RIS
Revista de Inteligencia y Seguridad

"ESTUDIOS DE INTELIGENCIA EN EL SIGLO XXI: EVOLUCIÓN DEL CAMPO Y RETOS PARA LA SEGURIDAD"

NÚMERO 5
(ENERO-JUNIO 2026)

ISSN 2992-7455
www.inap.mx/ris

INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

71 AÑOS
MEJORANDO LAS INSTITUCIONES PÚBLICAS
1955 -2026

RIS
Revista de Inteligencia y Seguridad

Número 5
(enero-junio 2026)

"Estudios de inteligencia en el siglo XXI: Evolución del campo y retos para la seguridad"

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

71 AÑOS
MEJORANDO LAS INSTITUCIONES PÚBLICAS
1955 - 2026

Revista de Inteligencia y Seguridad, No. 5, enero-junio 2026, es una publicación semestral digital (www.inap.mx/ris), editada por el Instituto Nacional de Administración Pública, ubicado en Km. 14.5 Carretera México-Toluca No. 2151, Col. Palo Alto, C.P. 05110, Alcaldía de Cuajimalpa, Ciudad de México. Teléfono (55) 5081 2636. www.inap.mx
contacto@inap.org.mx

Editor responsable: Iván Lazcano Gutiérrez
Reserva de Derechos al Uso Exclusivo No. 04-2023-032713274000-102, otorgado por Instituto Nacional del Derecho de Autor.
ISSN: 2992-7455

Consejo Directivo 2026-2029

Eber Omar Betanzos Torres
Presidente

Olga Sánchez Cordero
Vicepresidenta

Rafael Enrique Valenzuela Mendoza
Vicepresidente para los IAPs de los Estados 2026-2027

CONSEJEROS
Arely Gómez González
Indira Isabel García Pérez
Esther Nissán Schoenfeld
Luis Humberto Fernández Fuentes
David Villanueva Lomelí
David Gómez Álvarez
Carlos Iván Moreno Arellano
Sergio Ampudia Mello

Armando Alfonzo Jiménez
Secretario Ejecutivo del INAP

Jessica Eliane Padilla Ramírez
Directora de la Escuela Nacional de Profesionalización Gubernamental

Juan Pablo Pampillo Baliño
Director de Investigación

Ricardo Corral Luna
Director de Consultoría

Luis Armando Carranza Camarena
Director de Administración y Finanzas

CONSEJO DE HONOR
Luis García Cárdenas
José Natividad González Parás
Alejandro Carrillo Castro
José R. Castelazo

IN MEMORIAM
Gabino Fraga Magaña
Gustavo Martínez Cabañas
Andrés Caso Lombardo
Raúl Salinas Lozano
Ignacio Pichardo Pagaza
Adolfo Lugo Verduzco
Carlos Reta Martínez

FUNDADORES

Francisco Apodaca y Osuna
José Attolini Aguirre
Enrique Caamaño Muñoz
Antonio Carrillo Flores
Mario Cordera Pastor
Daniel Escalante Ortega
Gabino Fraga Magaña
Jorge Gaxiola Zendejas
José Iturriaga Sauco
Gilberto Loyo González
Rafael Mancera Ortiz
Antonio Martínez Báez
Lorenzo Mayoral Pardo
Alfredo Navarrete Romero
Alfonso Noriega Cantú
Raúl Ortiz Mena
Manuel Palavicini Piñeiro
Álvaro Rodríguez Reyes
Jesús Rodríguez y Rodríguez
Raúl Salinas Lozano
Andrés Serra Rojas
Catalina Sierra Casasús
Ricardo Torres Gaitán
Rafael Urrutia Millán
Gustavo R. Velasco Adalid

REVISTA DE INTELIGENCIA Y SEGURIDAD
Número 5 (enero-junio 2026)

"Estudios de inteligencia en el siglo XXI: Evolución del campo y retos para la seguridad"

Directora del Número: Dra. Magdalena Alcocer Vega

REVISTA DE INTELIGENCIA Y SEGURIDAD
Número 5
Enero-junio 2026

ÍNDICE

PRESENTACIÓN

La seguridad constituye hoy uno de los pilares fundamentales sobre los que descansa la estabilidad de las instituciones democráticas, el desarrollo de las naciones y la confianza de la ciudadanía en el Estado. En un entorno internacional caracterizado por transformaciones tecnológicas aceleradas, amenazas híbridas, criminalidad transnacional, ciberataques, disputas geopolíticas y una creciente complejidad en los procesos de toma de decisiones públicas, resulta indispensable seguir fortalececiendo las capacidades institucionales del Estado para anticipar riesgos, comprender escenarios y diseñar respuestas sustentadas en el conocimiento.

Desde su fundación, el Instituto Nacional de Administración Pública (INAP) ha asumido el compromiso de promover el conocimiento aplicado a los grandes desafíos del Estado mexicano. Nuestra vocación consiste en robustecer la generación de espacios donde converjen la investigación científica, la reflexión académica y la experiencia profesional para fortalecer la capacidad del servicio público frente a los retos del presente y del futuro. La *Revista de Inteligencia y Seguridad* forma parte de ese esfuerzo permanente por impulsar una cultura de análisis, pensamiento estratégico y formación especializada que contribuya al fortalecimiento de las instituciones.

El quinto número de esta publicación representa un paso significativo en la consolidación de un espacio editorial que, en pocos años, se ha convertido en un referente para personas investigadoras, servidoras públicas, especialistas y estudiantes interesados en los estudios de inteligencia. El tema que articula esta edición, *Estudios de inteligencia en el siglo XXI: evolución del campo y retos para la seguridad*, invita a reflexionar sobre la profunda transformación que ha experimentado esta disciplina y sobre la necesidad de desarrollar enfoques innovadores capaces de responder a escenarios cada vez más dinámicos e interdependientes.

Los trabajos reunidos en este volumen abordan, desde diversas perspectivas teóricas y metodológicas, cuestiones esenciales para comprender la evolución de la inteligencia contemporánea. El lector encontrará reflexiones sobre los nuevos modelos de inteligencia colaborativa, el desarrollo de la enseñanza y la investigación especializada en distintas regiones del mundo, la evolución histórica de la disciplina, los desafíos derivados de los conflictos híbridos y de la protección de los espacios estratégicos, así como el papel que desempeña la inteligencia estratégica en la seguridad nacional del Estado mexicano. En conjunto, estos aportes permiten apreciar la amplitud y riqueza de un campo del conocimiento cuya relevancia continuará creciendo en los próximos años.

En el INAP estamos convencidos de que la generación de conocimiento constituye un componente esencial para el fortalecimiento del Estado. La inteligencia, entendida como una herramienta para reducir la incertidumbre mediante el análisis sistemático de la información, representa una capacidad estratégica que debe desarrollarse con pleno respeto al Estado de derecho, a los derechos humanos, a la legalidad y a los principios democráticos que rigen nuestra vida institucional.

Confío en que las investigaciones que integran este número estimularán nuevas líneas de estudio, enriquecerán el debate especializado y contribuirán a fortalecer la formación de quienes tienen la responsabilidad de analizar, prevenir y enfrentar los desafíos que inciden en la seguridad y el desarrollo nacional.

Reitero mi reconocimiento a la directora de este número, a los integrantes del comité editorial, a las y los autores, así como a todas las personas que hicieron posible esta publicación. Su trabajo confirma que el conocimiento, cuando se construye con rigor académico y vocación de servicio público, constituye una de las herramientas más valiosas para fortalecer nuestras instituciones y contribuir al bienestar de México.

Dr. Eber Omar Betanzos Torres
Presidente del INAP

INTRODUCCIÓN

El presente número tiene distinguidos académicos y profesionales de la inteligencia en el mundo civil y del ejército y de la marina armada. Se intitula "Estudios de Inteligencia", porque la palabra inteligencia sigue despertando suspicacia, desconfianza y confusión aún en diversos sectores. Tuve el honor de dirigir la primera licenciatura en Inteligencia Estratégica desde una universidad privada en México y no dejaba de sorprenderme lo poco que se conoce de este campo de estudios tan rico y tan necesario en el mundo actual. Cualquier curso introductorio de inteligencia apunta al hecho que no existe una definición universal de inteligencia, ya que cada Estado la conceptualiza según sus valores nacionales, su marco institucional y el ethos de su régimen político. No obstante, hay un núcleo común: la inteligencia consiste en la recolección, procesamiento y análisis de información para convertirla en conocimiento útil y accionable orientado a la toma de decisiones en seguridad nacional, especialmente en niveles estratégicos y al más alto nivel en el ámbito público en el poder ejecutivo.

En este proceso, el elemento clave no es solo la acumulación de datos, sino su interpretación crítica por parte de analistas que contextualizan información inevitablemente sesgada. Asimismo, se distingue claramente de espionaje, el cual tiene connotaciones ilícitas, mientras que la inteligencia es una función institucional que otorga una ventaja al tomador de decisiones en un contexto altamente volátil y de incertidumbre. La irrupción de la inteligencia artificial está transformando profundamente el campo de los estudios de inteligencia, al acelerar el procesamiento de datos, redefinir el rol del analista y generar nuevos riesgos de sesgos cognitivos. La inteligencia estratégica se configura como un campo dinámico en expansión que exige mayor rigor epistemológico, supervisión humana y sobre todo control democrático, particularmente a través de mecanismos civiles desde los poderes legislativo y judicial.

En México, las instituciones de educación superior, como el INAP han dejado de ser actores periféricos para convertirse en nodos estratégicos

en la producción, circulación y aplicación del conocimiento vinculado a la seguridad nacional y de los estudios de inteligencia. Este tránsito responde a la intensificación de amenazas transnacionales como la actividad del crimen organizado trasnacional, el terrorismo, la radicalización, ataques cibernéticos, amenazas híbridas; en medio de una reconfiguración del sistema internacional y de una competencia geopolítica por el desarrollo de la inteligencia artificial entre los Estados Unidos y China, que han obligado a una mayor interacción e incluso interdependencia entre la academia, sector privado y de manera limitada con agencias de seguridad del estado mexicano.

El campo de los estudios de inteligencia es aún emergente y en construcción en América Latina y el papel que asuman los centros de estudio y las universidades en su estudio y expansión serán clave para la construcción de una arquitectura sólida de seguridad nacional y de un amento de las capacidades de los estados nacionales en la región.

El primer texto del Cor. Ret. de España, el Mtro. Jesús de Miguel, plantea que la inteligencia tradicional, caracterizada por estructuras cerradas y compartimentadas, resulta insuficiente para enfrentar un entorno contemporáneo definido por la globalización, la interconexión y la complejidad. En este contexto, tanto las agencias estatales como las organizaciones privadas carecen, por sí solas, de las capacidades necesarias para generar la superioridad informativa requerida para la toma de decisiones. A partir de esta premisa, el autor expone la necesidad de transitar hacia un nuevo paradigma de inteligencia colaborativa como un modelo que supera la lógica lineal del ciclo de inteligencia y propone un sistema abierto, dinámico y multidisciplinario en el que múltiples actores —públicos y privados— participan en la generación colectiva de conocimiento.

El artículo del Capitán de Navío de la Armada de la República de Colombia, Ricardo Enrique Sánchez Piedrahita, analiza de manera comparada el desarrollo desigual de los estudios de posgrado en inteligencia entre Norteamérica, Reino Unido, Europa continental y América Latina, identificando una brecha estructural significativa. A partir de un enfoque mixto (revisión de programas 2024–2025 y encuesta a 250 expertos), demuestra que los países anglosajones han consolidado ecosistemas académicos maduros, estrechamente vinculados al Estado y con programas diversificados (académicos y profesionales), mientras que Europa ha optado por una especialización técnica (ciberinteligencia, inteligencia económica). En contraste, América Latina presenta un desarrollo incipiente, con oferta limitada,

concentrada en instituciones militares o policiales y con escasa apertura civil, lo que refleja no solo una diferencia cuantitativa, sino una divergencia cualitativa en términos de institucionalización, orientación curricular y vinculación con la toma de decisiones estratégicas. El autor subraya que fortalecer la formación académica en inteligencia no es solo una necesidad educativa, sino una condición estratégica para mejorar la toma de decisiones, la legitimidad institucional y la autonomía del conocimiento en la región.

El artículo de Álvaro Cremades muestra cómo una práctica tradicionalmente asociada al secreto de Estado se transforma progresivamente en objeto legítimo de análisis científico. El autor resalta que el desarrollo del campo ha estado condicionado por factores externos como el acceso a información, coyunturas políticas y transformaciones institucionales, lo que explica su evolución desigual y su fuerte sesgo angloamericano. A pesar de su consolidación, persisten debilidades estructurales: escasa sistematización teórica, fragmentación metodológica y tensiones entre academia y práctica profesional. En este contexto, el texto plantea desafíos clave como la necesidad de fortalecer su carácter interdisciplinar, superar la hegemonía epistemológica anglosajona y promover agendas regionales, especialmente en América Latina, que contribuyan con enfoques propios y comparativos al desarrollo global del campo.

El texto de Eduardo Zerón, sostiene que México enfrenta una transformación estructural en su entorno de seguridad derivado de la incorporación acelerada de tecnologías geoespaciales y drones por parte del crimen organizado, lo que ha convertido el espacio aéreo en un nuevo dominio estratégico de disputa. El autor argumenta que esta dinámica debe entenderse como un conflicto híbrido en "zona gris", donde las fronteras entre seguridad pública, interior y defensa se diluyen, y donde el problema central no es solo la capacidad criminal, sino la debilidad estructural del Estado, lo que provoca fragmentación institucional, ciclos de inteligencia ineficientes y dependencia estratégica externa.

El artículo de Eduardo Sayavedra plantea que, en el contexto del siglo XXI, la inteligencia estratégica se ha convertido en el pilar indispensable para garantizar la seguridad nacional del Estado mexicano, frente a un entorno caracterizado por alta complejidad, interdependencia global y expansión exponencial de la "dataesfera". En este contexto, el autor argumenta que la seguridad nacional debe replantearse desde una lógica estratégica, preventiva y

multidimensional, donde la inteligencia estratégica funcione como eje articulador de la toma de decisiones. Conceptos como amenazas híbridas y asimétricas explican la forma en que actores estatales y no estatales operan en "zonas grises", combinando medios convencionales y no convencionales para explotar vulnerabilidades estructurales del Estado. Frente a ello, el autor propone fortalecer la inteligencia con una visión de largo plazo, integración interinstitucional, uso intensivo de datos, colaboración público-privada y desarrollo de capital humano especializado.

Magdalena Alcocer Vega*
Coordinadora del número

* Es Doctora en Gobierno y Administración Pública por la Universidad Complutense de Madrid con distinción "Cum Laude". Sus líneas de investigación son los estudios de seguridad y de inteligencia. Tiene un Posgrado en Integración Regional y Relaciones Económicas Internacionales de la Universitat de Barcelona.
Actualmente es Coordinadora de Posgrados en la Facultad de Estudios Globales de la Universidad Anáhuac México, en campus norte, de los programas- Doctorado en Seguridad Internacional y Maestría en Asuntos Internacionales. Es profesora en la Maestría en Inteligencia para la Seguridad Nacional del INAP y dirige tesis de maestría y doctorado en este Instituto.
Fue Asesora de Seguridad Regional para México y Centroamérica en el área de Global Security de Microsoft. Fue Coordinadora de la Licenciatura en Inteligencia Estratégica de la Universidad Anáhuac México y Co-coordinadora del Diplomado en Seguridad e Inteligencia Estratégica de la Universidad de Murcia y la Anáhuac.
Tiene un libro publicado por el INAP en 2019 titulado "Profesionalización de la Policía Federal en el marco de la Iniciativa Mérida 2009-2012". https://share.google/CrZcptorP9BnVBKhH

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

INTELIGENCIA COLABORATIVA

Jesús de Miguel*

Introducción.

La Inteligencia ha sido un área de conocimiento que ha estado tradicionalmente vinculada casi exclusivamente al ámbito estatal y su desarrollo histórico en gran parte ligado al mundo militar. Sin embargo, como sucediera con otros campos, en particular en el de la estrategia, su desarrollo se ha ido extendiendo al ámbito empresarial. Se podría afirmar que en las últimas décadas el sector privado ha ido tomando conciencia de la importancia de la Inteligencia, incorporándola como parte indisociable de los procesos de toma de decisiones de la mayoría de las grandes y medianas empresas.

Las posibles razones que podrían justificar la creciente importancia de esta disciplina en el sector privado radican en su carácter preventivo y en el hecho de ser una función clave en los procesos de toma de decisiones, las que son dos de sus principales señas de identidad. En relación con la primera de ellas, cabría considerar que la prevención está en relación directa con la incertidumbre, siendo una condición esencial para su mitigación adoptar las correspondientes medidas anticipatorias. Por otra parte, para garantizar la necesaria anticipación

* Coronel retirado del Ejército de Tierra de España con 35 años de servicio activo, trayectoria que incluye misiones internacionales en Bosnia, Irak, Líbano y Afganistán, así como el cargo de Agregado de Defensa en México. Posee una sólida formación académica como Diplomado de Estado Mayor y cuenta con diversos másteres en Seguridad y Defensa por universidades de prestigio como la Complutense de Madrid y la de Zaragoza. Durante su estancia en México (2014-2019), destacó como asesor de las Secretarías de Defensa y Marina, además de ejercer cargos directivos en el sector privado y centros de investigación naval. Actualmente reside en España, donde combina la consultoría estratégica en Two Worlds Collaborative Intelligence con la docencia en la Universidad de Murcia y la Universidad Anáhuac, consolidándose además como un prolífico autor de libros especializados en inteligencia estratégica y entornos complejos.

será necesario contar con una superioridad informativa, lo que permitirá alcanzar una ventaja estratégica.

Estrategia e Inteligencia son dos áreas de conocimiento profundamente interconectadas, no en vano la mencionada superioridad informativa es una condición *sine qua non* para alcanzar la ventaja estratégica, lo que la vincula a la segunda de las características citadas, su vinculación a las tomas de decisiones. Por ello, la Inteligencia como función en el ámbito de las organizaciones debe superar la abstracción para, de ese modo, poder generar un conocimiento útil que apoye las necesidades de los decisores (político, militar, empresarial, etc.).

La trascendencia de la Inteligencia se ve aún más reforzada si tenemos en cuenta el actual contexto internacional, el cual se podría considerar modulado, entre otros, por los factores que se citan a continuación. En primer lugar, por la influencia de la *globalización*, la cual hace que los efectos que generan muchos de los desafíos y problemas adquieran una dimensión global. Un ejemplo de ello se puede apreciar en el conflicto en Irán, cuyas repercusiones en los mercados y el comercio tienen una consecuencia directa en la economía mundial. Un segundo factor es el de la *interconexión*, fenómeno relacionado directamente con el desarrollo exponencial de la comunicación y la computarización, lo que para las organizaciones supone el acceso a unos ingentes volúmenes de información de gran dificultad para su gestión eficiente. En tercer lugar, otra de las variables es precisamente la *complejidad* del entorno, considerado como un sistema abierto, siendo una condición inseparable este tipo de sistemas en los que se multiplican exponencialmente el número de actores, las relaciones y los procesos. Estos tres factores contribuyen a configurar un contexto de gran volatilidad, lo que complicará los procesos de toma de decisiones, realzando la importancia de contar con un modelo de Inteligencia que dé respuesta a los múltiples retos a los que se enfrentan las organizaciones.

De acuerdo con lo anterior es fácil inferir la necesidad que tiene todo tipo de estructura organizacional de contar con la función de Inteligencia, con independencia de su tamaño y de su condición público o privada, solamente así podrán preservar sus intereses y alcanzar la requerida ventaja estratégica y competitiva. En síntesis, la Inteligencia es un área de conocimiento indispensable en el ámbito institucional y en el empresarial, en la que no caben la falta de rigor ni la improvisación, cuyo desarrollo debe de estar sustentado en unos

principios y procedimientos sistémicos que requiere contar con personas capacitadas y dotada de los medios y recursos adecuados.

Admitida la importancia y necesidad de la Inteligencia, De Miguel propone plantear dos preguntas clave [1] : *¿disponen las organizaciones/agencias de inteligencia de las capacidades necesarias para enfrentar este entorno global, interconectado, complejo e incierto?*, y, como segunda cuestión, llevando este problema al mundo empresarial, *¿pueden todas las empresas contar con su propio departamento de inteligencia?* Se podría afirmar que las respuestas a ambas preguntas son negativas, por un lado, las agencias se ven desbordadas hoy en día por el hecho de que las principales amenazas a las que se enfrentan se corresponden con sistemas abiertos, y, por otra parte, las corporaciones privadas no solo no disponen de recursos para disponer de la Inteligencia requerida para cubrir todo el espectro de sus actividades.

Admitida esta vulnerabilidad, cabría una tercera pregunta: *¿cómo alcanzar la necesaria superioridad informativa?* Para responderla, se propone comenzar con una reflexión recordando una frase que ha prevalecido tradicionalmente entre los tomadores de decisiones, *"la información es poder"*. Este enfoque ha conducido a la Inteligencia a una preocupante situación de estanqueidad, y si lo cual pudo ser aceptable en otros momentos, en el mundo en el que vivimos resulta totalmente inoperativo. Baste tomar como ejemplo tres situaciones bien conocidas como fueron los primeros atentados terroristas del nuevo modelo del terrorismo internacional que implantó Al Qaeda, como fueron los de Nueva York y Washington en 2001, los de Madrid en 2004, o los de Londres un año después, en los tres ataques terroristas las diferentes agencias nacionales apenas compartieron sus informaciones. Así pues esta función crítica se tiene que mover hoy en día en un escenario completamente diferente, en el cual, conviniendo que esta actividad está orientada a la generación del conocimiento, la idea fuerza que debe de prevalecer es la necesidad de compartir: *"cuanto más compartamos más tendremos"*.

A la vista de las respuestas a estas tres preguntas pareciera que el modelo tradicional de la Inteligencia no se ajusta a las características del contexto actual y precisa de un nuevo enfoque que permita alcanzar una mayor eficiencia entre las necesidades y las respuestas (productos).

[1] De Miguel, 2024

Como corolario a esta introducción se desprende la necesidad que tienen las organizaciones de contar con la Inteligencia como una función transversal y que para alcanzar la requerida eficacia y eficiencia el modelo a adoptar debe de estar basado en la colaboración y en la ventaja que aportar compartir el conocimiento de manera oportuna. Lo que, como se verá a lo largo del Capítulo se corresponde con el modelo de la Inteligencia Colaborativa.

Antecedentes y desarrollo del modelo de Inteligencia Colaborativa.

¿POR QUÉ FALLÓ LA INTELIGENCIA EN LOS ATENTADOS DEL 11S?

Resulta especialmente relevante analizar por qué, a pesar de la existencia de múltiples indicios y advertencias previas, el sistema de inteligencia de Estados Unidos no logró prevenir los atentados del 11 de septiembre de 2001. A diferencia de otros fallos puntuales, el 11S constituye un caso paradigmático de fallo sistémico, en el que confluyeron deficiencias estructurales, organizativas y analíticas. La amenaza del terrorismo yihadista ya había sido identificada como prioritaria, pero la incapacidad para integrar, interpretar y actuar sobre la información disponible derivó en una falla crítica del sistema. De manera esquemática, pueden señalarse las siguientes causas:

1. *Inadecuada valoración de la amenaza*. Aunque Al Qaeda era considerada una amenaza relevante, no se anticipó correctamente su capacidad ni su intención de ejecutar ataques de gran escala en territorio estadounidense. Persistía una percepción centrada en atentados en el exterior.
2. *Fragmentación del sistema de inteligencia*. La información relevante estaba distribuida entre agencias como la CIA y el FBI, sin mecanismos eficaces de integración. Esta compartimentación impidió construir una visión completa de la amenaza.
3. *Deficiencias en la coordinación entre las agencias de inteligencia*. La ausencia de protocolos efectivos de cooperación y el predominio de culturas organizativas diferenciadas dificultaron el intercambio fluido de información crítica, generando vacíos operativos.
4. *Fallo en la explotación de indicios tácticos*. Existían señales concretas —como la presencia de individuos vinculados a redes yihadistas en territorio estadounidense o el interés en formación aeronáutica— que no fueron adecuadamente analizadas ni conectadas entre sí.
5. Incorrecto análisis de inteligencia. La información disponible no fue oportunamente interpretada en términos de amenaza inminente. Se produjo un fallo en la conversión de datos en inteligencia accionable, evidenciando déficits en el ciclo analítico. La inteligencia no logró anticipar la innovación operativa del adversario.
6. *Debilidades en la seguridad interna*. Las vulnerabilidades del sistema de aviación civil eran conocidas, pero no fueron corregidas con la suficiente urgencia, facilitando la ejecución material de los atentados.
7. *Desconexión entre inteligencia y decisión política*. A pesar de advertencias elevadas a los niveles decisores, como el informe presidencial de agosto de 2001 ("Bin Laden Determined to Strike in U.S."), no se adoptaron medidas proporcionales a la gravedad de la amenaza.

Ilustración 1. Cuadro resúmen Fallos Inteligencia 11S

Como se exponía en la introducción, la inteligencia tradicional no responde a la complejidad del mundo actual, abriendo la necesidad de acometer un cambio profundo, lo que se hizo más evidente con la irrupción del modelo del terrorismo internacional de la mano de Al Qaeda.

En el cuadro de la Ilustración 1 se muestran algunas de las principales razones por las que la Inteligencia no permitió anticipar los atentados del 11 de septiembre de 2001.[2] Circunscribir este error a una simple ausencia de información sería simplista y no respondería a una realidad mucho más grave. El problema identificado se corresponde con la incapacidad del sistema para integrar, analizar y traducir la información en un producto de inteligencia que permita adoptar las acciones preventivas eficaces. Es decir, se podría inferir se trata de una disfunción estructural y procedimental.

Los atentados del 11S pueden ser considerados como un punto de inflexión en el contexto de la seguridad internacional, lo que iba a obligar a los decisores políticos a adoptar profundos cambios en muchos campos, siendo uno de ellos la Inteligencia. Clark pone el foco de los fallos de Inteligencia principalmente en los procesos de análisis y en la oportunidad de su difusión, poniendo el énfasis en la necesidad de colaborar y compartir. El citado autor identifica tres problemas principales.[3]

1º. *No compartir información*. Aunque se ha avanzado mucho en este campo, sigue existiendo la tendencia a circunscribir la Inteligencia en compartimentos estancos, a pesar de que los actuales escenarios requieren manejar inmensos volúmenes de información procedentes de fuentes diversas, para lo que ninguna organización dispone de las capacidades para dar respuesta de manera autónoma. Al contrario, se precisa compartir, lo que no quiere decir que la Inteligencia está abocada a perder la discreción y confidencialidad, evidentemente nada más lejos de la realidad, la colaboración en el acceso a la Inteligencia se realiza en el marco de un principio básico: la *"necesidad de conocer"*, de manera que solamente se puede acceder a la información, siempre con las debidas garantías de seguridad y confidencialidad, en función de

[2] National Commission on Terrorist Attacks Upon the United States, 2004; y Central Intelligence Agency, 2005
[3] Clark, 2017

que lo precise una organización o un puesto dentro de ella y en un entorno temporal determinado.

2º. *No analizar de manera objetiva*. Esta disfunción analítica se encuentra íntimamente vinculada con los sesgos cognitivos, siendo éstos unas de las causas más notables de las que se derivan los errores en el campo de la Inteligencia. Además, la complejidad del entorno exige una mayor especialización del análisis, lo que abunda en la mayor necesidad de contar con un modelo colaborativo de la Inteligencia

3º. *El destinatario de la Inteligencia no la explota de manera oportuna y eficiente*. Es necesario asumir que el receptor de la información elaborada forma parte del *ciclo de inteligencia*, por una parte, señalando sus necesidades identificadas en este campo, pero también, y no menos importante, como destinatario para explotar el conocimiento, y, de este modo, sustentar de manera realista, oportuna y eficaz las decisiones. Esta disfunción no es atribuible de manera exclusiva a los responsables de la obtención o del análisis de la información, sino también, y en la misma medida, a los propios tomadores de decisiones. Este punto abunda en la necesidad de contar con una *cultura de inteligencia* en las organizaciones, algo, por otra parte, que, en opinión del autor, se encuentra muy lejos de la realidad en la mayoría de las empresas e incluso en algunas instituciones.

Estados Unidos ha liderado el cambio en el mundo de la Inteligencia, utilizando para ello la experiencia adquirida en los escenarios de lucha contra la insurgencia en Irak y Afganistán. El nuevo enfoque es lo que se conoce como *"Modelo de Dominio de Inteligencia"* (IDM, por sus siglas en inglés).[4] Su principal elemento diferenciador consiste en desarrollar el conocimiento local para permitir que las fuerzas operativas militares y/o policiales debiliten, desarticulen y neutralicen los desafíos que plantean los grupos armados a la autoridad gubernamental, dentro de los límites del Estado de derecho.

