bbc.com/mundo/articles/cjwd0xv4997o

BBC News. (2024, 20 de setiembre). "Qué es el Mossad, la agencia de inteligencia de Israel a la que responsabilizan de las explosiones de beepers y walkie-talkies en Líbano" ["What is Mossad, the Israeli intelligence agency blamed for the beeper and walkie-talkie explosions in Lebanon?"]. BBC. https://www.bbc.com/mundo/articles/c2lndxqpyzpo

The New York Times. (2024, 19 de septiembre). "Una nueva era del sabotaje: convertir dispositivos cotidianos en explosivos" https://www.nytimes.com/es/2024/09/19/espanol/mundo/israel-ataque-beepers-hezbola.html

Naciones Unidas. (2024, 20 de setiembre). "Los ataques a través de aparatos personales de comunicación en Líbano violan el derecho internacional, la guerra tiene reglas" https://news.un.org/es/story/2024/09/1532991

BBC News. (2024, 28 de diciembre). "No tenían ni idea de que se los estaban comprando al Mossad": ex agentes israelíes revelan detalles de los sofisticados ataques con beepers que dejaron más de 40 muertos en Líbano. ["They had no idea they were buying them from Mossad": Israeli ex-agents reveal details of the sophisticated beeper attacks that killed over 40 in Lebanon"]. BBC. https://www.bbc.com/mundo/articles/c77jm4g8e65o

Stahl, L. (2025, 8 de junio). "Ex agentes del Mossad israelí detallan cómo construyeron y vendieron buscapersonas explosivos a terroristas de Hezbolá". ["Former agents from Israel's Mossad detail how they built and sold explosive pagers to Hezbollah terrorists"]. 60 Minutes, CBS News. Recuperado de https://www.cbsnews.com/news/israel-former-mossad-agents-detail-explosive-pagers-hezbollah-terrorists-plot-60-minutes-transcript/

Operación Pagers, que se sabe de la acción de Israel y cuáles son sus consecuencias. (2024, septiembre 2024) https://www.patreon.com/posts/operacion-pagers-112300083

López Mezanze, L. B., Gálvez, E. A., & Grosso, R. A. (2024). Guerra híbrida y ciberguerra: El rol de las topologías de red inteligentes en el conflicto Israel–Hezbolá (Trabajo final integrador, Diplomatura Universitaria en Gestión de la Ciberdefensa, Instituto de Ciberdefensa de las Fuerzas Armadas). https://cefadigital.edu.ar/bitstream/1847939/3017/1/TFI%202024%20G3%20GALVEZ-GROSSO-LOPEZ%20MEZANZA.pdf