[4] Godson, 2012

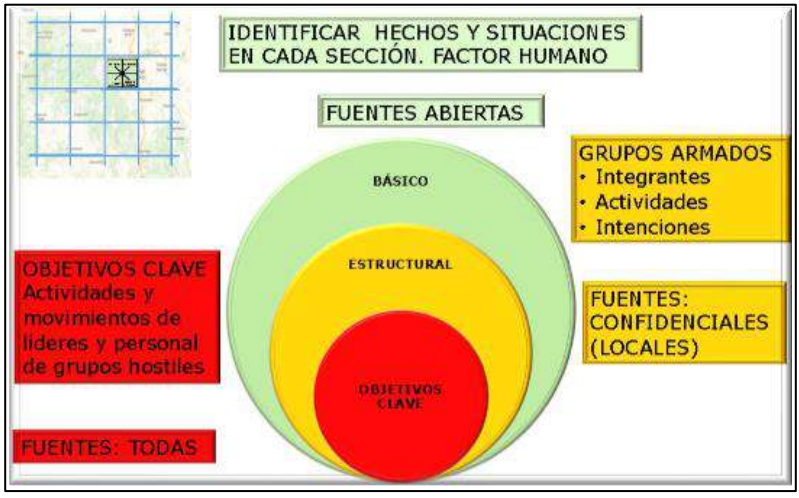


Ilustración 2. Esquema Dominio de Inteligencia. Elaboración propia

La característica clave este enfoque, y que supone su principal innovación, radica en el desarrollo de un conocimiento sistemático en el nivel local. Se articula en tres círculos concéntricos (dominios), el más amplio es el que se corresponde con la inteligencia básica. Se trata con ella de analizar el entorno general en el que se mueve una organización, identificando aquellos hechos y/o situaciones que son susceptibles de afectarla potencialmente. El segundo dominio se refiere a los actores/estructuras que componen el *terreno humano*[5] en el que las organizaciones desarrollan su actividad, o entorno específico. El tercer dominio, el de menor extensión, pero de gran importancia, se dirige hacia aquellos objetivos prioritarios (líderes, movimientos, actividades, etc.) que pueden afectar a las organizaciones. El primero de los dominios citados fundamenta la obtención en las fuentes abiertas, los otros dos requerirán una adecuada combinación de otro tipo de fuentes, en particular las humanas, de señales, geoespacial, documental, etc.

Este modelo aplicado en el marco empresarial permite determinar impacto de las actividades de una empresa y/o corporación en un

[5] Esta expresión fue acuñada por el Ejército de Estados Unidos en el marco de la lucha contra la insurgencia en Afganistán, pudiendo ser definida como el conjunto de factores sociales, culturales, políticos y psicológicos que caracterizan a una población en un entorno determinado y que condicionan su comportamiento, percepciones y relaciones, influyendo de manera decisiva en el desarrollo y resultado de cualquier acción estratégica.

entorno determinado, implantar un determinado producto e identificar posibles competidores y/o adversarios (*stakeholders*), es decir, identificar los aspectos relacionados con la competencia, evitando de este modo los efectos no deseados.

En lo que se refiere a la explotación de la Inteligencia, este modelo también introduce un elemento innovador de la mano de la *fusión de la inte*ligencia, entendida como un proceso integrador que permite transformar información dispersa y heterogénea procedente de múltiples fuentes y disciplinas en conocimiento estructurado, orientado a la anticipación y a la toma de decisiones en entornos complejos. Este proceso se ve significativamente potenciado por el desarrollo tecnológico, en particular por la consolidación de arquitecturas digitales distribuidas que permiten el almacenamiento, procesamiento y explotación de grandes volúmenes de información. Este patrón de "*inteligencia en la nube*" es en sí mismo un facilitador esencial, al posibilitar el acceso compartido a información estructurada, actualizada y disponible en tiempo casi real, superando las limitaciones tradicionales derivadas de la compartimentación de los sistemas de inteligencia.

Por otra parte, para superar la rigidez del ciclo de inteligencia clásico en lo que respecta a la difusión, este modelo se apoya en el citado principio de "*necesidad de conocer*" (*need to know*), el cual, sin abandonar los fundamentos de seguridad y control, se adapta a entornos más dinámicos, en los que la inteligencia puede ser accesible de manera inmediata para aquellos actores que, estando debidamente autorizados, la requieren para el desempeño de sus funciones. De este modo, se transita desde modelos restrictivos basados en la retención de la información hacia esquemas más flexibles, en los que prima su circulación controlada, apoyada en mecanismos avanzados de gestión de accesos, autenticación y trazabilidad.

Este cambio de paradigma de la función de inteligencia sienta las bases de un modelo en el que la colaboración es esencial, en la idea de compartir el conocimiento de manera sistémica entre múltiples actores.

Inteligencia Colaborativa. Descripción del concepto.

Como punto de partida se podría afirmar que la Inteligencia Colaborativa constituye una evolución necesaria de esta función con el objeto de garantizar la superioridad informativa en entornos complejos. Sin embargo, este cambio debe entenderse como una

profunda transformación en la propia concepción de la Inteligencia, evitando centrarse únicamente en la mejora o adaptación de los procesos existentes.

En los modelos, centrados en el ciclo tradicional de inteligencia, incluso en esquemas más avanzados basados en la fusión de la información, este nuevo enfoque colaborativo introduce como elemento diferenciador el de la generación de conocimiento, fruto de la interacción entre múltiples actores. De este modo, su verdadero valor supera la simple capacidad de integrar información, para constituirse como un referente para la articulación del conocimiento, permitiendo así compartir, contrastar y explotar la Inteligencia de manera colectiva.

Este enfoque responde directamente a las limitaciones identificadas para los modelos tradicionales, particularmente en lo que se refiere a la fragmentación de la información, la insuficiente capacidad analítica individual y las deficiencias en la difusión y explotación del conocimiento, proponiendo un sistema más abierto, dinámico y adaptativo. De este modo, la Inteligencia deja de ser un producto estático para convertirse en un proceso continuo de construcción colectiva del conocimiento, orientado a mejorar la anticipación y la toma de decisiones en contextos caracterizados por la incertidumbre y la complejidad.

> *La Inteligencia Colaborativa representa una lógica de funcionamiento que redefine la relación entre información, conocimiento y decisión.*

La Inteligencia como ciencia se sustenta en el conocimiento especializado y en la experiencia compartida. Como arte, se apoya en dos de las que son sus características existenciales, la innovación y la adaptación. Desde esta doble perspectiva -ciencia y arte- nos aproximaremos a la colaboración en el campo de la Inteligencia.

Partiendo de la premisa fundamental de que la colaboración es un término que supera el ámbito de lo colectivo cabe preguntarse para qué y por qué colaborar. Pero, antes de abordar las condiciones que la hacen posible, conviene detenerse en una cuestión previa de carácter estructural, como es la creciente dificultad para generar conocimiento útil de manera autónoma en entornos caracterizados por la sobreabundancia informativa y la complejidad sistémica.

En efecto, el desarrollo exponencial de las tecnologías de la información ha multiplicado tanto el volumen de datos disponibles

como la velocidad a la que estos se generan y difunden. Sin embargo, este incremento cuantitativo no se traduce necesariamente en una mejora cualitativa del conocimiento. Por el contrario, introduce nuevas fricciones en el proceso analítico, al exigir mayores capacidades de filtrado, contextualización e interpretación. En este escenario, el acceso a la información deja de ser un problema para la Inteligencia, mientras que su procesamiento y consecuente transformación en conocimiento explotable pasan a ser el verdadero desafío para superar.

A esta realidad se añade la progresiva multidimensionalidad de los fenómenos que afectan a la seguridad y a la actividad de las organizaciones, como un segundo factor de naturaleza estructural. Los riesgos y las amenazas requieren aproximaciones integrales que combinen dimensiones políticas, económicas, sociales, tecnológicas y culturales, y no una simple perspectiva disciplinar. Lo que introduce un factor limitativo muy importante, por cuanto ninguna organización, por sí sola, dispone de todas las capacidades necesarias para abarcar de manera completa todo el espectro analítico que conforma la complejidad.

Como consecuencia de ambos factores, sobrecarga informativa y complejidad multidimensional, se produce una tensión creciente entre las necesidades de inteligencia y las capacidades disponibles para satisfacerlas. Esta brecha obliga a replantear los modelos tradicionales, basados en estructuras relativamente cerradas y autosuficientes, para evolucionar hacia esquemas más abiertos en los que el conocimiento se construya de manera compartida.

Desde esta perspectiva, la colaboración deja de ser una opción para convertirse en una necesidad estructural. No se trata únicamente de sumar capacidades, sino de articularlas de forma que permitan generar un conocimiento más robusto, contrastado y adaptado a la naturaleza de los problemas a los que se enfrentan las organizaciones. Es en este marco donde cobra sentido analizar las condiciones que hacen posible dicha colaboración y las formas que puede adoptar en la práctica.

La respuesta a las cuestiones planteadas -por qué y para qué colaborar-, a la vista de lo anteriormente expuesto, adquieren una mayor claridad. Se colabora, en primer lugar, porque ninguna organización dispone de manera autónoma de las capacidades necesarias para comprender y gestionar entornos caracterizados por la complejidad, la interdependencia y la sobrecarga informativa. En segundo término, la colaboración es necesaria para generar un conocimiento de mayor

calidad, más contrastado y eficiente, que permita reducir la incertidumbre y mejorar la eficacia en la toma de decisiones.

Este modelo colaborativo constituye, por tanto, un elemento esencial para la generación de inteligencia en los contextos actuales. Ahora bien, asumir su necesidad no resuelve por sí mismo el problema fundamental de cómo articular dicha colaboración de manera efectiva. Esta cuestión remite directamente a la configuración, el funcionamiento y el rendimiento de los equipos y estructuras colaborativas, en otras palabras, disponer de un modelo sistémico de colaboración.

De acuerdo con lo hasta aquí expuesto, se podría afirmar que la Inteligencia Colaborativa representa una reformulación de los fundamentos de los modelos tradicionales de la Inteligencia, respondiendo su configuración a una serie de principios rectores que orientan tanto su diseño como su funcionamiento.

En primer lugar, la interdependencia estructural se configura como un elemento definitorio del modelo. La creciente complejidad de los entornos en los que operan las organizaciones impide que la generación de inteligencia pueda realizarse de manera autónoma, requiriendo la integración de capacidades distribuidas entre múltiples actores. En segundo término, la integración multidisciplinar se presenta como una condición necesaria para abordar fenómenos de naturaleza transversal, cuya comprensión exige la convergencia de distintos ámbitos de conocimiento. A ello se suma la circulación controlada de la información, que implica la superación de modelos excesivamente restrictivos basados en la retención, para evolucionar hacia esquemas más flexibles en los que la información fluye de manera segura entre los actores autorizados. Finalmente, su contribución a generar un conocimiento compartido y su orientación a la toma de decisiones constituyen los ejes sobre los que se articula el valor diferencial del modelo, al situar la interacción como mecanismo generador de inteligencia útil.

La Inteligencia Colaborativa puede ser entendida como un sistema estructurado que se articula en distintos niveles. En el plano organizativo, integra una pluralidad de actores de naturaleza pública y privada los cuales desempeñan cometidos diferenciados en el ciclo de inteligencia. En el plano funcional, el modelo se apoya en los procesos de obtención, integración y análisis de la información, junto a los de

difusión y explotación, superando la lógica secuencial tradicional del ciclo de inteligencia.

Por su parte, el plano tecnológico actúa como facilitador esencial del sistema, a través de plataformas compartidas, arquitecturas digitales distribuidas y mecanismos avanzados de gestión de accesos, que permiten el tratamiento eficiente de grandes volúmenes de información y su disponibilidad en tiempo casi real.

Aplicación de los mecanismos de colaboración a la Inteligencia.

Como primer paso es importante señalar las diferencias entre el trabajo en equipo y la colaboración, a este fin Hackman[6] se formula una serie de cuestiones, de las que se han seleccionado las que se refieren a las diferentes manifestaciones del trabajo colaborativo y a la oportunidad de recurrir a la conformación de equipos. Las respuestas permitirán establecer de una manera clara su diferenciación entre ambas modalidades de trabajo e incluso del modelo colectivo.[7]

1º. *¿Qué se entiende por un equipo?* Se podría afirmar que la colaboración en el campo de la Inteligencia se manifiesta como un *continuum*, adoptando una gran variedad de formas, como se exponen a continuación. De las siete opciones abajo planteadas solamente las tres centrales responderían propiamente al modelo colaborativo, los dos primeros se corresponderían con situaciones específicas más próximas a lo que podría asociarse a la inteligencia colectiva, mientras que los dos últimos se orientan a la organización de equipos organizacionales, superando, en consecuencia, el ámbito de la colaboración inter agencias.

2º.

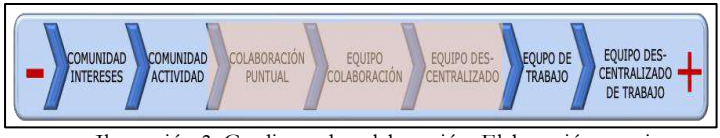


Ilustración 3. Gradiente de colaboración. Elaboración propia

Lo anterior se muestra gráficamente (Ilustración 3) en un gradiente basado en la fortaleza de los equipos. Esta articulación de los grupos en función de su menor o mayor robustez no responde a un modelo

[6] Hackman, 2011
[7] De Miguel, 2024

rígido, sino que puede ir evolucionando de un tipo a otro en función de las necesidades e intereses de la organización.

- Comunidad de intereses. Se limita a la participación en reuniones y eventos en los que se pueden intercambiar observaciones y opiniones sobre intereses compartidos. Ejemplo de ellos serían los foros sobre el terrorismo, el crimen organizado, el desarrollo humano, etc.
- Comunidad relacionada con una determinada actividad. Esta forma de colaboración se refiere a los espacios en los que pueden interactuar grupos profesionales con intereses afines, recabando apoyos o incluso construyendo proyectos comunes. Se podría identificar con este patrón a la *"comunidad de inteligencia"*, la cual no responde a una organización formal pero la mayoría de las organizaciones en este campo tienen formación, objetivos, procedimientos, y, en no pocas ocasiones, intereses comunes.
- Colaboración puntual. Se produce cuando concurren e interactúan diferentes agencias y organizaciones (consultoras de inteligencia) que poseen información diversa y que puede contribuir a consolidar el conocimiento sobre un tema emergente.
- Equipos de colaboración. Es la relación que se establece entre dos agencias u organizaciones de inteligencia para desarrollar un proyecto sin que exista una responsabilidad compartida en el resultado final.
- Equipos descentralizados. Se trata de un caso de mayor alcance y de permanencia en el tiempo que el anterior, en el que los equipos, grupos u organizaciones no comparten un espacio físico de trabajo e incluso no mantienen contactos personales regulares, pero que desarrollan de una manera sistemática su actividad de manera remota a través de las redes de información.
- Equipo de trabajo. Es el que se constituye entre varios individuos o, en su caso entre organizaciones, para llevar a cabo un trabajo específico, normalmente por tiempo limitado. Tiene una estructura organizativa y unas responsabilidades definidas para cada uno de sus elementos. Un ejemplo de este tipo de asociación es lo que en términos militares se conoce por su expresión inglesa de *Task Force*.

- Equipo semipermanente de trabajo. Puede ser considerado como una variación del anterior para períodos de tiempo prolongados.

En el cuadro adjunto se muestran algunos ejemplos de la aplicación de estos modelos de colaboración al campo de la Inteligencia Colaborativa en el ámbito empresarial.

MODELOS COLABORATIVOS EN EL ÁMBITO EMPRESARIAL

De los modelos colaborativos descritos los tres centrales constituyen la esencia de la Inteligencia Colaborativa en el ámbito empresarial. Se presentan a continuación algunos ejemplos basados en experiencias profesionales del autor de este capítulo

- Colaboración puntual. Empresas especializadas en inteligencia en diversos campos ofrecen a un determinado cliente un producto propio y especializado. Ejemplo de ello sería el caso de la empresa A que aporta sus capacidades de análisis geopolítico para generar un informe de riesgo país con la finalidad de apoyar expansión de negocio de un determinado cliente. Simultáneamente, y sin que exista una relación entre ellas, la empresa B, especializada en inteligencia competitiva, proporciona al mismo cliente un informe de "*due dilligence*"[1] sobre un determinado colaborador en el país de destino. En este caso la relación responde a una necesidad específica y la colaboración se materializa de manera unidireccional entre los proveedores (inteligencia) y el cliente.
- Equipos de colaboración. Una organización empresarial precisa los servicios de inteligencia para un determinado proyecto. En este supuesto, el departamento de seguridad corporativa de una compañía contrata los servicios de una empresa para la activación de un servicio de vigilancia e inteligencia con el objeto de detectar situaciones que pudieran afectar a la viabilidad de un determinado proyecto y a la reputación empresarial. Como condición esencial para el éxito del proyecto, la colaboración debe de estar basada en una detallada coordinación y precisa además de una continua interacción entre ambas organizaciones. A diferencia de la colaboración puntual, en este tipo de relación, la colaboración se materializa adopta la forma bidireccional cliente y proveedor.
- Equipos descentralizados. Este modelo de colaboración es una variante del anterior, pero con un mayor alcance y extensión en el tiempo. Este caso supone la concurrencia de una o varias organizaciones empresariales del área de inteligencia con diferente especialización, las cuales ofrecen soluciones integrales de seguridad e inteligencia. Un ejemplo de equipos descentralizados podría ser la contratación por el departamento de seguridad corporativa de un grupo de empresas especializadas que, bajo un modelo "*joint venture*"[2], ofrecen soluciones de vigilancia e inteligencia, gestión de crisis y ciberseguridad. Como en el caso anterior, la relación se establece en la doble dirección entre las empresas proveedoras y el cliente, aunque su permanencia suele ir más allá de la duración de un determinado proyecto.

1. Proceso de investigación para evaluar riesgos y tomar decisiones informadas en una operación.
2. Acuerdo estratégico entre dos o más partes para crear y gestionar conjuntamente una entidad o proyecto, compartiendo recursos, riesgos y beneficios.

Ilustración 4. Modelos colaborativos aplicados al sector empresarial

3º. ¿Cuándo se estima oportuna la creación de un equipo y cuándo sería la última opción por considerar? Más allá del tipo de colaboración del que estemos hablando hay que resaltar que los equipos tienen normalmente más recursos que un individuo trabajando de

manera autónoma, así como una mayor flexibilidad para adaptarse a los cambios de situación.

Sin embargo, la conformación de equipos no constituye en sí mismo una solución con carácter universal, ni necesariamente óptima en todos los contextos organizativos. En determinados supuestos, lejos de incrementar la eficacia, puede introducir fricciones adicionales que comprometan el resultado final, como sería el caso, por ejemplo, los de producir costes de extraordinarios en la coordinación, o bien, provocar la difusión de responsabilidades o introducir disfunciones en las tomas de decisiones, por citar algunos ejemplos. Desde esta perspectiva, la decisión de articular un equipo debe sustentarse en un análisis previo de su verdadera necesidad y utilidad.

Siguiendo el enfoque de Hackman,[8] la oportunidad de constituir un equipo se justifica únicamente cuando concurren condiciones específicas, entre las que se podrían enumerar, en primer lugar, cuando la naturaleza de la tarea excede la capacidad de un individuo, bien por la magnitud de los recursos requeridos, bien por la necesidad de integrar competencias, conocimientos o perspectivas diversas; y, en segundo término, cuando la interacción entre sus miembros genera un valor añadido tangible, ya sea en términos de calidad del resultado o de desarrollo de capacidades relevantes para la organización.

En consecuencia, la creación de equipos debe entenderse como una decisión estratégica y no como una práctica rutinaria. Solo resulta plenamente justificable cuando su aportación diferencial es clara, medible y superior a la que podría obtenerse mediante la actuación individual, evitando así incurrir en estructuras colaborativas que, lejos de optimizar el desempeño, introduzcan complejidad innecesaria.

Impacto de las tecnologías en la Inteligencia Colaborativa.

Siguiendo con la descripción del modelo de Inteligencia Colaborativa, si hasta aquí se ha referido la que es su principal seña de identidad -la necesidad de compartir-, a continuación, se acomete su relación con el *desarrollo tecnológico*, el cual no debe ser entendido únicamente como un facilitador, sino como una condición habilitadora y configuradora del

[8] Ibídem

propio modelo. El desarrollo de las tecnologías de la información y la comunicación, junto con las capacidades avanzadas de procesamiento de datos, ha permitido la transición desde estructuras jerárquicas tradicionales hacia modelos de inteligencia en red, en los que la generación, integración y difusión del conocimiento se realiza de manera distribuida. En este contexto, las plataformas compartidas, las arquitecturas digitales distribuidas y las capacidades analíticas avanzadas, incluyendo el tratamiento masivo de fuentes abiertas y el uso de inteligencia artificial, optimizan los procesos y facilitan el marco colaborativo.

Volviendo al esquema de Dominio de Inteligencia (Ilustración 2), de los tres ámbitos en los que se articula es en el primero de ellos -nivel básico- dónde se conforma el entorno general, en el que Inteligencia Colaborativa se configura como un excelente instrumento, en buena parte como consecuencia del importante desarrollo tecnológico acaecido en las últimas décadas, lo que permite contar con importantes recursos tecnológicos, habida cuenta de los grandes volúmenes de información que se manejan.

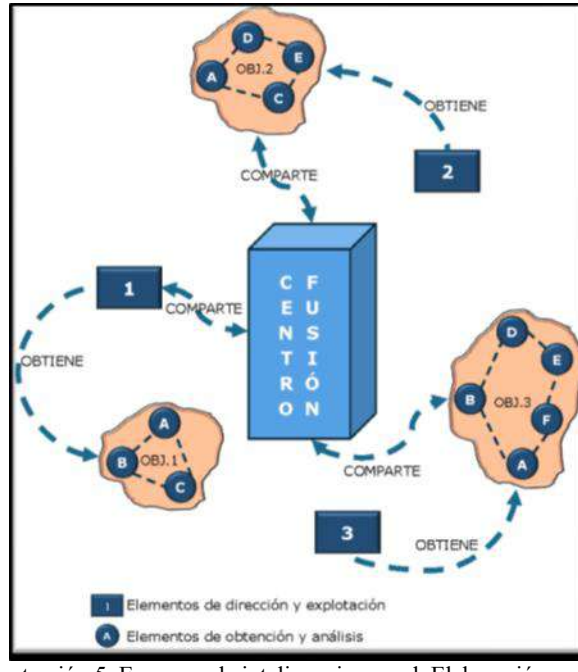


Ilustración 5. Esquema de inteligencia en red. Elaboración propia

Causa y efecto de la relación existente entre la Inteligencia y la tecnología motiva la necesidad que se adopten estructuras que rompan el típico modelo jerárquico de otras épocas, para transitar hacia un esquema de "*inteligencia en red*". Para describir este enfoque reticular se tomará en cuenta a los actores, los procesos y las fuentes. Si nos referimos a los primeros, se deberían distinguir aquellos relacionados con la dirección y la explotación del conocimiento -los tomadores de decisiones- y los que su actividad se concentra en la obtención de información por diferentes fuentes y su posterior análisis. Este segundo grupo se caracteriza por la concurrencia de varias unidades especializadas en distintos campos que comparten su conocimiento sobre el objetivo en diferentes ámbitos. El actual desarrollo tecnológico, en particular en las áreas de comunicación y computación, aporta una invaluable ventaja a los modelos colaborativos en los que las unidades de obtención y análisis desarrollan sus cometidos de manera remota y con cierto grado de descentralización.

Para dimensionar apropiadamente el impacto que la tecnología tiene en los procesos aconseja centrar el estudio en los procesos de obtención y difusión por ser los que posiblemente aporten el valor más diferenciador de la Inteligencia Colaborativa frente a otros modelos de abordar esta fusión. Con ello no se pretende restar la importancia del resto de los procesos que se desarrollan en un sistema de inteligencia, sino que su descripción, además excede del alcance de este Capítulo. Por una parte, los procesos directivos están orientados fundamentalmente a la determinación de las necesidades de inteligencia y a la explotación de los resultados; por su parte los correspondientes al análisis de la información, que podría consverdadero motor del sistema de inteligencia), cuya descripción excede del alcance de este capítulo, para centrarnos en las repercusiones de la tecnología sobre los otros dos, la obtención y la difusión.

Se puede considerar pues que el modelo de Inteligencia Colaborativa se ve fuertemente facilitado por los referidos avances tecnológicos. Hoy en día es un hecho que la facilidad para acceder a inmensos volúmenes de información no se corresponde con la capacidad de procesarla y analizarla sin el auxilio de las tecnologías relacionadas con ella, siendo necesario, en consecuencia, recurrir a una equilibrada relación entre el elemento humano y tecnológico.

En el proceso de obtención intervienen una red de elementos que interactúan permanentemente, en el que se materializa un equilibrio ponderado entre, por una parte, la explotación de fuentes y el análisis

de la información adquirida y, por otra, la capacidad de compartir. Las tecnologías de la información facilitan este intercambio permanente de información, tutelado por el ya mencionado principio de "*necesidad de conocer*".

Resulta pertinente en este punto hacer una referencia a las fuentes de obtención. En el referido modelo de Dominio se aplican todo tipo de fuentes (HUMINT, SIGINT, COMINT, IMINT, etc.), pero en el nivel básico (conocimiento del entorno general), cobran una importancia singular la inteligencia de fuentes abiertas (OSINT, por sus siglas en inglés).[9] Los volúmenes de información que se obtienen por este tipo de fuentes son tan inmensos que se hace necesario tomar conciencia de la dificultad de su proceso y manejo. Lo que, en consecuencia, se traduce en la necesidad de contar con herramientas informáticas en la forma de softwares analizadores de fuentes para que, a través de la monitorización de aquellas seleccionadas, filtren la información de interés y de valor para la organización. Es decir, se trata de introducir una serie de parámetros que permitan depurar la información relevante obtenida.

En referencia al último de los procesos considerados, la explotación y la difusión de la inteligencia, se debe precisar que también se ve facilitado por los recursos tecnológicos, permitiendo así la integración, el procesamiento y la distribución, prácticamente en tiempo real, de grandes volúmenes de información procedentes de múltiples fuentes. En el esquema de inteligencia en red, los centros de fusión se configuran como nodos críticos donde convergen capacidades analíticas avanzadas (big data, inteligencia artificial y analítica predictiva) que no solo optimizan la generación de inteligencia accionable, sino que aseguran su difusión oportuna y adaptada a los distintos niveles de decisión. Una muestra más del hecho de que la tecnología refuerza la Inteligencia Colaborativa.

No obstante, la eficacia de este modelo no puede darse por supuesta, sino que depende de la concurrencia de determinadas condiciones habilitadoras. Entre ellas, la existencia de un nivel suficiente de confianza organizativa resulta fundamental para posibilitar el intercambio de información sensible. Asimismo, se requiere el

[9] *"La inteligencia de fuentes abiertas (OSINT) es una inteligencia que se produce a partir de información disponible públicamente y que se recopila, explota y difunde de manera oportuna a una audiencia adecuada con el fin de abordar un requisito específico de inteligencia".* Definición del Departamento de Defensa de Estados Unidos, citado por Hassan & Hijazi, 2018

desarrollo de una cultura de inteligencia compartida, que integre a todos los actores implicados en el proceso, incluidos los decisores. A ello debe añadirse la necesidad de establecer mecanismos claros de gobernanza, que definan responsabilidades, niveles de acceso y procedimientos de validación del conocimiento. La estandarización de procesos y lenguajes analíticos contribuye igualmente a facilitar la interoperabilidad entre organizaciones, mientras que el equilibrio entre seguridad y apertura se configura como un elemento crítico para garantizar la viabilidad del modelo.

EMPLEO DE LAS FUENTES ABIERTAS EN LA INTELIGENCIA EN LA EMPRESA

En el contexto actual en el que se mueve la Inteligencia orientada al mundo empresarial las OSINT constituyen el soporte de la obtención y son valoradas especialmente por su capacidad para proporcionar una visión amplia y detallada de situaciones o amenazas, las cuales podrán ser complementadas por otras formas de recolección de inteligencia más restrictivas o confidenciales.

En línea con el gradiente *datos-información-inteligencia*, se precisa diferenciar de manera clara estos tres términos. Primero, los datos que provienen de la fuente primaria, y aquellos abiertos a los que pueden acceder todos aquellos que dispongan de los correspondientes recursos de obtención -metadatos-. Segundo, la información obtenida de datos sometidos a algún tipo de filtros, que se transforman así en una fuente secundaria -información abierta-, como sería el caso de la obtenida de artículos, entrevistas, u otras publicaciones. Y tercero, la Inteligencia obtenida de fuentes abiertas se refiere a la información elaborada para un determinado propósito -inteligencia centrada en el objetivo-.

Por último, mencionar muy brevemente las fuentes OSINT atienden a la obtención pasiva, en la que el objeto no es consciente de que se está obteniendo información sobre él de forma anónima; la semipasiva, cuando la actividad se limita a la información general; y la activa, en la que se utilizan técnicas invasivas sobre la protección tecnológica de los objetivos, lo que en no pocas ocasiones vulnera el propio código ético de la inteligencia (Hassan & Hijazi. 2018).

Es innegable reconocer las indudables ventajas que aporta la transformación digital en los procesos de Inteligencia; sin embargo, la velocidad y el alcance en su implementación abre la puerta de nuevos y peligrosos riesgos como son los relacionados con el cibercrimen, el terrorismo internacional, el crimen organizado, los regímenes opresores y todos aquellos grupos y actores que han encontrado en el ciberespacio un entorno ideal para cometer sus actividades delictivas y/o criminales, en ocasiones, con gran impunidad, lo que sin bien genera una ventana de vulnerabilidad en el sistema de inteligencia en red, sus beneficios superan con creces sus debilidades.

Ilustración 6. Cuadro. Las OSINT en la empresa

Resulta igualmente conveniente hacer mención de los límites y riesgos inherentes a este enfoque. La apertura de los sistemas de inteligencia puede incrementar la exposición de información sensible, especialmente en entornos en los que coexisten actores con diferentes niveles de capacidad o intereses potencialmente divergentes.

Asimismo, la participación de múltiples organizaciones puede generar problemas de difuminación de responsabilidades, dificultando la atribución de errores o la adopción de decisiones en contextos críticos. A ello se suman los riesgos derivados de una posible dependencia excesiva de las infraestructuras tecnológicas y la aparición de sesgos colectivos, que pueden afectar a la objetividad del análisis cuando no se gestionan adecuadamente los procesos de interacción.

En consecuencia, este modelo de inteligencia debe ser entendida como un modelo que, si bien ofrece una respuesta adecuada a las exigencias de los entornos contemporáneos, requiere de un diseño riguroso y de una gestión eficaz para maximizar sus beneficios y mitigar sus vulnerabilidades.

Finalmente, la propia lógica de este modelo, reforzada por el desarrollo de arquitecturas tecnológicas distribuidas que permiten la interacción en red entre múltiples actores, proyecta la función de inteligencia más allá de los límites de las organizaciones individuales. La necesidad de integrar capacidades, compartir información y generar conocimiento de manera conjunta conduce de forma natural a un enfoque sistémico de la colaboración, que es el marco en el que se desarrolla la Inteligencia Colaborativa.

La colaboración público-privada en Inteligencia.

La interacción entre actores públicos y privados adquiere una relevancia creciente, al configurarse como un elemento esencial para garantizar la eficacia de los sistemas de inteligencia en su conjunto, especialmente en aquellos ámbitos en los que los riesgos y amenazas trascienden de las capacidades de actuación de cualquier organización considerada de manera aislada.

La necesidad de mantener una relación fluida entre lo público y lo privado se muestra más evidente en el incierto y complejo contexto mundial en el que se mueven las organizaciones, las cuales para garantizar su supervivencia precisan un amplio conocimiento al que no pueden llegar de ninguna de las maneras sin una permanente colaboración. Conviene enfatizar que la supervivencia de una organización pública o privada es el fin último de la seguridad, siendo la inteligencia su escudo protector, en la medida que su carácter preventivo le permite anticipar situaciones no deseadas y enfrentar los desafíos. Por otra parte, dado el carácter multidimensional de la seguridad, su acción supera los ámbitos político y militar para

extenderse a otros como los económicos, sociales, humanos o medioambientales, entre otros, lo que se traduce en una mayor amplitud del área de conocimiento de la Inteligencia.

COLABORACIÓN PÚBLICO PRIVADA. UN ESTUDIO DE CASO

En este marco de colaboración público-privada, la OTAN desarrolló en el año 2008 el concepto *"Comprehensive Approach"* (Enfoque Integral), sobre el que pivotaba la cooperación cívico-militar en situaciones de crisis. Con él se asumía una responsabilidad compartida. Por un lado, las corporaciones civiles deberían de disponer de sus correspondientes planes de seguridad adaptados a la situación y, por otro, se establecerían las sinergias correspondientes entre éstas y las organizaciones estatales para definir y alcanzar objetivos compartidos.

Lo especialmente novedoso que aporta este concepto al tema que se desarrolla en este capítulo consiste en el examen del papel que deben desempeñar los actores del sector privado en esta estrategia integral. Se podría decir que esta inclusión de las empresas privadas a las estrategias integrales de seguridad responde a un modelo circular, entendiendo con ello que, por una parte, los riesgos y amenazas son generadores de inestabilidad en los países, especialmente en los menos desarrollados que son a su vez los más inseguros, situando a los actores de naturaleza empresarial en el primer plano de sus efectos adversos; pero simultáneamente con ello, en la medida que la actividad empresarial contribuye de una manera directa al desarrollo económico, y por ende a una mayor estabilidad y seguridad, su dimensión circular se manifiesta en la medida de que se corresponde con un instrumento de mitigación de los riesgos.

Estos actores desempeñan un protagonismo esencial en campos muy diversos, como por ejemplo el desarrollo de infraestructuras esenciales como pueden ser las de generación y distribución de energía. Este protagonismo de los actores empresariales se incrementa en entornos especialmente inseguros o volátiles, ya que exige de ellos el desarrollo de capacidades para una más amplia comprensión del entorno, de los riesgos y amenazas y su capacidad para gestionarlos, con el fin de poder desarrollar sus propias capacidades de una forma integrada. (Cumplido. 2017, citado en De Miguel. 2024)

Ilustración 7. Cuadro. Estudio de caso colaboración público-privada

Es primordial asumir la necesidad de una sólida convergencia entre ambos ámbitos, y para justificar esta afirmación categórica se podría recurrir al siguiente razonamiento. Como primer argumento se conviene que toda actividad empresarial (privada) tiene un impacto económico que repercute en las economías nacionales, hasta el punto de evidenciar una relación de causalidad en ambas direcciones. La segunda premisa es la que se refiere a la influencia directa de las políticas económicas en la seguridad (nacional), pues permiten alcanzar los intereses nacionales, los que contribuyen a la mejora el desarrollo económico y social. En base a este silogismo, se podría concluir que cuanto mayor fortaleza tenga el tejido empresarial (sector privado) más sólido será el marco económico y, en consecuencia, mejorarán las condiciones de desarrollo de la sociedad, lo que al fin redunda en la solidez de la seguridad nacional.

La actividad privada es el fundamento del desarrollo económico de un país, lo que al fin y a la postre lo hace más seguro.

Una vez que se ha establecido el marco conceptual de la colaboración público-privada, cabría considerar dos líneas de acción que, entre otras, las corporaciones empresariales deberían implementar para su materialización.[10]

1º. *Concienciación e implicación activa de la dirección corporativa*. Se trata de una responsabilidad irrenunciable de la alta dirección, la cual debiera orientar su esfuerzo en el ámbito de la relación público-privada:
   - Colaboración con entidades públicas de seguridad e inteligencia, mediante el desarrollo de programas de capacitación relacionados con los riesgos en el ámbito internacional, garantizar el acceso a la Inteligencia disponible, siempre bajo el principio ya indicado de necesidad de conocer, o el apoyo en el cumplimiento de regulaciones y normativas tanto de ámbito internacional como interno de los países de destino, entre otras iniciativas.
   - Colaboración con corporaciones privadas, siendo algunas de las posibles actuaciones la constitución de consorcios y asociaciones para compartir mejores prácticas en materia de seguridad e inteligencia, la participación en foros y conferencias donde se aborden temas de seguridad corporativa y se fomente la colaboración interempresarial, y la contratación de asesoramiento de compañías especializadas de consultorías de seguridad e inteligencia.

2º. *Redefinición y establecimiento de una nueva estructura organizacional*. De manera similar al primer punto, la adaptación estructural deberá armonizarse en los dos ámbitos considerados
   - Colaboración con entidades públicas, para ello se podrán impulsar el establecimiento de alianzas con fuerzas de seguridad locales y agencias de seguridad y defensa para garantizar una respuesta rápida y coordinada ante incidentes de seguridad, la implementación de proyectos piloto en colaboración con entidades gubernamentales para probar nuevas tecnologías y enfoques de seguridad en mercados internacionales, y el acceso a fondos y subvenciones

[10] De Miguel, 2024

disponibles para la implementación de tecnologías avanzadas y programas de seguridad internacional.

- Colaboración dentro del sector privado, tomando en consideración iniciativas como la creación de redes de intercambio de información entre empresas que operan en la misma región para compartir datos de interés compartido, la formación consorcios o asociaciones con otras corporaciones para desarrollar y financiar iniciativas que aporten una mayor seguridad al conjunto, y la externalización de servicios de inteligencia proporcionados por compañías especializadas.

Conclusiones.

La Inteligencia Colaborativa podría considerarse como una expresión avanzada de un modelo colectivo de gestionar el conocimiento que surge de la dificultad que representa la creciente especialización necesaria en los diferentes campos del conocimiento que requieren los entornos complejos e inciertos de nuestros días.

La colaboración en la función de Inteligencia, siendo fundamental en el ámbito estatal e institucional, bien podría ser considerada trascendental que el marco corporativo, de hecho, este modelo se adapta de una manera muy particular a las necesidades de las organizaciones empresariales, como consecuencia del impacto de las tecnologías de la información. De hecho, bien se podría afirmar que la Inteligencia Colaborativa se ha convertido en una herramienta clave en el desarrollo de lo que se podría denominar compañías inteligentes, entendidas aquellas cuya aspiración pasa por mantener una adaptación permanente al cambio, afrontando las necesidades organizativas y enfrentando los diferentes desafíos emergentes.

> *"Sólo se aguanta una civilización si muchos aportan su colaboración al esfuerzo. Si todos prefieren gozar el fruto, la civilización se hunde"*. (Ortega y Gasset)

Por todo lo expuesto es fácil colegir que las empresas necesitan contar, hoy más que nunca por la incertidumbre del contexto en el que desarrollan su actividad, con una superioridad en la información que les permita, por una parte, asegurar sus activos y procesos y, por otra, obtener la necesaria ventaja competitiva. En la consecución de este fin, la Inteligencia pasa a ser una disciplina indispensable en toda actividad empresarial.

Sin embargo, la mayoría de las empresas no pueden asumir los costos que supone incorporar a su organización una sección o departamento de inteligencia, ni tampoco la mayoría de las empresas especializadas en esta disciplina pueden incorporar a su organización las personas, los medios y los sistemas que se precisan para ofrecer un producto adaptado a todas las necesidades. Por ello, el apoyo mutuo entre estas organizaciones es fundamental, y esta cooperación entre empresas y agencias y/o compañías consultoras de inteligencia debe de ser una constante, tanto en el sector público como en el privado. El exponencial desarrollo tecnológico de las últimas décadas ha permitido que esta colaboración pudiera quedar sistematizada, dando con ello su verdadera carta de naturaleza a la Inteligencia Colaborativa.

BIBLIOGRAFÍA

Central Intelligence Agency. (2005). Report of the Office of Inspector General on the Central Intelligence Agency's accountability regarding findings and conclusions of the Joint Inquiry into Intelligence Community Activities before and after the terrorist attacks of September 11, 2001. CIA.

Coll, S. (2004). Ghost wars: The secret history of the CIA, Afghanistan, and bin Laden, from the Soviet invasion to September 10, 2001. Penguin Press.

Cumplido Tercero, Miguel Ángel. 2017. La exposición al riesgo de seguridad internacional para la empresa española: el deber de protección y la estrategia de *comprehensive approach* (artículo) Instituto Español de Estudios Estratégicos. Madrid, España

De Miguel, Jesús. 2024. La Inteligencia Estratégica desde un enfoque integral. Eliva Press. Chisinau, Moldova

Godson, Roy. 2012. Operationalizing intelligence dominance. CIWAG case study series 2011-2012, ed. Marc Genest and Andrea Dew. Newport, RI: US Naval War College, Center on Irregular Warfare and Armed Groups.

Hassan, Nihad A. and Hijazi, Rami. 2018. Open Source Intelligence. Methods and Tools. Apress. New York, USA

National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report: Final report of the National Commission on Terrorist Attacks Upon the United States. W. W. Norton & Company.

U.S. Senate Select Committee on Intelligence & U.S. House Permanent Select Committee on Intelligence. (2002). Joint inquiry into intelligence community activities before and after the terrorist attacks of September 11, 2001. U.S. Government Printing Office.

Wright, L. (2006). The looming tower: Al-Qaeda and the road to 9/11. Alfred A. Knopf.

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

Desarrollo Divergente de los Estudios de Posgrado en Inteligencia: Análisis comparado de los factores institucionales, epistemológicos y culturales en Norteamérica, el Reino Unido, Europa Continental y América Latina.

Ricardo Sánchez Piedrahita*

Resumen: Este artículo analiza por qué los estudios de posgrado en inteligencia se han desarrollado de forma tan distinta en Norteamérica, el Reino Unido, Europa y América Latina. Mediante una revisión de la oferta educativa actual (2024-2025) y una encuesta a 250 expertos del sector, se identificó una brecha profunda: mientras que los países anglosajones tienen sistemas académicos maduros y conectados con sus gobiernos, en América Latina la formación es aún escasa y limitada. Al respecto, la encuesta sugiere percepciones convergentes: el 83,2% de los especialistas considera que este retraso se debe a fallas del sistema, destacando principalmente la falta de convenios entre universidades y el Estado (37,6%) y una desconfianza histórica hacia estas instituciones. Además, el 66,4% de los consultados percibe que la región todavía depende excesivamente de teorías extranjeras. El estudio concluye que, para cerrar esta brecha, las universidades latinoamericanas deben crear programas civiles y multidisciplinarios que permitan generar una inteligencia estratégica propia, moderna y adaptada a la realidad regional.

Palabras clave: Inteligencia, Educación superior, Epistemología, América Latina, Cultura.

---

* El Capitán de Navío Ricardo Enrique Sánchez Piedrahita es Profesional en Ciencias Navales y posee las maestrías en Seguridad y Defensa Nacional, así como en Gerencia Logística con énfasis en Puertos, ambas con distinciones académicas, además de ser especialista en Política y Estrategia Naval y en Gerencia Logística. Con más de 25 años de trayectoria en la Armada Nacional de Colombia, ha comandado Fuerzas Especiales Navales, el Componente Naval de la Presidencia y diversas jefaturas de inteligencia regional. Destaca por liderar el diseño operacional de la Campaña Naval Orión y el desarrollo de plataformas tecnológicas como RADAR y SIGMA para la seguridad marítima. Actualmente se desempeña como Director de la Academia Naval de Estudios Estratégicos y lidera la Red Iberoamericana de Estudios en Inteligencia, especializándose en líneas de investigación sobre guerra híbrida, inteligencia estratégica y prospectiva.

Abstract: This article explores why postgraduate intelligence studies have developed so differently across North America, the United Kingdom, Continental Europe, and Latin America. By reviewing the current educational landscape (2024-2025) and surveying 250 experts in the field, a profound gap was identified: while Anglo-Saxon countries possess mature academic systems closely linked to their governments, training in Latin America remains scarce and limited. The results reveal that 83.2% of specialists attribute this delay to systemic failures, highlighting the lack of formal agreements between universities and the State (37.6%) and a long-standing historical distrust toward these institutions. Furthermore, 66.4% of those surveyed perceive that the region still relies excessively on foreign theories. The study concludes that to bridge this gap, Latin American universities must create civilian, multidisciplinary programs that foster the development of independent strategic intelligence, modern and adapted to regional realities.

Keywords: Intelligence, Higher Education, Epistemology, Latin America, Culture.

INTRODUCCIÓN

La inteligencia estratégica se ha consolidado en el siglo XXI como una función esencial del Estado moderno. Su utilidad principal radica en optimizar la acción estatal: actúa como factor de ilustración para los tomadores de decisiones al reducir la incertidumbre y fundamentar las políticas a través de un conocimiento claro de la realidad (Herman, 1996). Este fenómeno impulsó el surgimiento de los Estudios de Inteligencia (EI) como un campo académico interdisciplinario conectado con la ciencia política, las relaciones internacionales, la historia, la economía, la tecnología y la psicología (Michael y Kornbluth, 2019).

Sin embargo, la expansión global de este campo no ha sido, homogénea. En los países anglosajones y europeos, los EI se han consolidado como una disciplina académica reconocida, con programas de posgrado articulados, ecosistemas institucionales maduros y vínculos formales entre universidades y agencias estatales. En contraste, América Latina permanece en una etapa incipiente de institucionalización: la oferta académica se concentra principalmente en ámbitos militares y policiales, la producción teórica propia es escasa y persiste una desconfianza cultural históricamente arraigada hacia el campo como objeto de estudio universitario civil. Esta disparidad no es únicamente cuantitativa, (número de programas disponibles), sino profundamente cualitativa, pues responde a condicionantes históricos, epistemológicos e institucionales que han impedido la consolidación

del campo como disciplina autónoma en la región (Battaglino, 2012: 68; Tickner y Waever, 2009: 332).

Michael y Kornbluth (2019) definen la academización de la inteligencia como el proceso de investigación académica, conceptualización y enseñanza universitaria de este campo, cuyo objetivo es proveer de mayor pensamiento estratégico, criterio analítico y flexibilidad a los futuros profesionales mediante programas universitarios (2019: 117). Corvaja, Jeraj y Borghoff (2016) han documentado el surgimiento de los EI como subdisciplina aceptada de los estudios de seguridad, articulando áreas clave como fallos de inteligencia, politización, supervisión, ética y culturas nacionales de inteligencia (2016: 80). Gearon (2020) analiza la relación entre universidades, seguridad e inteligencia en perspectiva internacional, mientras que Tickner y Waever (2009) examinan cómo las teorías dominantes en relaciones internacionales han sido producidas principalmente en Estados Unidos y Europa, relegando a otras regiones a una posición periférica en la producción del conocimiento (2009: 332).

Desde el eje histórico-institucional, la consolidación del campo en Estados Unidos fue impulsada por la experiencia de la Segunda Guerra Mundial y la Oficina de Servicios Estratégicos (OSS), que condujo a la integración de científicos sociales como William Langer y Sherman Kent en la Agencia Central de Inteligencia (CIA) entre 1950 y 1953, institucionalizando los métodos de las ciencias sociales en el análisis de inteligencia y estableciendo un estándar para las estimaciones durante décadas (Grace, 2022: 3, 10-11). En el Reino Unido, la evolución histórica del MI5, MI6 y el Cuartel General de Comunicaciones del Gobierno (GCHQ) generó una cultura académica de escrutinio que legitimó este tipo de formación y facilitó su inserción en el sistema universitario civil (Goodman y Omand, 2008: 1-12). En América Latina, este proceso no tuvo paralelo: las instituciones de inteligencia surgieron en contextos autoritarios, orientadas hacia el control interno bajo los preceptos de la Doctrina de Seguridad Nacional (DSN) , generando una desconfianza estructural entre la academia civil y las comunidades de inteligencia que Swenson (2003) caracteriza como una huella de sospecha mutua que persiste hasta el presente (p. 109).

El desarrollo de una nación y la salvaguarda de su soberanía dependen intrínsecamente de la consolidación de una cultura estratégica robusta. De acuerdo con Shapira (2025), la cultura estratégica constituye el contexto general y fundamental que da forma al pensamiento y a la acción estratégica de un Estado (p. 14), y se define técnicamente como

el "conjunto de valores, creencias, experiencias y tradiciones que moldean la forma como un Estado conceptualiza su seguridad" (Cortés y Cufiño, 2022: 32).

En este marco, la cultura estratégica opera como un esquema inspirador del cual emergen subculturas especializadas, siendo la cultura de inteligencia una de las más esenciales para la toma de decisiones. Esta última se entiende como el conjunto específico de normas, valores y hábitos que moldean el entorno de las agencias de inteligencia (Shapira, 2025: 12); Esteban Navarro (2007, pp. 68-69) la define como el conjunto de conocimientos que la sociedad debe poseer sobre la necesidad, el fin y la función de los servicios de inteligencia, de modo que los ciudadanos perciban como propias las cuestiones vinculadas a su seguridad, su libertad y la defensa de sus intereses.

Esta concepción es ampliada por Sans-Rubert Pascual y Pulido-Gragera (2022, p. 1), quienes la entienden como una política de sensibilización pública orientada a mejorar el conocimiento colectivo sobre los objetivos y funciones de los servicios de inteligencia, fomentando que todos los actores sociales desarrollen conciencia de su papel activo en la salvaguarda de la seguridad y la defensa de valores democráticos. En ambas aproximaciones subyace una premisa común: la inteligencia no es un asunto exclusivo del Estado, sino una responsabilidad compartida que exige comprensión y apropiación ciudadana, su desarrollo en contextos democráticos exige, según Matei et al. (2022), un equilibrio constante entre eficacia operacional, secreto profesional, transparencia y rendición de cuentas (p. 5).

La inteligencia estratégica cumple, en consecuencia, la función principal de reducir la incertidumbre y proveer conocimiento de alto nivel para la generación de políticas públicas y exteriores. Como señala Kent (1986), la inteligencia exterior no solo fundamenta la política nacional, sino que salvaguarda la supervivencia del Estado frente a actores externos (pp. 24-25), proporcionando una ventaja competitiva que permite anticipar los planes de rivales e identificar tendencias globales (Acuff et al., 2022). Sin embargo, la implementación de estos principios enfrenta desafíos particulares en la región: el legado de regímenes autoritarios ha vinculado a los servicios de inteligencia con la represión política, generando una desconfianza ciudadana persistente (Matei et al., 2022: 2). Martín (2024) destaca que, históricamente, muchos gobiernos latinoamericanos se enfocaron más en el control interno y la represión violenta que en las preocupaciones de seguridad

externa (p. 14), lo que derivó en una carencia de fiscalización técnica, facilitó la politización de las agencias y reforzó su oscuridad operacional (Matei et al., 2022:6).

Ante esta realidad, los EI emergen como una necesidad académica y profesional multidisciplinaria. Situados en la intersección entre la ciencia política, las relaciones internacionales, la economía y el desarrollo científico y tecnológico, buscan conceptualizar la influencia de la inteligencia en la seguridad nacional (Dimitrijević, 2023: 51). La formación académica de posgrado resulta vital en este proceso, pues promueve el pensamiento crítico al situar al estudiante en niveles cognitivos superiores para analizar e integrar información compleja (Bloom, 1956); además, estos espacios actúan como mediadores entre el hermetismo gubernamental y la opinión pública, promoviendo la legalidad y la rendición de cuentas (Gomez, 2023: 4). En este sentido, la profesionalización del analista constituye el pilar de un servicio de inteligencia eficiente: Pettee (1946) sostiene que para evitar que la inteligencia sea una ocupación casual, se requiere personal altamente cualificado, con pensamiento crítico y una formación análoga al método científico (p. 93). La transformación de la inteligencia en una institución de relevancia estratégica depende de una formación de alto nivel que combine el rigor metodológico para mitigar sesgos cognitivos (Heuer y Pherson, 2015) con la capacidad analítica de mentes brillantes orientadas a la producción de valor transcendental (Herman, 1996: 324).

La brecha identificada posee, además, una dimensión epistemológica que la investigación latinoamericana no ha resuelto. Como señalan Centeno y López-Alves (2001), los estudios latinoamericanos han tendido a ser predominantemente descriptivos, con escasa elaboración teórica, lo que ha impedido la consolidación de escuelas de pensamiento regionales con capacidad de influir en el debate global (Schenoni, 2016). Acharya (2014) corrobora esta tesis al señalar el fin progresivo del orden unipolar en la producción intelectual global, mientras Kendall (1949) advierte que, sin una base teórica autónoma, la inteligencia corre el riesgo de volverse irrelevante para los decisores políticos, fomentando una peligrosa desconexión entre el conocimiento y la acción (1949: 550). Esta dependencia teórica dificulta el desarrollo de enfoques propios ajustados a las realidades regionales (Tickner y Waever, 2009: 332), y priva a la región de los mecanismos institucionales necesarios para producir conocimiento que retroalimente la práctica analítica.

En consecuencia de lo anterior, la pregunta de investigación que orienta este estudio es: ¿Qué factores institucionales, epistemológicos y culturales explican la brecha en el desarrollo de la oferta académica de posgrado en Estudios de Inteligencia entre Norteamérica, el Reino Unido, Europa Continental y América Latina? y, ¿qué oportunidades estructurales existen para superar dicha brecha en el contexto latinoamericano? El objetivo general consiste en analizar comparativamente la oferta académica de posgrado en EI en las cuatro regiones señaladas, identificando los factores estructurales, epistemológicos y culturales que explican las disparidades regionales y las oportunidades para el desarrollo de plataformas académicas especializadas en el ámbito latinoamericano. En paralelo, el artículo busca: (1) caracterizar y comparar los programas de posgrado en EI disponibles en las cuatro regiones según nivel de profesionalización, perfil de ingreso, orientación curricular y modelo de gobernanza institucional; (2) diagnosticar el estado del campo en América Latina a partir de tres ejes analíticos, debilidad institucional, dependencia epistemológica y ausencia de pensamiento estratégico autónomo, y (3) identificar elementos para incentivar a universidades latinoamericanas a desarrollar posgrados en Inteligencia Estratégica que generen cultura estratégica de Estado y trasciendan el ámbito de la seguridad y defensa.
En términos metodológicos, el estudio adopta un enfoque mixto, con predominio cualitativo y apoyo cuantitativo no probabilístico, con alcance descriptivo-comparativo. La unidad de análisis son los programas de posgrado en Estudios de Inteligencia Estratégica, comparados en cuatro variables estructurales: nivel de profesionalización, perfil de ingreso y salida del estudiante, contenido curricular y enfoque disciplinar, y modelo de gobernanza institucional, (universitario civil, militar o institucional-estatal). La recolección de información se realizó mediante revisión documental, análisis de contenido y un estudio comparativo de programas vigentes en el período 2024-2025. La población del estudio es de tipo finita e integrada por 250 profesionales e investigadores del ámbito de la seguridad, defensa e inteligencia estratégica en Iberoamérica, con alta cualificación académica y procedencia mayoritaria de Colombia, Argentina, México, Ecuador y España. Se aplicó un cuestionario estructurado en Google Forms mediante muestreo no probabilístico de sujetos voluntarios entre el 30 de marzo y el 6 de abril de 2026.

HALLAZGOS

1. Caracterización Comparativa de los Programas de Posgrado en Estudios de Inteligencia

El estudio de mercado académico comparado (2024-2025) permitió identificar y sistematizar la oferta activa de posgrado en las cuatro regiones, clasificándola en función de cuatro variables estructurales: nivel de profesionalización, perfil de ingreso, orientación curricular y modelo de gobernanza institucional (ver Tabla 1).

Tabla 1: Distribución de la oferta según el nivel de profesionalización y perfil del estudiante

Región	Predominio de programas	Perfil de ingreso principal	Orientación de la salida profesional
Norteamérica (EE.UU./Canadá)	Híbrido (Graduate y Postgraduate)	Estudiantes de carrera y oficiales activos	Análisis de inteligencia, tecnología, apoyo para generación de política pública.
Reino Unido (UK)	Graduate (académico)	Graduados en RR. II. o Política	Análisis estratégico, Historia, Ética,
Europa Continental	Especializado (Ciber/Económica)	Profesionales del sector privado	Inteligencia económica y ciberseguridad
Latinoamérica	Institucional (militar/defensa)	Miembros de fuerzas públicas y civiles	Enfoque hacia la seguridad interna, policivo.

Fuente: elaboración propia con base en revisión de oferta académica verificada (2024-2025*)*.

Norteamérica concentra el ecosistema más sólido y diversificado. La oferta se articula en dos modalidades complementarias: los programas graduate, como el MA in Strategic Intelligence del Institute of World Politics (EE.UU.) y el MA in International Affairs with Intelligence Specialization de Carleton University (Canadá), orientados a estudiantes de carrera con énfasis en investigación; y los programas postgraduate de la National Intelligence University (NIU), diseñados exclusivamente para oficiales en servicio activo con experiencia operacional. Como señalan Corvaja et al. (2016), esta distinción no es solo formal: los programas postgraduate "son ideales para oficiales de inteligencia con experiencia, enfocados en habilidades analíticas y contexto estratégico, a diferencia de los graduate, de carácter más académico" (2016: 88). Esta doble modalidad posiciona a Norteamérica como referente en la articulación entre formación académica y práctica.

La amplitud de la oferta norteamericana se extiende también hacia programas que cubren perfiles temáticos y metodológicos específicos: el MSc in Applied Intelligence de Mercyhurst University, el MA in Security Studies with Intelligence Concentration de Georgetown University, el Master of Arts in Strategy, Cybersecurity, and Intelligence (MASCI) de Johns Hopkins SAIS, el Master of Arts in National Security and Intelligence de Northeastern University y el Master of National Security & Intelligence de la Bush School of Government de Texas A&M University. A estos se suman el Strategic Intelligence M.S. de Saint Louis University, orientado a la toma de decisiones estratégicas, el M.S. Intelligence Studies de la University of South Florida, y el programa de Intelligence and Security Studies de The Citadel, con formación estratégica y operativa (Carleton University, s.f.; Institute of World Politics, s.f.; Mercyhurst University, s.f.; Georgetown University, s.f.; Johns Hopkins SAIS, s.f.; Northeastern University, s.f.; Bush School of Government & Public Service, s.f.; Saint Louis University, s.f.; University of South Florida, s.f.; The Citadel, s.f.). La NIU complementa esta oferta con dos títulos postgraduate diferenciados: el MSc in Strategic Intelligence (MSSI), de acceso exclusivo para oficiales activos con enfoque estratégico, y el MSc in Strategic Technology Intelligence (MSTI), orientado a inteligencia tecnológica y capacidades estratégicas (National Intelligence University, s.f.). Esta diversidad programática no es casual: refleja décadas de construcción institucional en las que el vínculo entre la academia y las agencias de inteligencia se forjó desde la Segunda Guerra Mundial y la experiencia de la OSS, lo que llevó a la institucionalización de esta relación en universidades y think tanks (Grace, 2022: 76-78).

A ello se añaden iniciativas aplicadas que ilustran cómo el ecosistema norteamericano va más allá de la oferta de títulos formales, construyendo plataformas de formación continua y transferencia de conocimiento que no tienen equivalente en otras regiones: el Intelligence Project del Belfer Center de Harvard, orientado a formar una nueva generación de profesionales de inteligencia y articular redes entre agencias, investigadores y estudiantes; el Center for Intelligence Research, Analysis and Training (CIRAT) de Mercyhurst, unidad orientada a contratos, subvenciones y alianzas que profesionalizan las capacidades analíticas; y el Intelligence Studies Project de la University of Texas at Austin, que impulsa experiencias formativas mediante clases, estudios de caso, simulaciones y visitas profesionales, a través de la Texas Intelligence Academy (Belfer Center, 2026; Mercyhurst University, s.f.; University of Texas at Austin, s.f.).

El Reino Unido, por su parte, ha apostado por un modelo graduate de alto perfil académico. Programas como el MA in Intelligence and International Security de King's College London o el Security, Intelligence & Strategic Studies del programa Erasmus Mundus articulan desde sus orígenes la dimensión analítica con las exigencias del servicio exterior del Estado (Goodman y Omand, 2008: 1-12). La evolución histórica del MI6 y el GCHQ generó una cultura académica de escrutinio que legitimó este tipo de formación y facilitó su inserción en el sistema universitario civil, proceso que Michael y Kornbluth (2019) describen como la "academización de la inteligencia" (2019: 117). Completan la oferta británica el MA in Intelligence and Strategic Studies de Aberystwyth University y el MA in Intelligence and Security Studies de Brunel University, programas que consolidan la tradición del escrutinio académico sobre los servicios de inteligencia como rasgo definitorio del modelo anglosajón (Aberystwyth University, s.f.; Brunel University, s.f.; King's College London, s.f.).

Europa Continental ofrece una oferta moderada y técnicamente especializada. España ha desarrollado una variedad de programas de formación permanente en análisis, ciberinteligencia e inteligencia económica: el Máster en Análisis de Inteligencia y Ciberinteligencia de la Universidad Nebrija, el Máster en Analista de Inteligencia de la Universidad Rey Juan Carlos, el Máster en Dirección, Operaciones y Análisis de Inteligencia de la Universidad CEU San Pablo, el Máster en Inteligencia y Seguridad de la Universidad Isabel I, y el Máster en Inteligencia del LISA Institute (Universidad Nebrija, s.f.; Universidad Rey Juan Carlos, s.f.; Universidad CEU San Pablo, s.f.; Universidad Isabel I, s.f.; LISA Institute, s.f.). Francia vincula la inteligencia con la competitividad económica a través del Master Intelligence Économique de la Universidad de Lorraine y del Master Intelligence Économique et Stratégie del ILERI, mientras Italia y el consorcio Erasmus Mundus integran perspectivas comparadas de seguridad e inteligencia estratégica, con el Máster en Inteligencia de INISEG en colaboración con la Universidad Pegaso (Universidad de Lorraine, s.f.; ILERI, s.f.; INISEG/Universidad Pegaso, s.f.; IMSISS Erasmus Mundus, s.f.). En este contexto, la orientación curricular refleja las prioridades estratégicas de cada contexto nacional, lo que da lugar a un perfil de estudiante proveniente mayoritariamente del sector privado y orientado a la inteligencia económica y la ciberseguridad (ver Tabla 2). Como señala la literatura especializada, países europeos como Alemania, Francia, Italia y España han adoptado modelos de estudios de inteligencia para analizar las habilidades analíticas fundamentales, el marco legal y la interacción política (Corvaja et al., 2016), avanzando

por un camino propio que privilegia las competencias operativas y analíticas sobre la dimensión académico-investigativa predominante en el mundo anglosajón.

Tabla 2: Análisis de mallas curriculares y enfoques disciplinares por región

Región	Áreas curriculares clave	Enfoque teórico-metodológico
Norteamérica / UK	Geopolítica, Ética, Análisis de Fallos, Historia de Agencias	Empírico-analítico orientado a decisiones
Europa Continental	Inteligencia Económica, Ciberinteligencia, Marco Legal	Multidisciplinario (competitividad y ley)
Latinoamérica	Amenazas Híbridas, Crimen Transnacional, Lucha contra las Drogas, Grupos Armados Ilegales, Contrabando.	Doctrinario-estatista (Seguridad, soberanía y orden)

Fuente: elaboración propia con base en revisión de programas académicos verificados (2024-2025).

América Latina muestra el patrón inverso: baja densidad institucional, concentración de la oferta en instituciones de defensa y marcada ausencia de programas civiles abiertos. El modelo de gobernanza predominante es el institucional-militar, dato que la encuesta aplicada a 250 especialistas corrobora: el 44% de los encuestados identificó el modelo híbrido como el prevalente en su región, mientras que un significativo 32% señaló el modelo institucional militar cerrado y apenas el 9,2% reconoció la existencia de un modelo universitario civil abierto al público. Este resultado es coherente con la afirmación de que el patrón regional es "la formación en seguridad, defensa o relaciones internacionales, pero no en inteligencia como disciplina autónoma" (Michael y Kornbluth, 2019). El hallazgo sistemático de la oferta confirma que los programas existentes en la región corresponden principalmente a: la Maestría en Inteligencia Estratégica de la ESICI (Colombia), la Maestría en Inteligencia Estratégica Nacional de la UNLP (Argentina), la Especialización en Análisis de Inteligencia Estratégica de la Universidad Argentina de la Defensa, la Especialización en Inteligencia Estratégica del CALEN (Uruguay), el Magíster en Inteligencia Estratégica de la ANEPE (Chile) y la Maestría en Inteligencia Estratégica del CAEN (Perú) (ver Tabla 3). Estas excepciones parciales no alteran la tendencia estructural dominante

(ESICI, s.f., s.f.; s.f.; Universidad Nacional de La Plata, s.f.; Argentina Ministerio de Defensa, s.f.; CALEN, s.f.; ANEPE, s.f.; CAEN, s.f.). La ausencia es especialmente pronunciada en Centroamérica, donde Guatemala, El Salvador, Honduras, Costa Rica y Panamá no cuentan con programas de posgrado formalmente estructurados en inteligencia estratégica abiertos al público, lo que confirma la caracterización de la región como un caso de dependencia de formación interna institucional y de ausencia de institucionalización académica autónoma del campo.

Tabla 3: Oferta de posgrados en inteligencia estratégica en América Latina (2024-2025)

Programa	País	Institución	Tipología
Maestría en Inteligencia Estratégica	Colombia	ESICI	Militar/estatal
Maestría en Inteligencia Estratégica Nacional	Argentina	UNLP	Académico consolidado
Especialización en Análisis de Inteligencia Estratégica	Argentina	Universidad Argentina de la Defensa	Institucional/defensa
Especialización en Inteligencia Estratégica	Uruguay	CALEN	Estatal/defensa
Magíster en Inteligencia Estratégica	Chile	ANEPE	Militar/civil híbrido
Maestría en Inteligencia Estratégica	Perú	CAEN	Militar/estatal

Fuente: elaboración propia con base en revisión de oferta académica verificada (2024-2025)[11].

El análisis comparado permite establecer una progresión clara en el nivel de madurez del mercado académico de posgrados en inteligencia (ver Tabla 4). Este contraste estructural constituye el marco de referencia para los tres ejes de déficit identificados en la sección siguiente.

[11] Los programas identificados reflejan instituciones activas con oferta comprobable en el período de análisis.

Tabla 4: Nivel de madurez del ecosistema académico de posgrados en inteligencia por región

Región	Nivel de madurez	Característica estructural
Norteamérica	Muy alto	Ecosistema completo y articulado; diferenciación graduate/postgraduate; redes academia-Estado consolidadas
Reino Unido	Alto	Modelo académico consolidado; tradición institucional MI6/GCHQ; cultura de escrutinio académico
Europa Continental	Medio	Especialización técnica en ciberinteligencia e inteligencia económica; orientación profesional
América Latina	Bajo	Fragmentado y emergente; dominio institucional-militar, policial; incipiente apertura civil

Fuente: elaboración propia con base en el análisis comparado del estudio de mercado (2024-2025).

2. Diagnóstico del campo en América Latina: tres ejes de déficit estructural

2.1 Debilidad institucional y ausencia de ecosistema académico consolidado

El primer eje de déficit estructural en América Latina es la debilidad institucional del campo. La investigación en seguridad e inteligencia en la región "presenta altos niveles de fragmentación y una débil institucionalización, lo que dificulta la consolidación de comunidades académicas estables" (Battaglino, 2012: 68). Esta condición es consecuencia directa de la "ausencia de vínculos sólidos entre universidades, centros de pensamiento y organismos estatales" (Diamint, 2015: 45), que en el mundo anglosajón fueron construidos paulatinamente desde la Segunda Guerra Mundial y consolidados a través de eventos como el Comité Church[12], que obligaron a las agencias a buscar validación externa y escrutinio académico para recuperar legitimidad (Gearon, 2020).

[12] El Comité Church fue una comisión del Senado de Estados Unidos creada en 1975 para investigar abusos de las agencias de inteligencia y revelar operaciones encubiertas y violaciones a derechos y leyes (Levin Center, 2024).

La encuesta confirma este diagnóstico: ante la pregunta por el principal factor institucional que explica la escasa oferta de posgrados civiles en Inteligencia Estratégica, el 37,6% de los 250 encuestados señaló la ausencia de vínculos formales entre universidades y organismos estatales de inteligencia como la causa principal. Un 21,2% atribuyó la brecha a la desconfianza estructural entre la academia civil y las comunidades de inteligencia, y un 24,4% identificó la prevalencia de programas cerrados en ámbitos militares o policiales sin apertura al sector civil.

Estos tres factores, acumulados, configuran el 83,2% de las respuestas y apuntan a una misma causa sistémica: la inexistencia de un ecosistema institucional que facilite la transferencia de conocimiento entre el mundo académico y el mundo operacional.

Este contraste con el mundo anglosajón ilustra con claridad las consecuencias estructurales de la falta de institucionalización. Mientras en Estados Unidos el escepticismo entre academia y agencias se resolvió mediante la integración y el debate, simbolizada por la incorporación de académicos y científicos en la CIA entre 1950 y 1953 (Grace, 2022), en América Latina la inteligencia permaneció como dominio exclusivo de militares o policías (Hilsman, 1956), perpetuando su marginalidad académica. El contraste se profundiza cuando se considera que el ecosistema norteamericano no solo produce titulaciones formales, sino que articula plataformas de conocimiento aplicado como el CIRAT de Mercyhurst o el Intelligence Studies Project de la University of Texas at Austin, cuya función es precisamente sostener el vínculo entre producción académica y práctica operacional, una dimensión prácticamente inexistente en la región latinoamericana (Mercyhurst University, s.f.; University of Texas at Austin, s.f.).

Esta debilidad institucional tiene consecuencias directas sobre la calidad de la práctica analítica. La ausencia de una educación profesional avanzada en gerencia, administración, análisis y producción de la inteligencia dificulta la comunicación entre productores y consumidores, pues carecen de un lenguaje común y un conocimiento detallado de la inteligencia como institución, proceso, función y cultura (Spracher, 2009). En el contexto latinoamericano, donde muchas direcciones de agencias de inteligencia son designaciones políticas sin formación especializada, esta carencia se traduce en una gestión intuitiva que genera conflictos y fallos analíticos con graves implicaciones estratégicas (Spracher, 2009). La falta de colaboración y

el aislamiento estructural entre analistas y formuladores de políticas impide que los primeros entiendan las necesidades reales, limitando el valor del conocimiento generado (Gomez, 2023). Sin una comprensión teóricamente informada, las organizaciones son propensas a la rigidez cognitiva y al pensamiento grupal, lo que les impide interpretar correctamente las señales de peligro (Herman, 1996: 221-224).

La debilidad institucional también se manifiesta en la ausencia de marcos legales específicos que regulen y legitimen la actividad de inteligencia dentro del Estado de Derecho. Como advierte Allen Dulles (1963/1965), el marco legal establecido por la Ley de Seguridad Nacional de 1947 en EE.UU. "prohíbe explícitamente a la CIA tener poderes policiales, de citación, de aplicación de la ley o funciones de seguridad interna, una salvaguarda fundamental para prevenir una inteligencia de estado policial" (Dulles, 1965: 31-32, 239-240). La ausencia de marcos equivalentes en buena parte de América Latina no solo expone a los servicios de inteligencia a la politización, sino que refuerza la desconfianza académica y ciudadana que inhibe el desarrollo del campo como disciplina civil. La integración de la dimensión ético-legal en los currículos de posgrado es, por tanto, una condición no negociable para la construcción de servicios de inteligencia que operen dentro del Estado de Derecho.

2.2 Dependencia epistemológica de marcos teóricos externos

El segundo eje de déficit estructural es la dependencia epistemológica. Por ésta se entiende la necesidad de validación externa del conocimiento por parte de instancias con autoridad y legitimidad científica (Suárez, A. 2021: 357-258)[13]. En este sentido, América Latina ha operado históricamente bajo una fuerte dependencia de teorías producidas principalmente en Norteamérica y el Reino Unido (Tickner y Waever, 2009). Esta posición periférica, documentada por Acharya (2014) en el conjunto de las ciencias sociales, adquiere en el campo de la inteligencia una dimensión particularmente relevante: la formación profesional y la doctrina operacional han sido importadas sin adaptación a las realidades regionales, generando una "dependencia teórica que dificulta el desarrollo de enfoques propios" (Tickner y Waever, 2009: 332).

[13] Según este autor, la epistemología sirve para analizar y debatir si un conocimiento es o no científico, o cómo puede serlo. Es decir, la epistemología discute los problemas de validez, autoridad y legitimidad del conocimiento (científico o con aspiración a este nivel). De aquí la inferencia del concepto indicado.

Los datos de la encuesta ratifican esta percepción con contundencia. Ante la pregunta sobre cómo calificar la dependencia de los programas latinoamericanos respecto a modelos teóricos y metodológicos externos, el 25,6% calificó la dependencia como alta, indicando que los modelos se importan sin adaptación al contexto regional, mientras que el 40,8% la consideró moderada, reconociendo la persistencia de influencia externa. Sumados, estos dos segmentos representan el 66,4% de los encuestados que perciben una dependencia epistemológica significativa. De manera reveladora, un 24,4% estimó que no existe suficiente oferta académica propia como para evaluar siquiera el grado de esa dependencia, lo que constituye en sí mismo un indicador de la profundidad del déficit.

Esta dependencia epistémica no es un fenómeno neutral: tiene consecuencias directas sobre la capacidad de los servicios de inteligencia de interpretar con precisión las realidades nacionales. Como advierte Platt (1961), ignorar el estudio sistemático del carácter nacional lleva a peligrosas incomprensiones en las relaciones internacionales (1961: 5), y Kent (1949) señala que, sin una base teórica autónoma, la inteligencia corre el riesgo de volverse irrelevante para los decisores políticos, fomentando una "peligrosa desconexión entre el conocimiento y la acción" (1949: 550).

Esta vulnerabilidad se agrava cuando se examina la genealogía del conocimiento analítico disponible en la región. La consolidación de los estudios de inteligencia en EE.UU. fue posible por la incorporación masiva de profesionales y científicos en la CIA entre 1950 y 1953 (Grace, 2022). Esta simbiosis, forjada en un contexto de amenaza existencial, no tuvo un paralelo en Latinoamérica, donde las instituciones de inteligencia surgieron en contextos autoritarios liderados por dictadores (Grace, 2022). El proceso transformó los informes de la CIA, otorgándoles una legitimidad basada en el rigor académico y estableciendo un estándar para las estimaciones durante décadas (Grace, 2022: 3, 10-11). Como consecuencia, gran parte del conocimiento en seguridad ha sido importado, sin que exista en la región una tradición equivalente de institucionalización del método y las técnicas de análisis en la práctica analítica de inteligencia.

Desde una perspectiva epistemológica más amplia, los estudios de inteligencia representan un cuerpo intelectual cuya base se ubica entre la Ciencia Política, las Relaciones Internacionales y los Estudios de Seguridad (Dimitrijević, 2023). Sin una masa crítica de programas

académicos civiles que cultiven esta intersección disciplinar, América Latina carece de los mecanismos institucionales para producir conocimiento que retroalimente la práctica. El análisis comparativo de las mallas curriculares regionales confirma que los programas latinoamericanos que existen privilegian un enfoque doctrinario-estatista centrado en crimen doméstico y trasnacional, amenazas híbridas y poder nacional (ver Tabla 2), mientras que las áreas de Geopolítica, ética, análisis de fallos, historia y métodos de análisis fundamentales para la formación de analistas resilientes, están prácticamente ausentes. Esta brecha curricular tiene consecuencias directas sobre la calidad del análisis producido: sin formación sólida en métodos analíticos estructurados para mitigar la mentalidad arraigada, los sesgos cognitivos y el pensamiento de grupo (Heuer y Pherson, 2014), los analistas formados en estos esquemas carecen de las herramientas para cuestionar sus propios supuestos y generar estimaciones de inteligencia procesable.

2.3 Limitada construcción de pensamiento estratégico autónomo

El tercer eje es la ausencia de tradiciones intelectuales propias que den lugar a escuelas de pensamiento estratégico regional. Los estudios latinoamericanos han tendido a ser predominantemente descriptivos, con escasa elaboración teórica (Centeno y López-Alves, 2001), lo que ha impedido "la consolidación de escuelas de pensamiento regionales con capacidad de influir en el debate global" (Schenoni, 2016). En Latinoamérica, la cultura estratégica fue influenciada por doctrinas externas que redefinieron el rol militar hacia el control interno (Gallego et al., 2005), orientando el esfuerzo de producción de inteligencia mayoritariamente hacia el interior de las fronteras y limitando su dimensión estratégica y anticipatoria frente a amenazas u oportunidades transnacionales.

Este déficit tiene una dimensión cultural que trasciende lo académico. La encuesta identificó que, el 43,6% de los encuestados considera que la inteligencia es un tema exclusivamente militar o policial y, en consecuencia, es el principal factor que ha influido en la desconfianza hacia los estudios universitarios de inteligencia en América Latina. Un 26,8% atribuyó esa desconfianza a la asociación de la inteligencia con represión o violaciones a derechos humanos y, un 17,2% la vinculó a la opacidad tradicional de los servicios frente a la sociedad civil. Estos resultados son coherentes con la tesis de Swenson (2003), quien sostiene que "en gran parte de América Latina, la herencia de la Doctrina de Seguridad Nacional ha dejado una huella de sospecha

mutua entre las comunidades de inteligencia y la academia civil" (2003: 109). La relación entre modelo de gobernanza institucional cerrado y dependencia epistemológica resulta, así, bidireccional: la prevalencia del modelo militar-policial limita el acceso civil al campo, y esa exclusión perpetúa la ausencia de producción teórica autónoma.

La construcción de pensamiento estratégico autónomo requiere, como condición previa, el desarrollo de una cultura de inteligencia entendida en su acepción más amplia. En América Latina, la ausencia de esta cultura de inteligencia, en su doble dimensión ciudadana e institucional, constituye tanto una causa como una consecuencia del déficit académico diagnosticado y de la escasa cultura y visión estratégica de largo plazo.

La consolidación de esta cultura de inteligencia demanda un esfuerzo bilateral: por un lado, la sociedad debe mostrar disposición genuina hacia el conocimiento y superar los prejuicios históricos asociados a estos organismos; por otro, los servicios de inteligencia están llamados a asumir compromisos de transparencia controlada, diseño de programas formativos, participación en debates públicos y desarrollo de estrategias editoriales y comunicacionales (Velasco Fernández y Díaz Fernández, 2016, pp. 112-113). Este proceso bidireccional no solo fortalece las reservas de profesionales altamente especializados en análisis y producción de inteligencia, sino que consolida la legitimidad institucional de los servicios, elemento indispensable para el funcionamiento eficaz y democrático de los sistemas de seguridad del Estado. En los contextos latinoamericanos donde este proceso bilateral está aún por consolidarse, la academia civil tiene un rol irreemplazable como catalizador de la legitimidad social del campo y como productora del conocimiento crítico que permite superar la dependencia epistemológica descrita en el eje anterior.

3. Oportunidades estructurales para el desarrollo de programas de posgrado en Inteligencia Estratégica en América Latina

Pese al diagnóstico descrito, el análisis identifica un conjunto de condiciones que configuran una ventana de oportunidad estructural para el desarrollo del campo en la región. Estas oportunidades son tanto de demanda como de oferta, y articulan dimensiones institucionales, curriculares y de cooperación regional.

En el plano de la demanda, el 41,6% de los encuestados consideró que, la creciente demanda de inteligencia estratégica en sectores público y

privado más allá de la seguridad y la defensa, es la oportunidad estructural más relevante para superar la brecha académica. Un 34,4% señaló la creación de una organización Iberoamericana de Estudios en Inteligencia como el mecanismo articulador más prometedor, y un 17,6% destacó la necesidad de producir información propia para reducir la dependencia de inteligencia externa. Esta distribución revela una demanda emergente que desborda el ámbito tradicional de seguridad y defensa, en consonancia con la tesis de que la inteligencia contemporánea "ha dejado de ser exclusivamente un secreto operacional para convertirse en un objeto de estudio necesario para la competencia integral entre Estados" (Corvaja et al., 2016).

En el plano de los incentivos institucionales, el 38,2% de los encuestados consideró que el diseño curricular multidisciplinario, que trascienda seguridad y defensa para incluir economía, tecnología y desarrollo, es el incentivo más efectivo para que universidades latinoamericanas desarrollen posgrados en Inteligencia Estratégica con visión de Estado. El 32,9% identificó el establecimiento de alianzas formales entre universidades y agencias de inteligencia como el segundo incentivo más relevante, y el 20,5% señaló la creación de redes académicas latinoamericanas que articulen formación e investigación. Estos datos son convergentes con la tesis de Corvaja et al. (2016) sobre los beneficios diferenciados de la formación universitaria frente a la capacitación cerrada o in-house: los programas académicos aportan investigación de vanguardia multidisciplinar, mecanismos de reflexión crítica, foros para la cooperación interagencial, académica e industrial, y exposición a marcos teóricos que amplían el horizonte estratégico (2016: 83).

Desde la perspectiva de la construcción de cultura estratégica de Estado, la evidencia sugiere que el paso previo a la creación de programas es la generación de condiciones de confianza entre la academia civil y las comunidades de inteligencia. En este sentido, la experiencia de países líderes de la región como México, Argentina y Colombia muestra que la institucionalización es posible cuando concurren voluntad política, marcos legales específicos y apertura civil de los servicios. El modelo del Intelligence Project del Belfer Center de Harvard, que articula formación, producción de conocimiento y práctica profesional en un ecosistema integrado, constituye una referencia estructural cuya escasa replicación en otros contextos sugiere, precisamente, la magnitud de la oportunidad disponible (Belfer Center, 2026). A nivel europeo, la experiencia del programa Erasmus Mundus IMSISS, que integra perspectivas de inteligencia, seguridad y

estudios estratégicos en consorcio transnacional (IMSISS Erasmus Mundus, s.f.), ofrece un modelo de cooperación académica regional que podría orientar el diseño de una eventual Red Iberoamericana de Estudios en Inteligencia.

La oportunidad estructural identificada adquiere mayor relevancia cuando se contrasta con los beneficios documentados de la formación universitaria frente a los modelos de capacitación in-house. Para los alumnos profesionales en inteligencia con experiencia, los posgrados universitarios fortalecen la comprensión del rol contextual de la inteligencia, las habilidades analíticas, el expertise temático, la resiliencia contra fallos y la actualización metodológica. Para el Estado, contribuyen a formar profesionales altamente calificados, mejorar los estándares analíticos en los servicios de inteligencia, fomentar la cooperación interagencial y contribuir a la seguridad y el desarrollo nacional a través de investigaciones relevantes (Corvaja et al., 2016: 87-88). Este argumento es particularmente poderoso en el contexto latinoamericano: si la sub-institucionalización del campo genera los costos analíticos e institucionales descritos en el diagnóstico, la inversión en formación universitaria especializada representa no un gasto académico, sino una condición de eficacia del sistema de seguridad del Estado.

La creación de maestrías iberoamericanas en inteligencia, programas híbridos civil-militares y una Red Iberoamericana de Estudios en Inteligencia como articulador académico regional no solo cubriría una necesidad formativa urgente, sino que contribuiría a dotar a la región de la capacidad de generar doctrina propia, romper con la dependencia teórica externa y transformar la inteligencia en un instrumento efectivo de poder nacional y competitividad estratégica, que en los términos que Acuff et al. (2022) y Herman (1996) definen como su función esencial. La transferibilidad de los modelos anglosajón y europeo a América Latina no es automática: el vínculo entre academia y agencias que se forjó en esos contextos requirió condiciones políticas, institucionales y culturales específicas, entre ellas, la existencia de una sociedad civil robusta, marcos legales consolidados y una tradición de escrutinio público a los servicios de inteligencia, que en gran parte de América Latina todavía están en construcción. Esta constatación no reduce la oportunidad, sino que la precisa: la formación académica especializada es, en este sentido, no solo una cuestión de calidad analítica, sino también una condición de democratización y legitimación del campo.

En síntesis, los hallazgos confirman que la brecha en el desarrollo de los Estudios de Inteligencia entre las regiones analizadas no es un fenómeno coyuntural ni cuantitativo, sino el resultado de trayectorias históricas e institucionales divergentes que han producido ecosistemas académicos radicalmente desiguales. América Latina enfrenta simultáneamente una debilidad institucional que inhibe la creación de programas, una dependencia epistemológica que limita la producción de conocimiento propio y una desconfianza cultural que restringe la demanda social. No obstante, la creciente demanda de inteligencia estratégica en sectores no tradicionales, el liderazgo incipiente de México, Argentina y Colombia, y el potencial articulador de redes académicas iberoamericanas configuran condiciones favorables para revertir esta tendencia. La creación de posgrados con orientación multidisciplinaria, gobernanza civil y articulación con agencias y sectores privados no solo respondería a una necesidad formativa urgente, sino que constituiría un paso estratégico hacia la construcción de cultura de inteligencia de Estado y la generación de doctrina propia ajustada a las realidades regionales, en los términos que Herman (1996) y Corvaja et al. (2016) definen como condición esencial para la consolidación del campo.

CONCLUSIONES

Los hallazgos de este estudio permiten responder de manera articulada a la pregunta de investigación: los factores que explican la brecha en el desarrollo de la oferta académica de posgrado en Estudios de Inteligencia (EI) entre las regiones analizadas son de naturaleza estructural, epistemológica y cultural. Estos factores actúan de forma sistémica y acumulativa en América Latina, configurando un déficit que no puede atribuirse a causas aisladas ni subsanarse mediante intervenciones puntuales.

En relación con la comparación regional, el estudio revela trayectorias de desarrollo divergentes. Mientras Norteamérica ha consolidado un ecosistema maduro que articula programas académicos (graduate) con profesionales (postgraduate), y el Reino Unido ha legitimado la formación mediante una sólida cultura de escrutinio institucional, Europa Continental ha optado por una vía de especialización técnica en ciberinteligencia y economía. América Latina, en contraste, exhibe una baja densidad institucional, con una oferta concentrada en instituciones de defensa y seguridad, y un perfil curricular de orientación doctrinaria-estatista que suele excluir áreas fundamentales como la ética, el análisis de fallos y la historia de las agencias.

Respecto al diagnóstico del campo en la región, se confirman tres ejes de déficit interrelacionados. La debilidad institucional se manifiesta en la fragmentación de la investigación y la prevalencia de modelos de gobernanza cerrados. La dependencia epistemológica se expresa en la importación de modelos anglosajones sin adaptación contextual, lo que limita la capacidad de generar estimaciones rigurosas y situadas. Finalmente, la ausencia de pensamiento estratégico autónomo posee una dimensión cultural arraigada en la desconfianza hacia la inteligencia, percibida aún como un dominio exclusivo militar-policial y vinculada al legado de la Doctrina de Seguridad Nacional. Estos ejes se retroalimentan en un ciclo donde la exclusión civil perpetúa la carencia de producción teórica propia.

No obstante, la investigación identifica una ventana de oportunidad estructural. Existe una demanda creciente de inteligencia estratégica en sectores no tradicionales que trascienden la seguridad y defensa. El fortalecimiento de incentivos institucionales, tales como el diseño de currículos multidisciplinarios (economía, tecnología y desarrollo) y la creación de una Red Latinoamericana de Estudios en Inteligencia, se perfilan como los mecanismos más prometedores para que las universidades generen una cultura estratégica de Estado.

En síntesis, la sub-institucionalización del campo en América Latina no es solo un vacío académico, sino una vulnerabilidad estratégica que genera costos analíticos directos y dependencia intelectual. Superar la desconexión entre el conocimiento y la acción requiere la creación de maestrías con gobernanza civil y enfoque multidisciplinario. Esta transición no constituye únicamente una respuesta a una necesidad formativa; es una condición indispensable para la democratización, la eficacia operativa y la legitimidad del sistema de seguridad del Estado latinoamericano en el siglo XXI.

REFERENCIAS BIBLIOGRÁFICAS

Aberystwyth University. (s. f.). *MA in War, Strategy and Intelligence*. https://courses.aber.ac.uk/postgraduate/war-strategy-L254/

Acharya, A. (2014a). Global international relations (IR) and regional worlds. *International Studies Quarterly*, *58*(4), 647–659.

Acharya, A. (2014b). *The end of American world order*. Polity Press.

Acuff, J. M., Craft, L., Ferrero, C. J., Kilroy, R. J., y Smith, J. C. (2022). *Introduction to intelligence*. CQ Press.

ANEPE. (s. f.). *Magíster en inteligencia estratégica*. https://anepe.cl/wpcontent/uploads/2021/04/Magister_en_Inteligencia_Estrategica_Programa.pdf

Argentina, Ministerio de Defensa. (s. f.). *Especialización en análisis de inteligencia estratégica*. https://www.argentina.gob.ar/especializacion-en-analisis-de-inteligencia-estrategica

Battaglino, J. (2012). Defense and democracy in Latin America: Reassessing civil-military relations. *Latin American Politics and Society*, *54*(2), 67–89.

Belfer Center for Science and International Affairs, Harvard University. (2026). *Intelligence Project*. https://www.belfercenter.org/project/intelligence

Bloom, B. S. (1956). *Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain*. David McKay.

Brunel University London. (s. f.). *MA in intelligence and security studies*. https://www.brunel.ac.uk/study/courses/intelligence-and-security-studies-ma

Bush School of Government & Public Service, Texas A&M University. (s. f.). *Master of national security & intelligence*. https://bush.tamu.edu/dc/degrees/nsi/

CAEN. (s. f.). *Maestría en inteligencia estratégica*. https://caen.edu.pe/maestria-en-inteligencia-estrategica-2025/

Carleton University. (s. f.). *MA in international affairs with intelligence specialization*. https://carleton.ca/lacs/graduate-studies/

Centeno, M. A., y López-Alves, F. (Eds.). (2001). *The other mirror: Grand theory through the lens of Latin America*. Princeton University Press.

Centro de Altos Estudios Nacionales (CALEN). (s. f.). *Especialización en inteligencia estratégica*. https://www.gub.uy/ministerio-defensa-nacional/calen

Cortés, A., y Cufiño, J. (2022). Cultura estratégica y seguridad nacional en América Latina. *Revista de Estudios en Seguridad Internacional*, *8*(1), 25–48.

Corvaja, A. S., Jeraj, B., y Borghoff, U. M. (2016). The rise of intelligence studies: A model for Germany? *Connections*, *15*(1), 79–106. https://doi.org/10.11610/Connections.15.1.06

Diamint, R. (2015). A new militarism in Latin America. *Journal of Democracy*, *26*(4), 155–168.

Díaz Fernández, A. M. (Ed.). (2016). *Conceptos fundamentales de inteligencia*. Tirant lo Blanch.

Dimitrijević, B. (2023). Intelligence studies between political science, international relations and security studies. *Security and Intelligence Studies*, *5*(1), 1–18.

Dimitrijević, I. R. (2023). Intelligence Studies – An Academic Discipline? En *Strategic Intersections* (pp. 42-55).

Dulles, A. W. (1965). *The craft of intelligence*. Signet Books. (Trabajo original publicado en 1963).

Escuela de Inteligencia y Contrainteligencia BG. Ricardo Charry Solano (ESICI). (s. f.). *Maestría en inteligencia estratégica*. https://esici.edu.co/index.php/maestria/

Esteban Navarro, M. Á. (2007). *Glosario de inteligencia*. Ministerio de Defensa de España.
Gallego, F., Sanhueza, R., y Arin, K. P. (2005). Military regimes and economic performance. *Journal of Applied Economics*, *8*(1), 113–138.
Gearon, L. F. (Ed.). (2020). *The Routledge international handbook of universities, security and intelligence studies*. Routledge.
Georgetown University. (s. f.). *MA in security studies (intelligence concentration)*. https://sfs.georgetown.edu/ma-security-studies/curriculum/concentrations/
Gómez, G. (2023). *Intelligence and policymaking: The opportunity for a more collaborative approach*. fp21.
Goodman, M. S., y Omand, D. (2008). What analysts need to understand: The King's intelligence studies program. *Studies in Intelligence*, *52*(4), 1–12.
Grace, M. (2022). *The intelligence analyst's sourcebook*. Rowman & Littlefield.
Grace, P. (2022). *The intel intellectuals: How social scientists helped legitimise the Central Intelligence Agency (1950–1953)* [Tesis doctoral, University of Otago].
Herman, M. (1996). *Intelligence power in peace and war*. Cambridge University Press.
Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill.
Heuer, R. J., Jr., y Pherson, R. H. (2015). *Structured analytic techniques for intelligence analysis* (2.ª ed.). CQ Press.
Hilsman, R. (1956). Strategic intelligence and national decisions. *World Politics*, *8*(4), 576–588.
Institute of World Politics. (s. f.). *MA in strategic intelligence studies*. https://www.iwp.edu/academics/graduate-degree-programs/master-of-arts-in-strategic-intelligence-studies/
Johns Hopkins University SAIS. (s. f.). *Master of arts in strategy, cybersecurity, and intelligence (MASCI)*. https://sais.jhu.edu
Kendall, W. (1949). The function of intelligence. *World Politics*, *1*(4), 542–552.
Kent, S. (1966). *Strategic intelligence for American world policy*. Princeton University Press. (Trabajo original publicado en 1949).
King's College London. (s. f.). *MA in intelligence and international security*. https://www.kcl.ac.uk
Leal Buitrago, F. (1992). Surgimiento, auge y crisis de la doctrina de seguridad nacional en América Latina y Colombia. Análisis Político, (15), 6–34. https://revistas.unal.edu.co/index.php/anpol/article/view/74379.
Levin Center. (2024, October 31). Portraits in oversight: Frank Church and the Church Committee. https://levin-center.org/frank-church-and-the-church-committee/
LISA Institute. (s. f.). *Máster en inteligencia*. https://www.lisainstitute.com
Matei, F. C., Halladay, C., y Estévez, E. E. (2022). *The handbook of Latin American and Caribbean intelligence cultures*. Bloomsbury.
Mercyhurst University. (s. f.). *MSc in applied intelligence*. https://www.mercyhurst.edu/academics/intelligence-studies

Michael, K., y Kornbluth, A. (2019). The academization of intelligence. *Cyber, Intelligence, and Security*, *3*(1), 117–140.
National Intelligence University. (s. f.). *MSc in strategic intelligence (MSSI)*. https://www.ni-u.edu/mssi/
National Intelligence University. (s. f.). *MSc in strategic technology intelligence (MSTI)*. https://www.ni-u.edu/msti-2/
Northeastern University. (s. f.). *Master of arts in national security and intelligence*. https://cps.northeastern.edu/program/master-of-arts-in-national-security-and-intelligence-boston/
Pettee, G. S. (1946). *The future of American secret intelligence*. Infantry Journal Press.
Platt, W. (1961). *National character in action: Intelligence factors in foreign relations*. Rutgers University Press.
Sans-Rubert Pascual, D., y Pulido-Gragera, J. (2022). Cultura de inteligencia y sociedad. *URVIO*, (34), 41–57. https://doi.org/10.17141/urvio.34.2022.5738
Schenoni, L. (2016). Subsystemic unipolarities? *Strategic Studies Quarterly*, *10*(1), 48–73.
Security, Intelligence and Strategic Studies – Erasmus Mundus. (s. f.). *International master in security, intelligence, and strategic studies*. https://www.securityintelligence-erasmusmundus.eu/
Shapira, I. (2025). *Israeli national intelligence culture: Problem-solving, exceptionalism, and pragmatism*. Routledge.
Spracher, W. C. (2009). *National security intelligence professional education* [Tesis doctoral, The George Washington University].
Suárez, A. (2021). *Ciencia policial: fundamentos de la seguridad pública*. Brasilia: ADP Editora. (pp. 357-358).
Swenson, R. G. (2003). Intelligence education in the Americas. *International Journal of Intelligence and CounterIntelligence*, *16*(1), 108–130.
The Citadel. (s. f.). *Intelligence and security studies*. https://www.citadel.edu/intelligence-and-security-studies/
Tickner, A. B., y Waever, O. (Eds.). (2009). *International relations scholarship around the world*. Routledge.
Universidad CEU San Pablo. (s. f.). *Máster en dirección, operaciones y análisis de inteligencia*. https://www.uspceu.com
Universidad de Lorraine. (s. f.). *Master intelligence économique*. https://formations.univ-lorraine.fr
Universidad Isabel I. (s. f.). *Máster en inteligencia y seguridad*. https://www.ui1.es
}Universidad Nacional de La Plata (UNLP). (s. f.). *Maestría en inteligencia estratégica nacional*. https://unlp.edu.ar
Universidad Nebrija. (s. f.). *Máster en análisis de inteligencia y ciberinteligencia*. https://www.nebrija.com
Universidad Rey Juan Carlos. (s. f.). *Máster en analista de inteligencia*. https://www.urjc.es
University of South Florida. (s. f.). *M.S. intelligence studies*. https://www.usf.edu/arts-

sciences/departments/information/graduate/ms-intelligence-studies.aspx
University of Texas at Austin. (s. f.). *Intelligence studies project / Texas intelligence academy*. https://clements.utexas.edu/intelligence-studies
Velasco Fernández, F., y Díaz Fernández, A. (2016). Cultura de inteligencia. En A. M. Díaz Fernández (Ed.), *Conceptos fundamentales de inteligencia* (pp. 109–117).

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

Del secreto al conocimiento: los estudios de inteligencia en perspectiva histórica

Álvaro Cremades Guisado*

Resumen: Este artículo analiza el desarrollo histórico de los estudios de inteligencia como campo de estudio, atendiendo a las condiciones que han marcado su configuración. Mediante una metodología cualitativa, de carácter documental e histórico-interpretativo, el trabajo reconstruye la evolución de este ámbito desde su fase de emergencia tras la Segunda Guerra Mundial hasta su actual expansión temática, geográfica y metodológica. En primer lugar, se examina el surgimiento de los estudios de inteligencia a partir de las primeras aportaciones doctrinales elaboradas por antiguos profesionales de la inteligencia estadounidense, así como la progresiva aparición de un vocabulario, una literatura especializada y unos marcos iniciales de reflexión. En segundo lugar, se aborda la institucionalización temprana del campo, favorecida por los procesos de desclasificación, los escándalos políticos y la creación de espacios académicos y editoriales especializados, especialmente en Estados Unidos y Reino Unido. Posteriormente, se analiza su fase de consolidación, caracterizada por una mayor interlocución entre servicios de inteligencia y universidad, así como por una reflexión creciente sobre la identidad y autonomía del campo de estudio. Finalmente, el artículo pone de relieve que los estudios de inteligencia atraviesan hoy una fase de expansión geográfica, temática y metodológica que abre nuevas expectativas para el futuro del campo de estudio.

Palabras clave: estudios de inteligencia; servicios de inteligencia; comunidad de inteligencia; historia de la inteligencia.

* Director del Máster Universitario en Seguridad y Defensa de la Universidad Antonio de Nebrija. Licenciado en Ciencias Políticas y de la Administración por la Universidad Complutense de Madrid; Máster en Analista de Inteligencia por la Universidad Rey Juan Carlos y la Universidad Carlos III de Madrid; Doctor en Ciencia Política y de la Administración y Relaciones Internacionales por la Universidad Complutense de Madrid, obteniendo la calificación de sobresaliente cum laude y Premio Extraordinario de Doctorado.

This article analyses the historical development of intelligence studies as a field of study, paying particular attention to the conditions that have shaped its configuration. Through a qualitative methodology of a documentary and historical-interpretive nature, the article reconstructs the evolution of this field from its phase of emergence after the Second World War to its current thematic, geographical, and methodological expansion. First, it examines the rise of intelligence studies through the early doctrinal contributions produced by former U.S. intelligence professionals, as well as the gradual emergence of a specialised vocabulary, a dedicated body of literature, and initial analytical frameworks. Second, it addresses the field's early institutionalisation, fostered by declassification processes, political scandals, and the creation of specialised academic and editorial spaces, particularly in the United States and the United Kingdom. It then analyses its phase of consolidation, characterised by greater interaction between intelligence services and universities, as well as by a growing reflection on the identity and autonomy of the field. Finally, the article highlights that intelligence studies are currently undergoing a phase of geographical, thematic, and methodological expansion that opens up new prospects for the future of the field.

Keywords: intelligence studies; intelligence services; intelligence community; intelligence history.

Introducción

En las últimas décadas, la inteligencia ha dejado de ser contemplada únicamente como una práctica reservada al secreto de Estado para convertirse también en un objeto legítimo de análisis académico. Ello no constituye un cambio menor, pues durante mucho tiempo la inteligencia fue concebida como una actividad estrictamente operativa, vinculada al espionaje, la seguridad nacional y la guerra, que se presentaba como una realidad opaca y vergonzante ante la que las Ciencias Sociales debían mantener prudente distancia. Sin embargo, la progresiva institucionalización de los servicios de inteligencia en el Estado contemporáneo, el aumento de la disponibilidad de fuentes documentales y el interés creciente por comprender la relación entre información y poder han favorecido la aparición y el desarrollo de un campo específico de reflexión: los estudios de inteligencia. Este campo, hoy relativamente consolidado en determinados entornos académicos, ha experimentado una evolución compleja, desigual y profundamente condicionada por factores históricos, políticos, institucionales y epistemológicos.

El examen del desarrollo histórico de los estudios de inteligencia resulta relevante por varias razones. En primer lugar, porque permite

comprender cómo una práctica tradicionalmente asociada al secreto, a la excepcionalidad y a la razón de Estado ha ido adquiriendo carta de naturaleza dentro del mundo universitario. En segundo lugar, porque pone de manifiesto que dicho proceso no ha sido lineal ni uniforme, sino que ha dependido de contextos nacionales concretos, de distintos niveles de apertura de los archivos, del grado de profesionalización de las comunidades de inteligencia y de la capacidad de las instituciones académicas para incorporar esta temática dentro de sus agendas de investigación y docencia. En tercer lugar, porque el propio recorrido histórico del campo revela tensiones todavía vigentes: la distancia entre académicos y profesionales, la escasa sistematización teórica de parte de la literatura, el predominio de determinadas tradiciones nacionales y la dificultad de construir marcos comparativos que permitan trascender la experiencia particular de las naciones que ejercieron como pioneras en este campo de estudio. Así, estudiar la trayectoria de los estudios de inteligencia no solo implica reconstruir su pasado, sino también identificar los límites y desafíos que condicionan su presente.

Para alcanzar los propósitos aquí señalados, la metodología empleada a lo largo de este trabajo se basa en una estrategia de investigación cualitativa, de carácter documental, histórico-interpretativo y con finalidad exploratoria, orientada a reconstruir la evolución de los estudios de inteligencia como campo de estudio y a identificar las principales coyunturas que han marcado su desarrollo, con el fin de establecer una periodización de su desarrollo. Para ello, se ha recurrido al análisis de corpus bibliográfico especializado siguiendo un criterio intencional con el propósito de trazar una visión diacrónica del objeto de estudio.

Conviene señalar, finalmente, que este diseño presenta algunas limitaciones. Al tratarse de una investigación documental, depende de la disponibilidad desigual de literatura y de la propia asimetría del campo, históricamente dominado por la producción angloamericana. Asimismo, la periodización propuesta tiene un alcance interpretativo y no pretende clausurar otras lecturas posibles sobre la evolución de los estudios de inteligencia. Precisamente por ello, el trabajo se plantea como una contribución de síntesis y ordenación crítica del campo, susceptible de ser ampliada en futuras investigaciones mediante análisis bibliométricos, estudios comparados o aproximaciones centradas en ámbitos regionales específicos, especialmente en América Latina.

El desarrollo histórico de los estudios de inteligencia
Fase de emergencia (1940-1970)

Aunque el uso del conocimiento para apoyar la toma de decisiones ha sido una constante en la historia de las sociedades humanas (tradicionalmente, a través de la práctica del espionaje (Navarro, 2009)), los servicios de inteligencia en el sentido contemporáneo del término son producto de procesos de institucionalización relativamente recientes, cuando, a finales de la Segunda Guerra Mundial, varios Estados constataron la utilidad de contar con grandes y permanentes organizaciones dedicadas a tal propósito. Sin embargo, en la actualidad, la práctica totalidad de naciones cuentan con algún tipo de organización dedicada a la producción de inteligencia. De hecho, la mayor parte de los Estados no cuentan con una única organización para tal labor, sino que en ellos conviven una multiplicidad de entidades de diferente naturaleza; lo que ha venido a denominarse "comunidad de inteligencia". Este es un concepto acuñado en el proceso de institucionalización de la inteligencia estadounidense tal y como la conocemos hoy, con el propósito fundamental de articular, aún de forma vaga y difusa, los entonces dispersos esfuerzos de diferentes organismos dedicados a la producción de inteligencia ubicados en diferentes ramas del gobierno federal. Más particularmente, el término comunidad de inteligencia es utilizado por primera vez de manera oficial en el marco de la Comisión sobre la Organización de la Rama Ejecutiva del Gobierno, también conocida como Segunda Comisión Hoover, en mayo de 1955, constituida con el propósito de optimizar el funcionamiento de las actividades gubernamentales, incluyendo un informe presentado por el Grupo de Trabajo sobre Actividades de Inteligencia. Dicho documento afirma que "la maquinaria para el cumplimiento de nuestros objetivos de inteligencia, en lo sucesivo denominada comunidad de inteligencia en su conjunto, incluye la Agencia Central de Inteligencia, el Consejo de Seguridad Nacional, la Agencia de Seguridad Nacional, la Oficina Federal de Investigaciones, las secciones de inteligencia del Departamento de Estado, del Ejército, de la Armada y de la Fuerza Aérea; y de la Comisión de Energía Atómica" (Second Hoover Commission, 1955, 663-664). Aunque durante las primeras décadas tras la primera referencia oficial a la comunidad de inteligencia, este concepto encontraría inicialmente una acogida desigual en los Estados Unidos (Troy, 1988), pero terminaría siendo empleado en este y otros países para referirse al conjunto de organizaciones que se dedican a la producción de inteligencia, haciendo

énfasis en la colaboración entre ellas, incluso a través de la constitución de un organismo director de dicho sistema.

No es de extrañar, en consecuencia, que el nacimiento de los estudios de inteligencia como campo de estudio se remonte, aun con algunos antecedentes[14], a los años posteriores al enfrentamiento bélico. Esta inicial fase de emergencia sería posible gracias al interés de diversos académicos que habían servido como miembros en activo de diferentes servicios de inteligencia de los Estados Unidos quienes se posicionarían como sus principales impulsores: en 1946, George S. Pettee, profesor en la Universidad de Harvard y director de *European Enemy Division* perteneciente a la *Foreign Economic Administration*, publica su libro *The Future of American Secret Intelligence*, exponiendo algunas de las particularidades institucionales de la inteligencia en los Estados Unidos y su desempeño en el conflicto bélico (Pettee, 1946); dos años después, los tenientes coroneles Robert R. Glass y Phillip B. Davidson publicarían *Intelligence is for commanders*, en el que sitúan los principales elementos doctrinales en el uso de la inteligencia militar, incluyendo la primera referencia registrada del conocido como "ciclo de inteligencia" (Glass y Davidson, 1948); en 1949 vería la luz *Strategic Intelligence for American World Policy*, de Sherman Kent (1949), profesor de la Universidad de Yale y oficial de la Oficina de Asuntos Estratégicos (OSS, por sus siglas en inglés) y de la Agencia Central de Inteligencia (CIA, por sus siglas en inglés), libro que es considerado por muchos como la obra inaugural de los estudios de inteligencia en los Estados Unidos; Willmoore Kendall (1949) publicaría en 1949 una reseña sobre el libro de Kent, planteando una sucesión de críticas sobre algunos de sus postulados dando lugar a un desencuentro intelectual de implicaciones todavía presentes en muchos servicios de inteligencia (Davis, 1992).

[14] Es necesario reconocer aquí la existencia de algunas obras relativas de una u otra forma a la inteligencia aparecidas con anterioridad al periodo histórico objeto de discusión en el presente artículo. Entre todas ellas, destacan los trabajos de Richard Wilmer Rowan, autor de obras como Spy and Counter-Spy: The Development of Modern Espionage (1928), que ofrece una síntesis histórica del espionaje moderno en un tono fundamentalmente narrativo; o The Story of Secret Service (1939), mediante la que establecer una historia general del espionaje a escala global. Resultan igualmente reseñables las obras de antiguos profesionales de la inteligencia como Nicolai (1924), exdirector de inteligencia del Ejército Imperial Alemán; o Yardley (1931), exintegrante de la Cable and Telegraph Section del MI-8 (primera unidad de inteligencia de señales en la inteligencia militar estadounidense). Sin embargo, es igualmente necesario señalar que esta producción se desarrolló de manera dispersa y escasamente sistematizada, con enfoques eminentemente narrativos y/o biográficos, por lo que no debe ser considerada como constituyente del campo de estudio.

Durante la década de los cincuenta, otras personalidades de la incipiente comunidad de inteligencia estadounidense publicarían diversos trabajos sobre aspectos relacionados con la función de inteligencia: por su parte, Washington Platt (1957) realizaría importantes contribuciones al estudio de la metodología empleada por los analistas de inteligencia; Roger Hilsman (1956), por otro lado, desentrañaría el vínculo existente entre la política exterior estadounidense y los servicios de inteligencia. Sin embargo, pese a la producción bibliográfica registrada en años anteriores, Kent sería consciente de las limitaciones que los estudios de inteligencia aún adolecían para consolidarse como un campo de estudio, haciendo referencia directa a la ausencia de literatura especializada[15]. Con el propósito de hacer frente a esta carencia, y bajo la influencia de Kent, nacería en 1955 la primera publicación especializada en este campo, *Studies in Intelligence*, promovida por la Oficina de Entrenamiento de la CIA y contando con las contribuciones de destacados integrantes de la comunidad de inteligencia de los Estados Unidos (Dujmovic, 2005).

Fase de institucionalización temprana (1970-1990)

Durante la década de los setenta, tal y como señala Johnson (2014), los sucesivos escándalos acaecidos en la comunidad de inteligencia estadounidense servirían como facilitador de un salto cuantitativo y cualitativo en el estudio de inteligencia. En 1975, año conocido como *Year of Intelligence* (Dylan y Gioe, 2020), cuatro investigaciones oficiales paralelas (conocidas como Comité Rockefeller, Comité Church, Comité Pike y Comité Murphy) se desarrollarían con el propósito de indagar en el funcionamiento y extralimitación de diferentes instituciones pertenecientes a la comunidad de inteligencia estadounidense, lo que permitiría a los investigadores trabajar con acceso a fuentes primarias gracias a la amplia cantidad de material desclasificado. En el caso del Reino Unido, según Moran (2011), el interés por los asuntos relativos a la inteligencia aumentaría no tanto

[15] "La inteligencia hoy no es meramente una profesión, sino que, como la mayoría de las profesiones, ha asumido los rasgos de una disciplina: ha desarrollado una metodología reconocida; ha desarrollado un vocabulario; ha desarrollado un cuerpo de teoría y doctrina; ha elaborado y perfeccionado técnicas. Ahora cuenta con una amplia comunidad profesional. Lo que le falta es una literatura. (…) Mientras esta disciplina carezca de una literatura, su método, su vocabulario, su cuerpo doctrinal e incluso su teoría fundamental corren el riesgo de no alcanzar nunca una plena madurez. No diré que no se pueda tener una disciplina sin una literatura, pero sí afirmaré que es poco probable que se tenga una disciplina sólida y en crecimiento sin ella" (Kent, 1955, 3).

como producto de mejores condiciones de acceso a material de archivo, sino por la publicación de toda una serie de obras relativas al papel de la inteligencia británica durante la segunda guerra mundial por parte de algunos de sus antiguos integrantes, entre las que destacan los trabajos de Winterbotham (1974) y de Hinsley (1979). Esta ventana de oportunidad abierta para la investigación en asuntos tan inexplorados como los relativos a la inteligencia atraería la atención de académicos procedentes de disciplinas consolidadas, lo que daría pie a un esfuerzo teórico más intenso del que se había realizado hasta ese momento (Phythian, 2022).

Gracias a lo anterior, a mediados de la década de los ochenta comienzan a materializarse una serie de iniciativas que pondrían de manifiesto la consolidación del campo de estudios, o lo que podemos considerar una fase de institucionalización. La creación de la Sección de Estudios de Inteligencia en el seno de la Asociación de Estudios Internacionales (ISA) en 1985 representa un hito fundamental, en la medida que supone el reconocimiento del campo de estudio por parte de disciplinas de mayor recorrido, así como una plataforma fundamental para la dinamización e internacionalización de los Estudios de Inteligencia. Es también en estos años cuando ven la luz las primeras publicaciones científicas dedicadas a este campo de estudio, *Intelligence & National Security* (1986) y más tarde International *Journal of Intelligence and Counterintelligence* (Brown y Dowden, 1986), todavía hoy referentes en el campo de estudio.

Durante esta misma década, la aparición de literatura especializada en inteligencia experimenta un crecimiento superlativo gracias al apoyo de editoriales universitarias y otras editoriales independientes, como Frank Cass & Co. Como consecuencia de las controversias suscitadas respecto a la comunidad de inteligencia estadounidense, Godson iniciaría la publicación de la serie de obras colectivas *Intelligence Requirements for the 1980's*, que a lo largo de siete volúmenes recogería las contribuciones de diferentes autores agrupados en torno al *Consortium for the Study of Intelligence* (Godson, 1979). Destacan igualmente los trabajos de Richelson (1985) y Johnson (1985), dedicados a exponer la arquitectura institucional de la comunidad de inteligencia estadounidense y los pormenores de las investigaciones oficiales iniciadas en 1975, respectivamente. Ya en 1987 Michael Handel publica con Frank Cass & Co. (adquirida por Routledge en 2003) la obra colectiva *Strategic and Operational Deception in the Second World War* (Handel, 1989), primera referencia producto de la serie de conferencias internacionales *Intelligence and Military Operations* celebradas

en el *US Army War College* durante la segunda mitad de la década y editadas como número especial de *Intelligence & National Security*, inaugurando lo que a la postre sería la serie Studies in Intelligence de Routledge.

En el Reino Unido, los primeros trabajos de Christopher Andrew supondrían un incuestionable punto de inflexión: primero, con *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century* (Andrew y Dilks, 1984), levantando una considerable expectación en torno a un objeto de estudio tan fuertemente inexplorado (Phythian, 2018; Van Puyvelde, 2020); y, un año más tarde, con *Secret Service: The Making of British Intelligence Community* (Andrew, 1985), que pondría de manifiesto la viabilidad de la investigación histórica en el ámbito de los estudios de inteligencia aun en condiciones de acceso no tan propicias como las ya existentes en Estados Unidos (Phythian, 2017). De este modo, Watt (1988) señala pocos años más tarde la existencia de una escuela británica emergente en los estudios de inteligencia, con claro protagonismo de la investigación historiográfica.

En definitiva, a lo largo de la década de los ochenta se producen hitos fundamentales para los estudios de inteligencia, cuyos frutos serían determinantes en el desarrollo posterior de lo que entonces comenzaría a entenderse como un campo de estudio con identidad propia. De este modo, en palabras de Stafford (1988, 217), "Aunque la literatura sobre inteligencia se remonta en realidad a varios milenios atrás, solo recientemente se ha vuelto lo bastante popular entre los académicos como para merecer aceptación académica, si no respetabilidad. (…) Se publican regularmente artículos sobre inteligencia en revistas profesionales y académicas, y varias revistas están dedicadas específicamente a la investigación en inteligencia. Los Estudios de Inteligencia constituyen hoy un campo reconocido de actividad académica y erudita".

Fase de consolidación (2000-2020)

Con el paso del tiempo, y ya con un pleno arraigo institucional, terminaría por constatarse la necesidad de articular mecanismos de interlocución respecto a otros actores e instituciones no pertenecientes a esta. Más particularmente, en la década de los noventa, con la transformación del entorno estratégico a consecuencia del fin de la Guerra Fría, se suscita en los Estados Unidos una fuerte preocupación

sobre el desempeño de la Comunidad de Inteligencia ante este nuevo escenario, tratando de identificar líneas de acción que permitan mejorar su cometido en un contexto general de desfinanciarización. Entre ellas, se encuentra la creación de programas de reserva que permitan aprovechar el conocimiento existente fuera de la Comunidad de Inteligencia que pueda resultar de interés para la seguridad nacional. Así, según el informe presentado por el Comité de Inteligencia de la Cámara de Representantes en 1995, "la habilidad de aumentar los recursos analíticos y capitalizar la experticia existente fuera de la Comunidad de Inteligencia será clave para la efectividad de esta en la entrada del siglo XXI (…). Esta capacidad debería ser aumentada mediante un programa de reserva civil de la Comunidad de Inteligencia, en la cual expertos no pertenecientes a ella (en la academia, la empresa, etcétera) puedan proveer de información en curso sobre alertas y tendencias y para ser utilizados durante las crisis para aumentar los activos de la Comunidad de Inteligencia" (Permanent Select Committee On Intelligence, 1996, 32-33)[16].

En un contexto como este, la comisión de acciones terroristas de alto impacto por parte de la organización terrorista internacional Al Qaeda supondría un fuerte revulsivo para el campo de estudio. Se produciría entonces un aumento drástico de los programas especializados en inteligencia y seguridad nacional (Thomas y Dujmovic, 2019), gran parte de los cuales adoptarían una orientación marcadamente contraterrorista (Dahl y Viola, 2017). De la misma forma, el debate suscitado sobre el desempeño de la comunidad de inteligencia estadounidense frente a la amenaza terrorista daría lugar a una considerable producción científica sobre fallos de inteligencia y sorpresas estratégicas (Betts, 2002; Goodman, 2003; Dahl, 2005; Marrin, 2011), al mismo tiempo que la promulgación de la *Intelligence Reform and Terrorism Prevention Act* (IRTPA) de 2004 abriría nuevas y viejas controversias sobre la arquitectura institucional de la inteligencia estadounidense (Zegart, 2005; Sims y Gerber, 2005; Svendsen, 2008; Lahneman, 2004).

Es principalmente a partir de este momento cuando se establece una relación abierta, formal y fluida (aun con limitaciones) entre los

[16] De manera posterior, esta noción daría pie a lo que ha venido a denominarse "comunidades ampliadas de inteligencia", marcos institucionales en los que sería posible incorporar a grupos de interés en esta materia no solo como meros repositorios de información, sino también permitiendo su colaboración directa y sostenida con los servicios de inteligencia, incluyendo entidades universitarias (Arcos y Antón, 2014).

servicios de inteligencia y el ámbito universitario. En España, con la creación del Centro Nacional de Inteligencia en 2002 se inaugura la denominada política de cultura de inteligencia, dirigida a la creación de un marco general de interlocución con entidades no pertenecientes a la comunidad de inteligencia, con el ámbito universitario como uno de sus principales objetivos, con la creación de la Cátedra de Servicios de Inteligencia y Sistemas Democráticos de la Universidad Juan Carlos I (Arcos, 2013; Cremades y Bueno, 2022). Algunos años más tarde, en 2005, con la creación de la Oficina del Director de Inteligencia Nacional en Estados Unidos se impulsaría el programa de Centros de Excelencia Académica de la Comunidad de Inteligencia (IC CAE), por el cual la comunidad de inteligencia estadounidense establecería programas de cooperación con entidades universitarias para fomentar programas formativos especializados e investigación aplicada (United States Government Accountability Office, 2019). De este modo, la creación de nuevas titulaciones universitarias especializadas y abiertas al público general bajo patrocinio institucional supondría no solo una vía de atracción del talento para los servicios de inteligencia, sino que ello también facilitaría la normalización de la relación entre estos y el mundo universitario (Arcos, 2013; Glees, 2015), así como la consiguiente dinamización del campo de estudio.

Es pertinente señalar que, llegados a este punto, los estudios de inteligencia dejan paulatinamente de encontrarse prácticamente circunscritos a Estados Unidos y Reino Unido para experimentar una primera expansión en su alcance. El campo de estudios emerge entonces en Europa continental, dando lugar a nuevos programas formativos dedicados a la inteligencia; y a nuevas publicaciones especializadas como Inteligencia y seguridad: Revista de análisis y prospectiva (2006), Journal for Intelligence, Propaganda and Security Studies (2007), Romanian Intelligence Studies Review (2009) o Journal of Mediterranean and Balkan Intelligence (2013). Por otra parte, con el muy temprano precedente de la Revista de la Escuela Nacional de Inteligencia en Argentina (1992, reeditada en 2002 como Nueva Inteligencia), en diferentes países latinoamericanos se fundan las primeras revistas especializadas, como Inteligencia Total en 2003, Revista Brasileira de Inteligencia en 2005 o Perspectivas en Inteligencia en 2009.

Un atributo característico de esta fase de consolidación es el énfasis en la reflexión sobre la configuración del propio campo de estudio. La "reflexividad disciplinar" encontraría un notable desarrollo en las publicaciones especializadas, incidiendo en el propósito de los estudios

de inteligencia y su estatuto científico, además de evaluar los avances en este campo de estudio. Llegados a este punto, la debilidad de los estudios de inteligencia no radicaría en la pretérita escasez de producción científica (pues era ya relativamente abundante para entonces), sino más bien en su escasa sistematización, que Marrin describe de la siguiente manera: "la literatura sobre inteligencia es rica en historia, pero también resulta cerrada sobre sí misma y teóricamente poco desarrollada, quizá debido a un fracaso generalizado a la hora de garantizar la acumulación y agregación del conocimiento a lo largo del tiempo" (Marrin, 2016, 4). En esta misma dirección de reflexividad disciplinar avanzarían Gill y Phythian (2016) para incidir de forma más clara en la identidad del campo de estudio y su relación con la práctica profesional de la inteligencia, reivindicando su autonomía relativa.

Una de las muestras más ilustrativas de este afán por la reflexividad disciplinar propio de la fase de consolidación de los estudios de inteligencia lo encontramos en el informe publicado por Johnson y Shelton (2013), editores de *Intelligence & National Security*, como resultado de una encuesta realizada a los integrantes del consejo editorial de dicha revista. En su contenido, se trasluce que, una vez alcanzado un cierto arraigo institucional, los estudios de inteligencia comenzaron a interrogarse de manera explícita sobre su propia identidad, sus límites y sus posibilidades de desarrollo. Lejos de reflejar un campo plenamente cerrado, el texto muestra un ámbito en proceso de maduración, atravesado por debates sobre su definición, su relación no siempre satisfactoria con las disciplinas académicas tradicionales, la brecha entre académicos y profesionales, la conveniencia de diversificar metodologías y la persistencia del secreto como obstáculo estructural para la investigación.

Fase de expansión (2020-actualidad)

Como ha podido comprobarse, a lo largo de este recorrido histórico los estudios de inteligencia han tenido un desarrollo desigual entre naciones, lo que ha llevado a un fuerte predominio del mundo angloparlante en este campo de estudio. Según Van Puyvelde y Curtis (2016), tras analizar 1913 trabajos publicados entre 1986 y 2015 en *Intelligence & National Security* e *International Journal of Intelligence and Counterintelligence*, concluyeron que existía un claro protagonismo de autores estadounidenses o ingleses (con 1066 y 608, respectivamente), que toman mayoritariamente como objeto de estudio organizaciones dedicadas a la producción de inteligencia radicadas en los EE. UU. y el

Reino Unido (996 y 519, respectivamente). Entre las causas que pueden haber conducido a esta situación pueden señalarse, entre otras, el papel protagonista de los Estados Unidos y sus servicios de inteligencia en el devenir histórico de la segunda mitad del siglo XX; la ventaja tecnológica y en materia de inteligencia estadounidense, y las consiguientes relaciones de dependencia a escala global; la alta disponibilidad de información de acceso público sobre la comunidad de inteligencia estadounidense, y entre ella, una gran cantidad de documentación desclasificada; el alto grado de internacionalización de la literatura especializada procedente de los EE. UU., y la habitual participación de expertos que han tenido una trayectoria en la comunidad de inteligencia estadounidense en los comités editoriales de algunas de las principales revistas del sector, como las ya mencionadas anteriormente (Cremades-Guisado y Cancelado-Franco, 2021).

A consecuencia del predominio angloparlante anteriormente referido, la diversidad de los estudios de inteligencia se ha visto limitada, recluyendo a la casuística existente fuera de la angloesfera en su periferia disciplinar (Aldrich y Kasuku, 2012). Se impone de esta forma una concepción positivista acerca del desarrollo histórico de los servicios de inteligencia, en base a la cual el modelo anglosajón, y particularmente el estadounidense, se introduce como canon para el conjunto de comunidades de inteligencia del resto del planeta; un modelo aspiracional que, al mismo tiempo que posiciona a los Estados Unidos en la cúspide, excluye tácitamente otras experiencias en este campo por considerarlos de menor relevancia. De este modo, "el sur global está notablemente ausente de los textos dominantes sobre teoría de la inteligencia o metodología de investigación en inteligencia. Estas obras de metanivel son importantes, pues constituyen los principales estudios conceptuales para un tema que es a menudo visto como subteorizado" (Shiraz y Aldrich, 2019, 4). Esta innegable carencia deja importantes obstáculos teóricos y metodológicos a quienes inician investigaciones sobre las comunidades de inteligencia en áreas geográficas marginadas hasta el momento, al tener estas sus propias culturas institucionales y al desenvolverse en contextos sociopolíticos profundamente disímiles, como es el caso de países en proceso de transición política y/o entornos de fragilidad estatal, que presentan realidades no necesariamente homologables a las de aquellos países que han recibido mayores cotas de protagonismo de los estudios de inteligencia.

A partir de lo anterior, puede afirmarse que durante los últimos años los estudios de inteligencia han entrado en una fase de expansión. Por

un lado, en términos geográficos, además de una producción local desigual que parte de décadas anteriores, diferentes plataformas editoriales de habla inglesa han comenzado a introducir paulatinamente, aún de forma muy minoritaria, trabajos dirigidos a aumentar el conocimiento del que disponemos acerca de las realidades tradicionalmente excluidas en este ambiente (Shaffer, 2023; Chaya, 2023; Matei et al, 2024; Shaffer, 2024; Shaffer y Ashraf, 2025; Gwatiwa, 2025; Lebakeng y Gwatiwa). Al mismo tiempo, en términos temáticos, se ha producido una creciente diversificación de la agenda de investigación, que de forma cada vez más palpable incluye aspectos relativos a la inteligencia más allá de los asuntos canónicos del campo de estudio, como el espionaje, el secreto de Estado, la estrategia militar, entre otros (Willmetts, 2019; Ben Jaffel y Larsson, 2024). Por último, también se ha manifestado una mayor variedad metodológica: más allá de la investigación histórica tradicional, en la actualidad encontramos muy diferentes aproximaciones, tales como la etnografía (Nolan, 2018; Basic y Yakhlef, 2022), los grupos focales (Sudkamp et al., 2022), la entrevista (Ben Aharon, 2023), los métodos mixtos (Oomens, van Wegberg y Klievink, 2024), el análisis cuantitativo de contenido (McLoughlin, Ward, y Lomas, 2020) o la encuesta (Díaz-Fernández y Del-Real, 2026).

Por último, cabe destacar que, de manera reciente, y a semejanza de otros campos de estudio más consolidados en el seno de la disciplina de las Relaciones Internacionales como los estudios de seguridad o los estudios de terrorismo, han emergido diversas aproximaciones no convencionales al estudio de la inteligencia que han sido nominalmente agrupadas como "estudios críticos de inteligencia". Al igual que la existente en otros campos de estudio y disciplinas de las Ciencias Sociales, la teoría crítica en los Estudios de Inteligencia se presenta como una alternativa a los planteamientos tradicionales que han imperado en este campo de estudio, con el propósito fundamental de poner de manifiesto las estructuras de poder que imperan en las sociedades humanas y sus instituciones y promover así "la emancipación del hombre de la esclavitud" (Horkheimer, 2002, 246).

En ese sentido, de acuerdo con Bean, de Werd e Ivan (2021), el estudio y la práctica de la inteligencia se han construido frecuentemente en torno a abstracciones disfuncionales, de modo que los estudios críticos de inteligencia "llaman a una desreificación intencional de la institución de inteligencia, es decir, la deconstrucción de las imágenes esencialistas de la práctica de la inteligencia" (Bean, de Werd e Ivan, 2021, 3). Para Goldewijk (2021), la emergencia de este

"giro crítico" en los estudios de inteligencia conlleva implicaciones a diferentes niveles: en el plano normativo, la creación de conocimiento con el fin último de la transformación, mediante una aproximación más analítica que descriptiva; en el plano epistemológico, la crítica al positivismo, poniendo en entredicho la forma en la que los servicios de inteligencia y los propios estudios de inteligencia producen conocimiento; en el plano ontológico, la concepción dinámica y plural de lo que la inteligencia es, lo que exige mayores cotas de transdisciplinariedad en la investigación; por último, en el plano metodológico, la introducción del concepto de reflexividad y el énfasis en los mecanismos de generación de discursos.

Discusión

La periodización propuesta en páginas anteriores permite identificar las principales etapas en la conformación de los estudios de inteligencia, así como los factores que han condicionado su desarrollo histórico. No obstante, más allá de esta reconstrucción secuencial, resulta conveniente examinar de manera crítica el alcance explicativo de dicho esquema y las implicaciones que se derivan de él para la comprensión actual del campo. En particular, la fase más reciente plantea interrogantes relevantes sobre la naturaleza de la expansión observada, el grado real de institucionalización alcanzado y las posibles divergencias en las trayectorias de desarrollo fuera del núcleo angloamericano. A partir de estas consideraciones, el presente apartado se orienta a discutir las tensiones que caracterizan el estado actual de los estudios de inteligencia a través de las experiencias de otros ámbitos de conocimiento:

Los estudios de inteligencia, ¿campo de estudio o disciplina?: en las últimas décadas, el estatuto epistemológico de los estudios de inteligencia se ha articulado como una controversia recurrente en la literatura especializada. Esta misma controversia se ha reproducido de manera similar en otros campos de estudios: en los estudios de seguridad, por ejemplo, la consolidación del campo no vino dada por una delimitación rígida de sus fronteras, sino por la capacidad de articular una conversación académica reconocible en torno a problemas comunes, pese a la creciente pluralidad de objetos, enfoques y tradiciones intelectuales que la integraban (Buzan y Hansen, 2009). De forma semejante, en los estudios sobre terrorismo se ha discutido abiertamente si nos encontramos ante una disciplina en sentido estricto o, más bien, ante un espacio interdisciplinar cuya fortaleza reside precisamente en su apertura a perspectivas múltiples (Gordon, 2010;

Youngman, 2020). Por su parte, en los estudios migratorios, su evolución reciente ha sido interpretada en términos de una tensión constante entre institucionalización y fragmentación, característica de aquellos campos que crecen con rapidez sin haber estabilizado por completo sus límites conceptuales, metodológicos e institucionales (Levy et al., 2020). En esta misma línea, trabajos recientes sobre los estudios de paz y conflicto han subrayado que la autopercepción de un campo interdisciplinar no elimina por sí sola sus jerarquías epistémicas, sus puntos ciegos ni las tensiones entre pluralismo declarado y prácticas reales de producción de conocimiento (Storch y Liening, 2025). Todo ello sugiere que los estudios de inteligencia podrían no necesitar una autonomía disciplinar plena para alcanzar mayores cotas de madurez científica, siempre que logren reforzar su acumulación conceptual, su densidad metodológica y su capacidad para integrar de manera coherente aportaciones procedentes de distintas tradiciones académicas. En este sentido, más que aspirar a constituirse en una disciplina cerrada, quizás el principal desafío del campo consista en consolidarse como un espacio de investigación interdisciplinar dotado de suficiente coherencia interna, con capacidad de preservar su especificidad analítica sin quedar subordinado a las agendas de otros ámbitos ya plenamente institucionalizados (Repko, 2008).

La relación de los estudios de inteligencia respecto al ejercicio profesional: como se ha podido constatar, el campo de estudio también ha debatido su identidad respecto al ámbito profesional en el que se desarrolla la inteligencia. Si bien esta relación ha estado histórica y específicamente mediada por la existencia del secreto, contribuciones recientes respecto a la materialización de esta brecha en el ámbito de la inteligencia muestra que, lejos de ser una relación simplemente unidireccional, se trata de una realidad más compleja y multifacética (Arcos et al, 2022). Otros ámbitos no han estado exentos de esta distancia: en los estudios de gestión, por ejemplo, se ha advertido que los intentos de cerrar por completo la distancia entre academia y práctica suelen ignorar diferencias estructurales de lenguaje, incentivos, horizontes temporales y criterios de validación del conocimiento, por lo que la colaboración resulta deseable, siempre y cuando ello no suponga diluir la especificidad intelectual de la investigación (Kieser y Leiner, 2012). En ese sentido, autores como Grafström et al (2025) han propuesto no concebir esta brecha como una patología, sino aceptarla como una condición en torno a la que articular una cooperación realista y productiva. También desde la ciencia política se ha señalado que la llamada brecha entre académicos y profesionales responde en buena medida a una diferenciación institucional entre

comunidades con funciones distintas, de modo que su existencia no implica necesariamente fracaso, sino el reto de diseñar mecanismos de interlocución sin cancelar su autonomía respectiva (Wilson, 2007).

La internacionalización del campo de estudio: una cuestión especialmente relevante para el futuro de los estudios de inteligencia es si su actual expansión geográfica bastará para corregir el persistente predominio angloamericano o si, por el contrario, existe el riesgo de reproducir ese canon bajo nuevas formas. La experiencia de otros campos de estudio sugiere que la internacionalización efectiva no se alcanza simplemente incorporando nuevos casos empíricos en las plataformas ya existentes (siendo ello un avance incuestionable), sino poniendo en cuestión las prácticas de producción de conocimiento que han estructurado el campo de estudio y promoviendo mecanismos institucionales a nivel local. Un ejemplo elocuente de este cuestionamiento lo encontramos en las relaciones internacionales, donde la propuesta de una *Global IR* por Acharya (2014) ha insistido en que trascender la división entre Occidente y el resto exige reconocer trayectorias históricas y aportaciones intelectuales no occidentales. Este mismo cuestionamiento del canon universal basado en la experiencia angloamericana se ha replicado en otros campos de estudio, como los estudios estratégicos (Black, 2020) o la historia militar (Roy, 2022). En este mismo sentido, en los estudios de área, autores como Ahram et al (2018) han defendido la necesidad de combinar conocimiento contextual profundo con comparación transregional, evitando así tanto el universalismo abstracto como el particularismo aislado.

Conclusiones

El recorrido histórico examinado permite afirmar que los estudios de inteligencia han dejado de ser un espacio periférico, fragmentario y marcadamente dependiente de la experiencia profesional de antiguos integrantes de los servicios para convertirse, con avances desiguales, en un campo académico reconocible. Esta evolución, lejos de ser espontánea o lineal, es el resultado de un proceso largo de acumulación bibliográfica, apertura institucional, diversificación temática y búsqueda de legitimidad científica.

Una de las principales conclusiones que se pueden extraer de la trayectoria aquí descrita es que el desarrollo del campo de estudio ha dependido en gran medida de factores externos al propio ámbito académico. La disponibilidad de fuentes, los procesos de

desclasificación, la aparición de escándalos públicos, la evolución de los servicios de inteligencia y la relación entre estos y el poder político han condicionado decisivamente la posibilidad misma de investigar. En otras palabras, los estudios de inteligencia no se han expandido únicamente por una maduración interna de sus debates, sino también porque determinados contextos históricos abrieron ventanas de oportunidad para examinar objetos que habían permanecido ocultos o poco accesibles. Esta relación de dependencia explica por qué los momentos de mayor dinamización del campo coinciden con episodios de escrutinio público, con reformas institucionales o con coyunturas estratégicas que impulsaron una reflexión renovada sobre el papel de la inteligencia en el Estado contemporáneo. Así, la evolución de este ámbito de estudio revela hasta qué punto la producción de conocimiento sobre inteligencia está profundamente mediada por condiciones institucionales que no afectan con la misma intensidad a otros campos de las ciencias sociales, como la economía y la ciencia política.

Otra conclusión central es que la consolidación de los estudios de inteligencia no debe confundirse con la resolución de sus debilidades estructurales. Sin duda, el campo ha alcanzado hitos significativos y hay sobradas condiciones para el optimismo, pero lo cierto es que dicha consolidación no ha eliminado por completo algunos problemas persistentes. Entre ellos destacan la escasa sistematización acumulativa de parte de la literatura, la fragmentación entre enfoques historiográficos, metodológicos, organizacionales y normativos, así como la brecha todavía visible entre quienes investigan la inteligencia desde la academia y quienes la practican desde las instituciones. En ese sentido, la brecha de conocimiento existente entre nuestros países sobre los asuntos que conciernen a los Estudios de Inteligencia representa no solo una oportunidad para las naciones que han ocupado tradicionalmente una posición subalterna en este ámbito, en las que la producción científica sobre sus propias realidades admite hoy un inmenso desarrollo, sino también es un momento propicio para contribuir decididamente a la resolución de algunas de las limitaciones que han caracterizado al campo de estudio.

En clave latinoamericana, el desarrollo de los estudios de inteligencia representa no solo una oportunidad para ampliar el mapa global del conocimiento en este campo, sino también una necesidad estratégica para comprender trayectorias históricas y diseños institucionales que no pueden ser explicados adecuadamente desde marcos construidos casi exclusivamente a partir de la experiencia angloamericana. La

región ofrece realidades particularmente relevantes para este propósito: procesos de democratización incompletos, legados autoritarios, debilidad institucional, violencia criminal compleja, fronteras porosas y relaciones históricas con los Estados Unidos. Todo ello convierte a América Latina en un espacio especialmente fértil para generar conocimiento original, comparado y conceptualmente valioso. En este sentido, la consolidación de una agenda latinoamericana de estudios de inteligencia exige fortalecer comunidades académicas propias, promover revistas, redes y programas de formación especializados, mejorar el acceso a fuentes y archivos, e impulsar diálogos más equilibrados entre academia y sector profesional. Solo así la región dejará de ocupar una posición periférica en el campo para convertirse en un ámbito capaz de aportar categorías, problemas y enfoques con valor universal.

Bibliografía

Acharya, A. (2014). Global International Relations (IR) and Regional Worlds: A New Agenda for International Studies. *International Studies Quarterly*, *58*(4), 647–659

Aldrich, R. J. y Kasuku, J. (2012). Escaping from American Intelligence: culture, ethnocentrism and the Anglosphere. International Affairs, 88(5), 1009-1028.

Andrew, C. (1985). Secret Service: The Making of the British Intelligence Community. MacMillan Publishers.

Andrew, C. y Dilks, D. (eds.) (1984). The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century. MacMillan Publishers.

Ahram, A. I.; Köllner, P. y Sil, R. (eds.) (2018). Comparative Area Studies: Methodological Rationalities and Cross-Regional Applications. Oxford Academic.

Arcos, R., Drumhiller, N. K., y Phythian, M. (eds.). (2022). *The academic-practitioner divide in intelligence studies*. Rowman & Littlefield.

Arcos, Rubén. (2013). Academics as Strategic Stakeholders of Intelligence Organizations: A View from Spain. International Journal of Intelligence and CounterIntelligence, 26(2), 332–346.

Basic, G., y Yakhlef, S. (2022). Anomie and collaboration in intelligence and operational police and border guard work in the Baltic Sea area: in-group mentality and construction of the other. *Policing and Society*, *32*(9), 1103–1123.

Bean, H; de Werd, P; e Ivan, C. (2021). Critical intelligence studies: introduction to the special issue. Intelligence and National Security, 36(4), 467-475.

Ben Aharon, E. (2023). Methodological and epistemological reflections on elite interviews and the study of Israel's intelligence history: interview with Efraim Halevy. *Intelligence and National Security*, *38*(1), 111–127.

Ben Jaffel, H., y Larsson, S. (2024). Why Do We Need a New Research Agenda for the Study of Intelligence? International Journal of Intelligence and CounterIntelligence, 37(2), 727–750.

Brown, F. R.; Dowden, A. M. (1986). From the Editor… International Journal of Intelligence and CounterIntelligence, 1(1), 1–2.

Buzan, B., y Hansen, L. (2009). *The evolution of international security studies*. Cambridge University Press.

Chaya, D. P. (2023). *India's intelligence culture and strategic surprises: Spying for South Block*. Routledge.
Cremades Guisado, A., y Bueno, A. (2022). El desarrollo de la política de cultura de inteligencia en España: un caso de isomorfismo institucional. *URVIO. Revista Latinoamericana De Estudios De Seguridad*, (34), 36–51.
Cremades-Guisado, A.y Cancelado-Franco, H. (2021). La inteligencia como organización burocrática: disfunciones del modelo weberiano. Revista Científica General José María Córdova, 19(34), 479-496
Dahl, E. J. y Viola, D. (2017). "Intelligence and Terrorism" en Nalanda Roy (ed.), *Oxford Research Encyclopedia of International Studies*. Oxford Academic.
Dahl, E. J. (2005). Warning of Terror: Explaining the Failure of Intelligence Against Terrorism. *Journal of Strategic Studies*, *28*(1), 31–55.
Davis, J. (1992). The Kent-Kendall Debate of 1949. Studies in Intelligence, 36(5), 91-103.
Díaz-Fernández, A. M., y Del-Real, C. (2026). Measuring Trust in Intelligence Services: A Conceptual Framework and Exploratory Study. *Democracy and Security*, *22*(1), 80–108.
Dujmovic, N. (2005). Fifty Years of Studies in Intelligence. Studies in Intelligence 49(4)
Dylan, H., y Gioe, D. (2020). 1975: The Year of the 'Intelligence Wars.' In M. S. Goodman (ed.), *The CIA and the Pursuit of Security: BG, Documents and Contexts* (pp. 190–196). Edinburgh University Press.
Gill, P. y Phythian, M. (2016). What is Intelligence Studies? The International Journal of Intelligence, Security, and Public Affairs, 18(1), 5-19.
Glass, R. R., y Davidson, P. B. (1948). Intelligence is for Commanders. Military Service Publishing Company.
Glees, A. (2015). Intelligence Studies, Universities and Security. *British Journal of Educational Studies*, 63(3), 281–310.
Godson, R. (ed.) (1979). Intelligence Requirements in the 80's: Elements of Intelligence. Transaction Books.
Goldewijk, B. (2021). Why still critical? Critical intelligence studies positioned in scholarship on security, war, and international relations. Intelligence and National Security, 36(4), 476-494.
Goodman, M. A. (2003). 9/11: The Failure of Strategic Intelligence. *Intelligence and National Security*, *18*(4), 59–71.
Gordon, Avishag. (2010). Can terrorism become a scientific discipline? A diagnostic study. Critical Studies on Terrorism, 3(3), 437–458.
Grafström, M., Jonsson, A., y Klintman, M. (2025). Embracing the academic–practice gap: Knowledge collaboration and the role of institutional knotting. *Management Learning, 56*(2), 160–183.
Gwatiwa, T. (ed.). (2025). *Contemporary intelligence in Africa*. Routledge.
Handel, M. I. (1989). Strategic and Operational Deception in the Second World War. Frank Cass
Hilsman, R. (1956). Strategic Intelligence and National Decisions. The Free Press.
Hinsley, F. H. (1979). British Intelligence in the Second World War. HMSO.
Horkheimer, M. (2002). Critical Theory: Selected Essays. Continuum.
Intelligence & National Security (1986). Editorial. Intelligence and National Security, 1(1), 3-3.
Johnson, L. J. (1985). A Season of Inquiry: The Senate Intelligence Investigation. University Press of Kentucky.

Johnson, L. J. (2014). The development of Intelligence Studies, en Dover, R.; Goodman, M. S; Hillebrand, C (eds.). Routledge Companion to Intelligence Studies. Routledge.
Johnson, L. K., y Shelton, A. M. (2013). Thoughts on the State of Intelligence Studies: A Survey Report. Intelligence and National Security, 28(1), 109-120.
Kendall, W. (1949). The function of intelligence. World Politics, 1(4), 542-552.
Kent, S. (1949). Strategic Intelligence for American World Policy. Archon Books.
Kent, S. (1955). The Need for an Intelligence Literature. Studies in Intelligence, 1(1), 1-8.
Kieser, A., y Leiner, L. (2012). Collaborate with practitioners: But beware of collaborative research. *Journal of Management Inquiry, 21*(1), 14–28.
Lahneman, W. J. (2004). Knowledge-Sharing in the Intelligence Community After 9/11. *International Journal of Intelligence and CounterIntelligence*, *17*(4), 614–633.
Laqueur, W. (1985). A World of Secrets: The Uses and Limits of Intelligence. Basic Books.
Lebakeng, J., y Gwatiwa, T. (2025). Editorial to special edition: frontiers in African intelligence studies. *Journal of Policing, Intelligence and Counter Terrorism*, *20*(2), 161–172.
Levy, N., Pisarevskaya, A., y Scholten, P. (2020). Between fragmentation and institutionalisation: The rise of migration studies as a research field. *Comparative Migration Studies, 8*, Article 24, 1–24.
Marrin, S. (2011). The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis. *Intelligence and National Security*, *26*(2–3), 182–202.
Marrin, S. (2016). Improving Intelligence Studies as an Academic Discipline. Intelligence and National Security, 31(2), 266–279.
Matei, F. C.; Halladay, C., y Estévez, E. E. (eds.). (2024). *The handbook of Latin American and Caribbean intelligence cultures*. Rowman & Littlefield.
McLoughlin, L., Ward, S., y Lomas, D. W. B. (2020). 'Hello, world': GCHQ, Twitter and social media engagement. Intelligence and National Security, 35(2), 233–251.
Moran, C. R. (2011). The Pursuit of Intelligence History: Methods, Sources, and Trajectories in the United Kingdom. Studies in Intelligence, 55(2), 33-55.
Navarro, D. (2009). ¡Espías! Tres mil años de información y secreto. Plaza y Valdés.
Nolan, B. (2018). "Ethnographic Research in the U.S. Intelligence Community: Opportunities and Challenges." *Secrecy and Society,* 2(1), 1-31.
Oomens, E. C., van Wegberg, R. S., Klievink, A. J., y van Eeten, M. J. G. (2024). To trust or to restrict? – mapping professional perspectives on intelligence powers and oversight in the Netherlands using Q-methodology. *Intelligence and National Security*, *39*(1), 40–63.
Permanent Select Committee On Intelligence (1996). IC21: Intelligence Community in the 21st Century. U.S. Government Printing Office, Washington D.C.
Pettee, G. (1946). The Future of American Secret Intelligence. Infantry Journal Press.
Phythian, M. (2018). Profiles in intelligence: an interview with Professor Richard J. Aldrich. *Intelligence and National Security*, *33*(7), 939–953.
Phythian, M. (2022). Profiles in Intelligence: an interview with Professor Loch K. Johnson. *Intelligence and National Security*, *37*(7), 939–967.
Platt, W. (1957). Strategic Intelligence Production: Basic Principles. Frederick A. Praeger Publishers.
Repko, A. F. (2008). *Interdisciplinary research: Process and theory*. SAGE.
Betts, R. K. (2002). Fixing Intelligence. Foreign Affairs, 81(1), 43–59.
Richelson, J. T. (1985). The U.S. Intelligence Community. Cambridge University Press.

Second Hoover Commission (1955). Task Force on Intelligence Activities of the Commission on Organization of the Executive Branch of the Government, 663-664.
Shaffer, R. (ed.). (2023). *The handbook of African intelligence cultures*. Rowman & Littlefield.
Shaffer, R. (ed.). (2024). *The handbook of Asian intelligence cultures*. Rowman & Littlefield.
Shaffer, R., & Ashraf, A. A. (eds.). (2025). *Intelligence services in South Asia: Colonial past and post-colonial realities*. Routledge.
Shiraz, Z. y Aldrich, R. J. (2019). Secrecy, spies, and the global South: intelligence studies beyond the "Five Eyes" alliance. International Affairs, 95(6), 1313-1329.
Sims, J. E. y Gerber, S. (2005). Transforming U.S. Intelligence. Georgetown University Press.
Stafford T. T. (1988): *Assessing current intelligence studies*, International Journal of Intelligence and CounterIntelligence, 2 (2), 217-244
Storch, K., y Liening, M. (2025). Critical reflections on peace and conflict studies: Empirical insights into the self-perception of an interdisciplinary field. *Zeitschrift für Friedens- und Konfliktforschung, 14*(1), 5–26.
Sudkamp, K. M., Williams, H. J., Jaycox, L. H., Dunigan, M., y Young, S. (2022, October). Trauma in the U.S. intelligence community: Risks and responses (PE-A1027-1). RAND Corporation
Svendsen, A. D. M. (2008). The Globalization of Intelligence Since 9/11: The Optimization of Intelligence Liaison Arrangements. *International Journal of Intelligence and CounterIntelligence*, *21*(4), 661–678.
Thomas, J. y Dujmovic, N. (2019). Educators Consider Alternative Approaches to US College Intelligence Programs. Studies in Intelligence, 63(4), 1-5.
Troy, T. F. (1988). The quaintness of the U.S. intelligence community: Its origin, theory and problems. International Journal of Intelligence and Counterintelligence, 2(2), 245-266.
United States Government Accountability Office (2019). Intelligence Community: Actions Needed to Improve Planning and Oversight of the Centers for Academic Excellence Program.
Van Puyvelde, D. (2020). Profiles in intelligence: an interview with Sir David Omand. *Intelligence and National Security*, *35*(2), 171–178.
Van Puyvelde, D., y Curtis, S. (2016). Standing on the shoulders of giants: diversity and scholarship in intelligence studies. Intelligence and National Security, 31(7), 1040-1054.
Van Puyvelde, D.; Wirtz, J. J.; Holeindre, J-V; Oudet, B.; Bar-Joseph, U.; Kotani, K.; Cristiana, F.; y Díaz, A. M. (2020). Comparing National Approaches to the Study of Intelligence. International Studies Perspectives, 21(3), 298-337.
Watt, D. Cameron. (1988). *Intelligence studies: The emergence of the British school. Intelligence and National Security, 3(2), 338–341.*
Willmetts, S. (2019). The cultural turn in intelligence studies. Intelligence and National Security, 34(6), 800–817.
Wilson, E. J., III. (2007). Is there really a scholar-practitioner gap? An institutional analysis. *PS*: *Political Science y Politics, 40*(2), 247–251.
Winterbotham, F. W. (1974). The Ultra Secret. Purnell.
Youngman, M. (2020). Building "Terrorism Studies" as an interdisciplinary space: Addressing recurring issues in the study of terrorism. *Terrorism and Political Violence, 32*(5), 1091–1105.
Zegart, A. B. (2005). September 11 and the Adaptation Failure of U.S. Intelligence Agencies. *International Security*, 29 (4): 78–111.
Black, J. (2020). Military Strategy: A Global History. Yale University Press.

Roy, K. (2022). A Global History of Pre-Modern Warfare: Before the Rise of the West, 10,000 BCE–1500 CE. Routledge.
Phythian, M. (2017). Profiles in intelligence: an interview with Professor Christopher Andrew. *Intelligence and National Security*, *32*(4), 395–410

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

¿México en Riesgo? El Espacio Aéreo Nacional como frente de batalla y prioridad estratégica en la Agenda de Inteligencia y Seguridad Nacional. Nuevas formas de Conflicto Híbrido en México

Eduardo Zerón García*

Resumen: El crimen organizado en México ha incorporado con notable rapidez tecnologías de vigilancia, reconocimiento aéreo y geolocalización que en el pasado eran exclusivas de los aparatos de seguridad del Estado. El uso de drones artillados, sistemas de inteligencia geoespacial y plataformas de mapeo ha reconfigurado la naturaleza del conflicto entre organizaciones criminales y las autoridades. Las organizaciones delincuenciales han evolucionado hasta convertirse en actores híbridos no estatales, con capacidades paramilitares propias de los grupos terroristas; la violencia se ha convertido en un instrumento de gobernanza criminal, control territorial e influencia social.

El creciente uso de sistemas de aeronaves pilotadas a distancia (RPAS) y de artefactos explosivos improvisados (IED) por parte de los grupos criminales incrementa la vulnerabilidad del Estado debido a la falta de capacidades técnicas. Esto eleva el riesgo de una sorpresa estratégica debido a la ausencia de instrumentos de alerta temprana y de conciencia situacional. Esto compromete la gobernanza y la seguridad interior y nacional. Este artículo examina los marcos conceptuales del conflicto híbrido y del uso de estas tecnologías desde la perspectiva de la recuperación de la soberanía geoespacial.

Palabras clave: inteligencia geoespacial, conflicto híbrido, soberanía geoespacial, alertamiento temprano, conciencia situacional, vulnerabilidad estratégica.

* Especialista mexicano en seguridad nacional e inteligencia. Es licenciado en Ciencias de la Comunicación por la Universidad de las Américas Puebla y maestro en Inteligencia y Seguridad Nacional por el Instituto Nacional de Administración Pública. Cuenta con formación en manejo de crisis, terrorismo y delincuencia organizada transnacional. Actualmente es doctorante en Seguridad Internacional en la Universidad Anáhuac del Norte y es consultor en seguridad nacional y columnista en *La Silla Rota*.

Abstract: Organized crime in Mexico has rapidly adopted surveillance, aerial reconnaissance, and geolocation technologies once reserved for state security apparatuses. The use of armed drones, geospatial intelligence systems, and mapping platforms has reshaped the conflict between criminal organizations and authorities. Criminal organizations have evolved into non-state hybrid actors with paramilitary capabilities characteristic of terrorist groups; violence has become an instrument of criminal governance, territorial control, and social influence.

The growing use of Remotely Piloted Aircraft Systems (RPAS) and Improvised Explosive Devices (IEDs) by criminal groups increases state vulnerability, given limited technical capabilities. It raises the risk of a strategic surprise due to the absence of early warning instruments and situational awareness, thereby compromising governance and internal and national security. This article examines the conceptual frameworks of hybrid conflict and the use of these technologies from the perspective of recovering geospatial sovereignty.

Keywords: geospatial intelligence, hybrid conflict, geospatial sovereignty, early warning, situational awareness, strategic vulnerability.

I. INTRODUCCIÓN

En los últimos años, el avance de la tecnología ha cambiado profundamente la forma en que se desarrollan los conflictos, especialmente en situaciones en las que los grupos no estatales han logrado emplear capacidades antes exclusivas de los ejércitos regulares. En México, esta tendencia se manifiesta con claridad en la adopción sistemática de tecnologías como sistemas de aeronaves no tripuladas (UAS), artefactos explosivos improvisados (IED) y plataformas de reconocimiento aéreo, así como de sistemas antidrones. Esta transformación advierte de nuevas dinámicas operativas del crimen organizado que plantean desafíos estructurales para la seguridad nacional.

Diversos análisis han advertido que las organizaciones criminales transnacionales representan una amenaza creciente a la seguridad y operan en un entorno cada vez más influido por tecnologías emergentes (Office of the Director of National Intelligence [ODNI], 2025). El caso mexicano evidencia la magnitud de esta transformación: entre 2020 y mediados de 2023 se registraron al menos 605 ataques con drones explosivos, con un incremento de 5 incidentes en 2020 a aproximadamente 260 en el primer semestre de 2023 (Villegas & Zehbrauskas, 2025). Para el año 2025, el uso ofensivo de sistemas

remotamente pilotados (RPAS) dejó de ser una práctica incipiente y se consolidó como parte de la operación cotidiana de las organizaciones criminales.

Este fenómeno forma parte de un cambio más amplio en la naturaleza del conflicto, en el que el acceso a tecnologías más asequibles permite a actores no estatales desarrollar capacidades asimétricas con efectos estratégicos (Horowitz, 2018). En este contexto, el uso de drones ha pasado de funciones logísticas —como el transporte de narcóticos— a aplicaciones cinéticas e inteligencia, vigilancia y reconocimiento (ISR). A ser empleados de manera táctica y cinética mediante explosivos contra sus adversarios (Bunker & Sullivan, 2021; Ziemer, 2025). Como señaló Willoughby (2025), las TCOs emplean estas plataformas tanto para actividades ilícitas transfronterizas como para la vigilancia hostil contra las fuerzas de seguridad. "En los últimos seis meses de 2024, se detectaron más de 27,000 drones a menos de 500 metros de la frontera sur. Las detecciones de drones (…) condujeron a la detención de más de 1,500 personas a lo largo de la frontera suroeste, lo que constituye un indicador claro de que las organizaciones criminales transnacionales están incorporando el uso de drones en sus tácticas como medio para vigilar y evadir a los agentes y oficiales, así como a otras autoridades de seguridad". (Willoughby, 2025)

La expansión de estas capacidades se evidencia en datos del Centro de Estudios Estratégicos e Internacionales (Center for Strategic and International Studies, 2025), que documentó 77 incidentes con drones en la región durante 2025 y 32 en el primer semestre de 2025, de los cuales 15 involucraron directamente a grupos armados. Esta tendencia también ha sido documentada por la prensa internacional: según Nicas y Villegas (2026), en octubre de 2025 tres drones lanzaron explosivos contra una oficina de la Fiscalía en Tijuana, y en paralelo se registraron ataques con drones contra fuerzas de seguridad mexicanas en Río Bravo y en otras zonas fronterizas, lo que confirma el carácter sistemático y no aislado de estos incidentes.

En estados como Michoacán —particularmente en los municipios de Apatzingán, Cotija y Tepalcatepec— el Cártel de Jalisco Nueva Generación (CJNG) normalizó el uso de drones tipo kamikaze para ataques en zonas pobladas, operaciones de vigilancia y la coordinación de ofensivas terrestres (Rodríguez, 2025; Bunker & Sullivan, 2021; Kramer et al., 2023). La conclusión del CSIS es que América Latina enfrenta una amenaza persistente, con escasas capacidades institucionales para afrontarla (Ziemer, 2025).

La expansión de esas capacidades no puede entenderse como una mera adaptación tecnológica, sino como parte de dinámicas complejas asociadas al conflicto híbrido. Según Frank Hoffman (2007), el conflicto híbrido se caracteriza por la combinación de medios convencionales, irregulares y criminales en un mismo teatro de operaciones. En el caso mexicano, las organizaciones criminales han comenzado a integrar estas dimensiones, utilizando tecnologías emergentes para ampliar su control territorial, mejorar su capacidad de vigilancia y reducir su vulnerabilidad frente a las fuerzas del Estado.

En ese sentido, el problema central no radica únicamente en la evolución de las capacidades criminales, sino también en las limitaciones estructurales del Estado para responder a estas transformaciones. México enfrenta una brecha en las capacidades de alerta temprana (early warning) y de conciencia situacional (situational awareness). La falta de una arquitectura integrada de inteligencia, vigilancia y reconocimiento (ISR) impide al Estado identificar, prever y responder a amenazas en tiempo real, lo que conduce a una pérdida gradual de control sobre su espacio aéreo.

Asimismo, diversos reportes han señalado la posible convergencia en el acceso a tecnologías antidrones entre las fuerzas armadas y las organizaciones criminales en México, lo que sugiere una erosión progresiva de la ventaja tecnológica nacional y, en consecuencia, una reducción de la asimetría en este aspecto, con implicaciones directas para la capacidad del Estado de ejercer el monopolio legítimo de la fuerza en dicho dominio (Más Información, 2026).

Estas condiciones se ven exacerbadas y potencialmente agravadas por tensiones de carácter geopolítico que complejizan aún más el entorno. Diversos reportes han documentado la presencia de plataformas no tripuladas vinculadas al gobierno americano realizando actividades de inteligencia de señales (SIGINT) así como de inteligencia, reconocimiento y vigilancia (ISR) persistente en territorio nacional, en paralelo con acciones de interdicción en espacio aéreo estadounidense contra drones asociados a organizaciones criminales (The War Zone, 2025; Forbes México, 2026; Willoughby, 2025), lo que supone un entorno aéreo más disputado, donde convergen actores estatales y no estatales con agendas, ambigüedades y competencia estratégica.

Estas limitaciones adquieren mayor relevancia, efectivamente, en los entornos de competencia estratégica que se sitúan por debajo del conflicto armado convencional. En este sentido, el caso mexicano

puede entenderse a partir del concepto de zona gris, definido como un espacio de interacción en el que actores estatales y no estatales persiguen objetivos estratégicos mediante acciones graduales que evitan la escalada directa, pero generan efectos acumulativos sobre la soberanía y la autoridad de los estados (Mazarr, 2015). En América Latina, estas dinámicas han sido particularmente visibles en contextos en los que el crimen organizado ejerce funciones de gobernanza en territorios donde el Estado presenta capacidades limitadas (Felbab-Brown, 2017a).

En este contexto, las organizaciones criminales no solo operan como actores ilícitos, sino también como competidores estratégicos que aprovechan vacíos institucionales y tecnológicos para consolidar su presencia en el dominio aéreo. La combinación de nuevas tecnologías, habilidades delictivas y debilidades del Estado crea un ambiente de conflicto híbrido en una zona gris. En este contexto, la línea entre la seguridad, la seguridad interior y la defensa nacional se vuelve cada vez más difusa.

El presente artículo sostiene que la ausencia de capacidades institucionales robustas en inteligencia geoespacial (GEOINT) y en sistemas de alertamiento temprano constituye una pérdida progresiva del control del dominio aéreo de primer orden (Gray, 2009, 2014). Esto se convierte en una falla sistémica que limita al Estado en el ejercicio del control territorial, reduce la capacidad de disuasión y compromete la seguridad nacional en su conjunto. En un entorno en el que no es posible integrar capacidades de inteligencia en el ámbito aéreo, el Estado se encuentra en una situación de desventaja frente a actores no estatales altamente adaptables.

El artículo se organiza en cinco secciones. Primero, se revisa el concepto de inteligencia geoespacial y los factores que inciden en la transformación del conflicto. En la segunda, se documenta el arsenal del crimen organizado y su evolución hacia formas de conflicto híbrido. En la tercera, se examina el marco conceptual del conflicto en el caso mexicano. En la cuarta parte, se evalúan las capacidades y limitaciones del Estado en materia de inteligencia geoespacial. Finalmente, se proponen acciones para recuperar la soberanía geoespacial del país mediante un modelo de inteligencia estratégica a largo plazo.

II. INTELIGENCIA GEOESPACIAL Y LA DEMOCRATIZACIÓN DEL CONFLICTO

La inteligencia geoespacial (GEOINT) puede definirse como el conocimiento obtenido al analizar imágenes y datos geoespaciales para describir, evaluar y supervisar objetos, fenómenos y actividades en entornos físicos y geográficos (National Geospatial-Intelligence Agency [NGA], 2006). En su formulación doctrinal, la GEOINT integra tres componentes fundamentales: imágenes obtenidas mediante plataformas satelitales y aéreas; datos geoespaciales, incluidos la cartografía, los modelos de elevación e información sobre infraestructura; y sistemas de posicionamiento global. Su relevancia estratégica radica en que constituye la base empírica sobre la cual se construyen estimaciones de inteligencia, se planifican operaciones y se toman decisiones en contextos de incertidumbre (Lowenthal, 2022; Sims, 2022).

Durante gran parte del siglo XX, el acceso a capacidades de GEOINT estuvo concentrado en un número limitado de Estados, debido a los altos costos asociados al desarrollo y la operación de satélites de reconocimiento, aeronaves especializadas y plataformas de análisis de imágenes. Sin embargo, esta concentración empezó a debilitarse en los primeros años del siglo XXI debido a varios factores tecnológicos que han reducido las barreras para acceder a y utilizar la información geoespacial.

El primero de estos factores es la miniaturización y el abaratamiento de los vehículos aéreos no tripulados. Lo que a inicios del siglo XXI requería una infraestructura militar compleja y recursos financieros significativos, hoy puede adquirirse en mercados comerciales a costos relativamente bajos, con capacidades de estabilización de imagen, posicionamiento global y transmisión de video en tiempo real comparables a las de sistemas militares de gama media (Boyle, 2020; Holland Michel, 2019). Este proceso ha reducido sustancialmente las barreras de acceso a las capacidades de reconocimiento aéreo para los actores no estatales.

El segundo factor es la disponibilidad masiva de imágenes satelitales de alta resolución a través de plataformas comerciales y de fuentes abiertas. Servicios como Google Earth, Sentinel Hub y Planet Labs ofrecen imágenes con resolución submétrica y frecuencias de revisita que permiten monitorear cambios territoriales casi en tiempo real. La inclusión de estas fuentes mediante herramientas de OSINT ha ampliado significativamente el acceso a capacidades analíticas que antes solo tenían las agencias estatales (Rogers, 2024; Kunertova, 2024; Gruszczak & Kaempf, 2023).

El tercer factor es la proliferación de dispositivos móviles inteligentes y de redes de comunicación de alta velocidad, que han convertido a la población civil en una red distribuida de sensores geoespaciales. Los datos de localización, los metadatos de imágenes y la información geoetiquetada en redes sociales generan flujos constantes de información sobre movimientos, actividades y configuraciones territoriales (NGA, 2006; Lowenthal, 2022). La inclusión de estos datos en el análisis de ciclos de inteligencia más rápidos ha cambiado la escala, la velocidad y la accesibilidad de las capacidades de vigilancia y reconocimiento (ISR).

En general, estos procesos han creado lo que se denomina la "democratización del conflicto": una situación en la que tecnologías que antes solo tenían los Estados se comparten con actores no estatales, lo que cambia la distribución del poder y las confrontaciones actuales (Gruszczak & Kaempf, 2023). Esta transformación parece no solo ampliar las capacidades operativas de dichos actores, sino también reducir la ventaja relativa de los Estados en dominios estratégicos clave.

En el caso mexicano, esta dinámica adquiere una relevancia particular. La combinación del acceso a tecnologías geoespaciales, la disponibilidad de drones y las capacidades financieras de los grupos criminales ha creado un escenario en el que los actores no estatales pueden llevar a cabo tareas básicas de inteligencia, vigilancia y reconocimiento (ISR) con un grado de sofisticación cada vez mayor. En ausencia de una arquitectura estatal integrada de alertamiento temprano y de conciencia del dominio aéreo (Air Domain Awareness), esta democratización tecnológica no solo incrementa la capacidad operativa del crimen organizado. También contribuye directamente a la erosión del control estatal sobre el espacio aéreo, lo que configura un entorno propicio para dinámicas de conflicto híbrido en la zona gris.

III. EL ARSENAL GEOESPACIAL DEL CRIMEN ORGANIZADO MEXICANO: EVOLUCIÓN, CAPACIDADES Y DOCTRINA

La incorporación de tecnologías de inteligencia geoespacial por parte del crimen organizado mexicano no constituye un fenómeno repentino ni improvisado. Es un proceso de adaptación tecnológica que ocurre poco a poco y se acumula con el tiempo, en línea con la evolución de los grupos criminales. Estos grupos, al mezclarse, adoptan tácticas y métodos vinculados al terrorismo.

Los cárteles han transformado cualitativamente sus operaciones a lo largo de una década. Este proceso supone tres etapas diferenciadas: una fase experimental, de reconocimiento y logística; una fase de instrumentación bélica ofensiva —es decir, la conversión sistemática de plataformas civiles en instrumentos de ataque— que transforma cualitativamente el arsenal operativo de los grupos criminales (Haugstvedt, 2023; Bunker & Sullivan, 2021) y una fase doctrinal. Esta evolución es coherente con los patrones de difusión tecnológica en entornos de conflicto identificados en la literatura, en los que las tecnologías son adoptadas e integradas inicialmente por actores no estatales (Horowitz, 2018; Gruszczak & Kaempf, 2023).

La primera etapa, ubicable aproximadamente entre 2015 y 2019, estuvo marcada por el uso de drones comerciales de consumo masivo con fines de vigilancia básica, reconocimiento territorial y documentación propagandística. Uno de los primeros registros documentados se remonta a 2015, cuando las autoridades estadounidenses detectaron un dron cargado con narcóticos que había cruzado la frontera desde México, lo que evidenció el potencial logístico de estas plataformas (Parker, 2015). En ese mismo año, el Cártel de Jalisco Nueva Generación (CJNG) demostró capacidades ofensivas avanzadas al derribar un helicóptero militar en Jalisco, lo que evidenció un nivel de confrontación que anticipaba una trayectoria de escalamiento tecnológico en el contexto del crimen organizado (BBC News, 2015). Para finales de la década, diversos reportes documentaron los primeros casos de drones utilizados para lanzar artefactos explosivos improvisados (IED) contra objetivos específicos, lo que marcó el inicio de la transición hacia usos ofensivos más sofisticados (ZETA, 2018; Bunker et al., 2020/2021).

La segunda etapa, comprendida entre 2020 y 2023, se caracterizó por una fase de instrumentación bélica ofensiva sistemática de los RPAS y la escalada en el uso de artefactos explosivos improvisados (IEDs). De acuerdo con datos oficiales de la Secretaría de la Defensa Nacional, durante este período se registraron más de 600 incidentes relacionados con drones explosivos en territorio nacional, con un crecimiento significativo en la frecuencia y la complejidad de estos ataques (Nicas & Villegas, 2026; Ziemer, 2025).

Paralelamente, organizaciones como el CJNG desarrollan estructuras especializadas para la operación de drones, que incluyen unidades dedicadas, procedimientos estandarizados y capacidades técnicas orientadas a maximizar el impacto operativo de estas plataformas. Esta

profesionalización ha sido documentada en estudios especializados que identifican la transición de los drones comerciales a sistemas adaptados para funciones ofensivas, incluyendo la integración de cargas explosivas y capacidades de ataque de precisión (Bunker & Sullivan, 2021; Bunker et al., 2020/2021).

Esta transferencia tecnológica adquiere una dimensión adicional con la documentación de operadores criminales mexicanos —incluidos presuntos miembros del CJNG y de las FARC colombianas— que viajaron a Ucrania bajo la modalidad train-the-trainer para recibir instrucción avanzada en el uso de drones FPV en condiciones de combate real, con el propósito de replicar esa doctrina operativa en México (Small Wars Journal, 2026; Höller, 2025).

La tercera etapa, que se consolida a partir de 2024, puede caracterizarse como una fase de institucionalización doctrinal. En este período, el uso de RPAS ha dejado de ser una capacidad emergente para convertirse en un componente estructural de las operaciones criminales. En regiones como Tierra Caliente, particularmente en municipios de Michoacán, se ha documentado el uso sistemático de drones para ataques tipo kamikaze, vigilancia persistente y coordinación de operaciones terrestres. Asimismo, incidentes documentados en zonas urbanas fronterizas han evidenciado la capacidad de estas organizaciones para emplear drones en ataques contra instalaciones gubernamentales, lo que representa una escalada cualitativa del riesgo (Ziemer, 2025; Nicas & Villegas, 2026; Kramer et al., 2023).

Datos recientes de centros de análisis estratégico confirman la aceleración de esta tendencia, mostrando un incremento sostenido en el número de incidentes relacionados con drones en América Latina y una participación creciente de actores armados no estatales. Este patrón sugiere la existencia de una difusión tecnológica escalonada, en la que las organizaciones criminales de mayor capacidad desarrollan innovaciones que posteriormente son replicadas por grupos de menor escala, lo que reproduce dinámicas observadas en otros contextos de conflicto contemporáneo (Kunertova, 2023; Horowitz, 2018).

Más allá de la dimensión ofensiva, la integración de capacidades de inteligencia, vigilancia y reconocimiento (ISR) en la estructura operativa del crimen organizado representa la transformación más significativa desde la perspectiva de la seguridad del Estado. Las organizaciones criminales han desarrollado sistemas de alertamiento temprano que combinan vigilancia humana, sensores fijos, plataformas

aéreas no tripuladas y datos de fuentes abiertas para construir arquitecturas funcionales de conciencia situacional territorialmente distribuida (Chaparro, 2021; Mendoza García, 2021). Estas capacidades permiten anticipar los movimientos de las fuerzas de seguridad, reducir la incertidumbre operativa y adaptar las tácticas en tiempo real, generando ventajas informacionales frente a instituciones estatales que operan con ciclos de inteligencia más tradicionales y, en consecuencia, pueden ser más lentas, en línea con los principios de alerta temprana (Grabo, 2010).

Reportes recientes sugieren que las organizaciones criminales han comenzado a incorporar drones de fibra de carbono, lo que reduce la capacidad del Estado para, primero, detectarlos y, segundo, utilizar instrumentos tradicionales de inhibición de señal (jamming) o de suplantación de señal (spoofing). Paralelamente, existe evidencia de mecanismos básicos de resistencia a interferencias electrónicas, que incluyen capacidades limitadas de anti-jamming y anti-spoofing, orientadas a mitigar la efectividad de sistemas convencionales de contramedidas, como los inhibidores de señal portátiles.

Aunque estas capacidades no reflejan un nivel avanzado de guerra electrónica, sí evidencian un proceso de adaptación tecnológica iterativa, consistente con las dinámicas de escalamiento observadas en entornos de amenaza híbrida, donde los actores no estatales responden activamente a las medidas de control implementadas por el Estado (Borch & Heier, 2025). Este proceso sugiere la emergencia de un ciclo de acción-reacción, en el que la introducción de nuevas herramientas de interdicción genera incentivos para la innovación adversaria, lo que incrementa la complejidad del entorno operativo.

En esta misma línea, algunos reportes han señalado el uso incipiente de técnicas orientadas a la degradación de las señales de posicionamiento satelital y a la evasión de los sistemas de detección, lo que sugiere un proceso de adaptación tecnológica en curso. Asimismo, análisis especializados han advertido sobre la posible inclusión de sistemas como el SkyFend C-UAS jammer, cuya disponibilidad en mercados internacionales sugiere la posibilidad de acceso por parte de actores no estatales, aunque su uso operativo documentado sigue siendo limitado (Ziemer, 2025; Rogers, 2024).
En este sentido, la adopción de tecnologías geoespaciales por parte del crimen organizado no debe entenderse únicamente como una mejora táctica, sino como un proceso de transformación estructural que altera las condiciones de competencia en el dominio aéreo. En el contexto

mexicano, esta evolución se inscribe en dinámicas más amplias de conflicto híbrido o de guerras de cuarta generación (4GW), en las que actores no estatales combinan capacidades tecnológicas, control territorial y violencia organizada para erosionar progresivamente la autoridad del Estado sin cruzar el umbral del conflicto armado convencional (Hoffman, 2007; Mazarr, 2015; Lind et al., 1989).

Es entonces cuando, bajo estas condiciones, el espacio aéreo deja de ser un dominio secundario para convertirse en un ámbito central de disputa estratégica. La ventaja ya no depende exclusivamente de la superioridad militar convencional, sino de la capacidad de integrar inteligencia geoespacial, vigilancia persistente y adaptación operativa en tiempo real. En ausencia de una arquitectura estatal robusta, esta transformación favorece a actores no estatales altamente adaptativos, lo que consolida un entorno en el que el Estado pierde progresivamente su capacidad de control sobre un dominio crítico para la seguridad nacional.

IV. CONFLICTO HÍBRIDO, ZONA GRIS Y SOBERANÍA GEOESPACIAL: UN MARCO ANALÍTICO PARA EL CASO MEXICANO

La comprensión del fenómeno descrito en los apartados anteriores requiere un marco analítico que trascienda las categorías convencionales del análisis de seguridad. En este sentido, las transformaciones observadas en el caso mexicano pueden interpretarse como parte de una evolución más amplia del conflicto contemporáneo hacia formas de lo que se denomina guerra de cuarta generación (4GW), caracterizadas por la erosión de la distinción entre actores estatales y no estatales, así como por el desplazamiento del campo de batalla hacia ámbitos no convencionales (Lind et al., 1989; Hammes, 2004). En este contexto, el concepto de conflicto híbrido desarrollado por Frank G. Hoffman (2007) permite comprender la combinación simultánea de medios convencionales, irregulares y criminales en un mismo teatro de operaciones. En el caso mexicano, esta convergencia se expresa en la integración de capacidades paramilitares, tecnologías de vigilancia geoespacial y estructuras de gobernanza criminal que desafían simultáneamente la seguridad pública, la seguridad interior y la seguridad nacional (Moghadam et al., 2024; Felbab-Brown, 2017a).

La evolución de las organizaciones criminales mexicanas hacia formas híbridas ha sido ampliamente documentada. Felbab-Brown (2017a) sostiene que estos grupos operan como competidores estratégicos que

construyen sistemas paralelos de gobernanza en territorios con presencia estatal limitada. Esta lógica coincide con lo que Mazarr (2015) denomina estrategias de zona gris: acciones graduales que evitan el conflicto abierto, pero generan efectos acumulativos sobre la soberanía. En este tipo de entornos, la ambigüedad operativa se convierte en un recurso estratégico central (Borch & Heier, 2025).

En el dominio aéreo, estas dinámicas adquieren una relevancia adicional. Los grupos criminales han incorporado capacidades de ISR, plataformas aéreas no tripuladas y mecanismos incipientes de resistencia a las interferencias electrónicas. Estas capacidades reflejan tendencias más amplias del conflicto contemporáneo, en las que las tecnologías emergentes permiten a los actores no estatales generar efectos estratégicos desproporcionados (Rogers, 2024). El uso de drones, sistemas de alerta temprana y tecnologías de negación de señales constituye una manifestación del conflicto híbrido en el espacio aéreo.

Aunque algunos autores cuestionan la aplicación del concepto híbrido a actores motivados por incentivos económicos, como los cárteles, esta distinción resulta insuficiente cuando dichos grupos desarrollan control territorial, sistemas paralelos de justicia y mecanismos de coerción social. Como señala Sullivan (2012), estas dinámicas aproximan funcionalmente a estas organizaciones a formas de insurgencia criminal. En este contexto, la violencia trasciende su función económica y se convierte en un instrumento de gobernanza y control social (Hoffman, 2007; Felbab-Brown, 2017a).

El concepto de soberanía geoespacial resulta clave para comprender este fenómeno. Puede definirse como la capacidad del Estado para ejercer control efectivo sobre su espacio aéreo mediante la detección, identificación, monitoreo y neutralización de amenazas, sustentada en sistemas integrados de inteligencia geoespacial e ISR (NGA, 2006; Lowenthal, 2026; Johnson, 2026). Esta noción se vincula con la ventaja informacional, en la que la superioridad depende de la capacidad de procesar y explotar información en tiempo real (U.S. Department of Defense, 2020a).

Su erosión no implica necesariamente una derrota convencional, sino una pérdida progresiva de control operativo. Esta dinámica es consistente con lo que la literatura sobre amenazas emergentes identifica como fallas sistémicas en entornos complejos, donde la incapacidad de anticipar innovaciones adversarias genera

vulnerabilidades acumulativas (Jackson & Loidolt, 2013; Coyne et al., 2026).

Las consecuencias son estructurales: se debilita el alertamiento temprano (Grabo, 2010; Betts, 1982), se reduce la conciencia situacional y se configura una vulnerabilidad estratégica acumulativa que favorece a los actores adaptativos (Gray, 2014).

Como argumenta Guerra Hernández (2024), estas organizaciones están compuestas por nodos que desempeñan funciones específicas y que pueden no conocer —ni depender directamente de— otros nodos dentro de la misma red. Esta estructura celular y descentralizada proporciona ventajas operacionales fundamentales, entre ellas la resiliencia, la adaptabilidad, la negación plausible y la capacidad de sostener redes interdependientes sin depender de una jerarquía rígida.

En síntesis, el caso mexicano ilustra un conflicto híbrido en la zona gris del dominio aéreo, donde la distinción entre la seguridad pública, la interior y la defensa nacional se diluye progresivamente. La persistencia de la operación de los actores no estatales en este dominio refleja una falla estructural en la arquitectura de inteligencia y seguridad del Estado mexicano (López Portillo Vargas, 2019; SSPC, 2022). Sin una respuesta sistemáticamente orientada a fortalecer la soberanía geoespacial, particularmente mediante la integración de sistemas de ISR y el control del espacio aéreo, esta dinámica tenderá a profundizarse, lo que consolidará un escenario de competencia estratégica desfavorable para el Estado.

V. CAPACIDADES Y LIMITACIONES DEL ESTADO MEXICANO EN MATERIA DE INTELIGENCIA GEOESPACIAL

La evolución de las capacidades estatales mexicanas en materia de inteligencia geoespacial debe partir de un reconocimiento fundamental: México carece, a la fecha, de una arquitectura integrada de inteligencia, vigilancia y reconocimiento (ISR) orientada específicamente al dominio aéreo en el contexto de la seguridad interior.

Esta ausencia no es accidental ni el resultado de restricciones presupuestarias menores, sino consecuencia de decisiones estructurales acumuladas a lo largo de décadas, que han privilegiado un enfoque reactivo y operativo por encima de uno estratégico y anticipatorio en

materia de seguridad nacional (López Portillo Vargas, 2019; SSPC, 2022).

Las Fuerzas Armadas mexicanas han realizado inversiones significativas en capacidades tecnológicas en años recientes. De acuerdo con reportes de prensa nacional, se han impulsado proyectos orientados al desarrollo de capacidades antidrones, de herramientas de análisis de información y de sistemas de apoyo operativo, además de destinar recursos a la detección y neutralización de UAS (Dávila, 2025; Zamarrón, 2023; Rodríguez, 2025). Estas iniciativas representan avances importantes; sin embargo, su alcance sigue siendo predominantemente táctico.

La brecha más significativa no reside en el equipamiento, sino en la integración: México no dispone de un sistema nacional de conciencia de dominio aéreo equivalente al concepto de Air Domain Awareness (ADA), que permita fusionar datos provenientes de sensores heterogéneos, plataformas satelitales, radares de baja altitud y fuentes de inteligencia humana (HUMINT) en un cuadro operacional común y en tiempo real. Esta limitación implica que, aunque existen capacidades dispersas en distintas instituciones —SEDENA, SEMAR, Guardia Nacional y en el Centro Nacional de Inteligencia (CNI)— en este sentido no existen aún protocolos de intercambio de información, ni arquitectura de fusión de datos que permitan una respuesta coordinada frente a amenazas en el dominio aéreo (Lowenthal, 2022; U.S. Joint Chiefs of Staff, 2022).

Esta fragmentación institucional tiene consecuencias operativas directas, primero, porque genera ciclos de inteligencia lentos e ineficientes, en los que la información sobre la actividad de los RPAS criminales no se procesa ni se distribuye a la velocidad necesaria para habilitar respuestas efectivas. En segundo lugar, produce vacíos de cobertura territorial, particularmente en zonas de alta conflictividad como Tierra Caliente, la sierra de Chihuahua y los valles de Sinaloa, Guerrero, Baja California o Tamaulipas, y, recientemente, Jalisco, donde la actividad no tripulada puede operar sin una detección sistemática. En tercer lugar, limita la capacidad del Estado para construir patrones de inteligencia sobre redes de drones criminales, sus historiales de vuelo y tendencias, lo que dificulta la identificación de sus centros de gravedad, cadenas de suministro y estructuras de comunicación, mando y control (Mendoza García, 2021; DroneSec, 2026).

La dimensión geopolítica agrava este diagnóstico. La evidencia del despliegue de aeronaves no tripuladas del gobierno estadounidense realizando operaciones de inteligencia de señales (SIGINT) e ISR persistente sobre territorio mexicano (The War Zone, 2025) puede estar suscrita en los acuerdos binacionales para la atención a estos grupos criminales, dado que el gobierno americano escaló su respuesta a los cárteles mexicanos como organizaciones terroristas extranjeras, lo cual supone también un asunto relacionado con su seguridad nacional, pero también con el fentanilo como un arma de destrucción masiva, según su legislación. Lo cierto es que esta dinámica, comprensible por sí misma, también puede entenderse como una dependencia estratégica de México y debilita su capacidad para ejercer y preservar la soberanía en su propio territorio.

Adicionalmente, las evaluaciones de inteligencia estadounidense identifican a las organizaciones criminales transnacionales con base en México como actores que han desarrollado capacidades tecnológicas que, en ciertos contextos operativos, superan las de las instituciones de seguridad locales (ODNI, 2025, 2026). Esta valoración constituye un indicador relevante de la magnitud del déficit estratégico que enfrenta el Estado mexicano.

En este contexto, resulta ilustrativo contrastar la situación mexicana con modelos consolidados de integración en defensa aérea, como el North American Aerospace Defense Command (NORAD), cuya arquitectura binacional se sustenta en la fusión de inteligencia, sistemas de alerta temprana y capacidades de respuesta coordinada a nivel continental. Aunque el entorno operativo de México difiere sustancialmente —particularmente por la naturaleza no estatal de las amenazas que enfrenta—, la comparación permite evidenciar una brecha crítica en términos de integración y alcance estratégico.

En una lectura más profunda, el conflicto que enfrenta México no es estrictamente doméstico, sino transnacional y de carácter hemisférico, en el que organizaciones criminales operan a través de múltiples jurisdicciones, cadenas logísticas y redes financieras internacionales. En este sentido, las capacidades desarrolladas por estos actores exceden el ámbito nacional y se proyectan sobre la seguridad regional, configurando lo que puede entenderse como un sistema de empresas criminales transnacionales con efectos estratégicos.

Sin embargo, la respuesta institucional del Estado mexicano continúa siendo predominantemente circunscrita a marcos operativos nacionales

y enfoques reactivos, lo que genera una desalineación entre la escala del fenómeno y la arquitectura de respuesta. Esta asimetría estratégica implica que, mientras los actores criminales expanden sus capacidades y operaciones a nivel regional, el Estado mantiene una aproximación fragmentada y de alcance limitado.

En ausencia de una respuesta sistémica orientada a cerrar esta brecha —en particular mediante la integración de capacidades de ISR, el desarrollo de sistemas de alertamiento temprano y la consolidación de una arquitectura nacional de conciencia de dominio aéreo—, la tendencia observada se profundizará. En este escenario, son los actores no estatales, y no el Estado, quienes lideran la innovación tecnológica en el dominio aéreo, consolidando una condición de vulnerabilidad estratégica estructural (Gray, 2009, 2014; Coyne et al., 2026).

VI. HACIA UNA POLÍTICA DE INTELIGENCIA GEOESPACIAL PARA LA SEGURIDAD NACIONAL

La construcción de una arquitectura estatal efectiva frente a amenazas en el dominio aéreo no constituye un problema nuevo en la escena internacional. En la última década, diversos Estados con experiencia directa frente a amenazas sostenidas con sistemas aéreos no tripulados —particularmente Estados Unidos, Israel, Ucrania, los Estados miembros de la Unión Europea, Corea del Sur y Singapur— han desarrollado modelos de gobernanza institucional, marcos jurídicos específicos y arquitecturas doctrinales que ofrecen lecciones relevantes para el caso mexicano. El análisis comparativo de estas experiencias permite identificar cinco pilares estructurales que deberían orientar el diseño de una estrategia nacional de soberanía geoespacial.

El primer pilar es la consolidación institucional bajo un mando interagencial con autoridad ejecutiva efectiva. La experiencia estadounidense resulta particularmente ilustrativa. En 2020, el Departamento de Defensa creó la Joint Counter-Small Unmanned Aircraft Systems Office (JCO) como respuesta a la proliferación de amenazas con drones pequeños (U.S. Department of Defense, 2020b). No obstante, sus limitaciones de autoridad derivaron, en 2025, en la creación de la Joint Interagency Task Force 401 (JIATF-401), con capacidades propias de adquisición, reporte directo al Subsecretario de Defensa y mandato explícito de coordinación interagencial (Congressional Research Service, 2025). El principio establece amenazas transversales, con mando unificado y capacidad de decisión y de ejecución aceleradas. Modelos análogos han sido adoptados en

Corea del Sur y Singapur, donde la centralización operativa ha permitido integrar capacidades dispersas en estructuras permanentes de mando (Asia Today/UPI, 2026; Ng, 2025). Para México, este pilar implica superar esquemas de coordinación ad hoc y avanzar hacia una arquitectura interagencial que integre a SEDENA, la SEMAR, la Guardia Nacional, la CNI y la Fiscalía General de la República, preferiblemente con mando naval o militar.

El segundo pilar es la doctrina de defensa anclada en la inteligencia. La experiencia israelí demuestra que la efectividad frente a amenazas aéreas asimétricas no depende exclusivamente de la superioridad tecnológica, sino también de la integración de capacidades de ISR con sistemas escalonados de neutralización. Como documenta Frantzman (2024a), Israel ha estructurado su defensa en tres capas: guerra electrónica, defensa cinética tierra-aire y defensa aire-aire, todas articuladas bajo un sistema de comando y control alimentado por inteligencia de diversas fuentes. Esta arquitectura ha permitido tasas de intercepción superiores al 95 % (Frantzman, 2024b). La lección central termina siendo no tecnológica, sino doctrinal: la integración precede a la efectividad. Para México, este pilar implica abandonar la lógica reactiva y construir una doctrina integrada que articule la detección, la identificación, el seguimiento y la neutralización bajo un mismo marco operativo.

El tercer pilar es la integración whole-of-nation y la adaptación iterativa. La experiencia ucraniana, desarrollada en condiciones de conflicto de alta intensidad, muestra cómo un Estado puede construir capacidades en plazos acortados mediante la movilización coordinada de recursos estatales, privados y sociales (Kunertova, 2023; Borch & Heier, 2025). Tres elementos resultan clave: ciclos de adquisición acelerados, soluciones de bajo costo para amenazas de bajo costo y la integración de inteligencia geoespacial abierta con capacidades de ciberinteligencia (Calder, 2025; Defense One, 2026). Este modelo evita la trampa de costos asimétricos y permite una adaptación continua ante la evolución de la amenaza. Para México, este pilar implicaría reformar los esquemas de contratación, fomentar la colaboración entre la industria nacional y desarrollar mecanismos de innovación continua.

El cuarto pilar es la cooperación supranacional como multiplicador de capacidades. Ningún Estado contemporáneo enfrenta de manera aislada las amenazas al dominio aéreo. Iniciativas como la European Drone Defence Initiative (Calder, 2025) y la Operation Eastern Sentry de la OTAN (NATO, 2025) reflejan un enfoque integrado basado en

la interoperabilidad, el intercambio de inteligencia y la coordinación multinivel (European Commission & High Representative, 2025; Reeves, 2025). En el plano jurídico-operativo, la Unión Europea ha avanzado en la armonización de los marcos regulatorios y de los procedimientos de prueba y de adquisición (European Commission, 2022). Para México, este pilar implica consolidar mecanismos robustos de cooperación bilateral con Estados Unidos, especialmente ante amenazas transnacionales, y explorar esquemas de coordinación hemisférica con países que enfrentan dinámicas similares.

El quinto pilar consiste en el desarrollo de un marco jurídico específico para el ejercicio de la soberanía aérea en el ámbito de la seguridad interior. Ninguno de los modelos analizados opera en ausencia de claridad normativa. En Estados Unidos, la Sección 130i del Título 10 del U.S. Code (2017) establece procedimientos claros para manejar amenazas con UAS, definiendo las capacidades, limitaciones y responsabilidades de las instituciones. El Congreso ha ampliado y extendido esta autoridad en sucesivas leyes de defensa, más recientemente en el NDAA FY2025 (Congressional Research Service, 2025). Como señala Zoldi (2025), la claridad normativa constituye un factor determinante para la efectividad operativa. La Unión Europea ha seguido un camino similar mediante la armonización de estándares regulatorios (European Commission, 2022). En el caso de México, la falta de un marco legal es una debilidad fundamental, ya que limita las acciones operativas, la cooperación internacional y la protección de los derechos fundamentales.

En conjunto, estos cinco pilares configuran una agenda política coherente, sustentada en la experiencia internacional comparada. Su adopción, sin embargo, exige voluntad para que el Estado conciba la seguridad en el dominio aéreo no como un problema técnico, sino como una dimensión estratégica de primer orden. Como advierte la literatura sobre sorpresa estratégica y planificación de defensa, este tipo de transformación solo es posible cuando las instituciones reconocen oportunamente la erosión de sus ventajas estructurales y actúan con una visión estratégica a largo plazo (Betts, 1982; Gray, 2009, 2014; Kane et al., 2024; Coyne et al., 2026).

VII. CONCLUSIONES

El análisis desarrollado a lo largo de este artículo ha documentado, con base en evidencia empírica, testimonios oficiales y literatura especializada, una transformación estructural en las condiciones de

seguridad del Estado mexicano: la irrupción del dominio aéreo como un ámbito central de disputa estratégica entre el Estado y las organizaciones criminales transnacionales. Esta transformación no constituye un problema técnico menor ni un asunto exclusivamente operativo; por el contrario, es una vulnerabilidad estratégica de primer orden que compromete el ejercicio efectivo de la soberanía nacional.

Las organizaciones criminales mexicanas han transitado, en menos de una década, desde el uso experimental de drones comerciales hasta la institucionalización doctrinal de capacidades de inteligencia, vigilancia, reconocimiento y ataque en el dominio aéreo. Este proceso evolutivo —estructurado en tres etapas diferenciadas— ha estado acompañado de una adaptación tecnológica iterativa que incluye plataformas de fibra de carbono, resistencia a interferencias electrónicas, sistemas de denegación satelital y, de manera particularmente preocupante, la incorporación de doctrina de combate desarrollada en teatros de guerra contemporáneos. En paralelo, el Estado mexicano ha mantenido una arquitectura institucional fragmentada, reactiva y carente de una doctrina integrada de soberanía geoespacial.

La combinación de estos dos procesos configura un escenario de conflicto híbrido en zona gris en el que la distinción clásica entre seguridad pública, seguridad interior y defensa nacional resulta analíticamente insuficiente. Lo que está en disputa no es únicamente la capacidad del Estado para prevenir delitos específicos, sino también su autoridad estructural para ejercer un control efectivo sobre un dominio crítico del territorio nacional. En ausencia de una respuesta sistémica, esta dinámica tenderá a profundizarse, consolidando una ventaja informacional a favor de actores no estatales altamente adaptativos.

La experiencia internacional comparada —desde los modelos estadounidenses, israelíes y ucranianos hasta las iniciativas europeas, asiáticas y del sudeste asiático— demuestra que la recuperación de la soberanía geoespacial es técnicamente viable y doctrinalmente factible, siempre que se acompañe de voluntad política, de una arquitectura institucional coherente y de una visión estratégica de largo plazo. Los cinco pilares propuestos —consolidación institucional, doctrina multicapa anclada en inteligencia, integración whole-of-nation, cooperación supranacional y marco jurídico específico— no constituyen un catálogo de recomendaciones técnicas, sino una agenda integral de transformación estatal.

La pregunta que da título a este artículo —¿está México en riesgo?— admite, a la luz de la evidencia presentada, una respuesta inequívoca. El riesgo no es potencial ni futuro: es actual, documentado y creciente. La decisión pendiente no es si el Estado mexicano debe responder, sino cuánto tiempo más puede demorar una respuesta estratégica sin comprometer de manera irreversible su capacidad para ejercer soberanía plena sobre su espacio aéreo nacional.

Bibliografía completa en orden de aparición

1. Office of the Director of National Intelligence (ODNI). (2026). Annual threat assessment of the U.S. intelligence community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf
2. Villegas, P., & Zehbrauskas, A. (2025, September 1). With drones and IEDs, Mexico's cartels adopt arms of modern war. The New York Times. https://www.nytimes.com/2025/09/01/world/americas/mexico-cartel-weapons.html
3. Horowitz, M. C. (2018). The diffusion of military power: Causes and consequences for international politics. Princeton University Press.
4. Bunker, R. J., & Sullivan, J. P. (2021, November 11). Mexican cartels are embracing aerial drones, and they're spreading. War on the Rocks. https://warontherocks.com/2021/11/mexican-cartels-are-embracing-aerial-drones-and-theyre-spreading
5. Ziemer, H. (2025, June 11). Illicit innovation: Latin America is not prepared to fight criminal drones. Center for Strategic and International Studies. https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones
6. Willoughby, S. (2025, July 22). Securing the skies: Law enforcement, drones, and public safety [Testimony before the United States Senate Committee on the Judiciary]. U.S. Department of Homeland Security. https://www.judiciary.senate.gov/imo/media/doc/94f53245-d172-92ba-152b-06bc9ee00a50/2025-07-22%20-%20Testimony%20-%20Willoughby%20-%20final.pdf
7. Center for Strategic and International Studies. (2025, November 20). Countering the criminal drone threat in the Americas [Event]. https://www.csis.org/events/countering-criminal-drone-threat-americas
8. Nicas, J., & Villegas, P. (2026, February 12). Do drug cartels actually use drones at the border? The New York Times. https://www.nytimes.com/2026/02/12/world/americas/mexico-drone-border-cartels.html
9. Rodríguez, A. (2025, December 14). Cartels in Mexico take a leap forward with narco-drones: 'It is criminal groups that are leading the innovation race.' El País. https://english.elpais.com/international/2025-12-14/cartels-in-mexico-take-a-leap-forward-with-narco-drones-it-is-criminal-groups-that-are-leading-the-innovation-race.html

10. Bunker, R. J., & Sullivan, J. P. (2021, November 11). Mexican cartels are embracing aerial drones, and they're spreading. War on the Rocks. https://warontherocks.com/2021/11/mexican-cartels-are-embracing-aerial-drones-and-theyre-spreading/
11. Kramer, G., Vivoda, V., & Davies, A. (2023). Narco drones: Tracing the evolution of cartel aerial tactics in Mexico's low-intensity conflicts. Small Wars & Insurgencies, 34(6), 1095–1129. https://doi.org/10.1080/09592318.2023.2226382
12. Ziemer, H. (2025, June 11). Illicit innovation: Latin America is not prepared to fight criminal drones. Center for Strategic and International Studies. https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones
13. Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.
14. Más Información. (2026, February 12). Ejército y CJNG cuentan con el mismo armamento antidrones. https://massinformacion.com.mx/ejercito-y-cjng-cuentan-con-el-mismo-armamento-anti-drones/
15. The War Zone. (2025, February 18). CIA MQ-9 Reaper drones are covertly spying on Mexican drug cartels: Reports. The War Zone. https://www.twz.com/air/cia-mq-9-reaper-drones-are-covertly-spying-on-mexican-drug-cartels-reports
16. Forbes México. (2026, February 11). Fiscal de EU confirma derribo de drones presuntamente ligados a cárteles. Forbes México. https://forbes.com.mx/fiscal-de-eu-confirma-derribo-de-drones-presuntamente-ligados-a-carteles/
17. Willoughby, S. (2025, July 22). Securing the skies: Law enforcement, drones, and public safety [Testimony before the United States Senate Committee on the Judiciary]. U.S. Department of Homeland Security. https://www.judiciary.senate.gov/imo/media/doc/94f53245-d172-92ba-152b-06bc9ee00a50/2025-07-22%20-%20Testimony%20-%20Willoughby%20-%20final.pdf
18. Mazarr, M. J. (2015). Mastering the gray zone: Understanding a changing era of conflict. U.S. Army War College Press. https://press.armywarcollege.edu/monographs/428
19. Felbab-Brown, V. (2017a). Organized crime, illicit economies, civil violence & international order: More complex than you think. Daedalus, 146(4), 98–111. https://doi.org/10.1162/DAED_a_00453
20. Gray, C. S. (2009). Modern strategy. Oxford University Press.
21. Gray, C. S. (2014). Strategy and defence planning: Meeting the challenge of uncertainty. Oxford University Press.
22. Lowenthal, M. M. (2022). Intelligence: From secrets to policy (9th ed.). CQ Press.
23. Sims, J. E. (2022). Decision advantage: Intelligence in international politics from the Spanish Armada to cyberwar. Oxford University Press.
24. Boyle, M. J. (2020). The drone age: How drone technology will change war and peace. Oxford University Press.

25. Holland Michel, A. (2019). Eyes in the sky: The secret rise of Gorgon Stare and how it will watch us all. Mariner Books.
26. Rogers, J. P. (Ed.). (2024). De Gruyter handbook of drone warfare. De Gruyter.
27. Kunertova, D. (2024). Learning from the Ukrainian battlefield: Tomorrow's drone warfare. ETH Zürich. https://doi.org/10.3929/ethz-b-000690448
28. Gruszczak, A., & Kaempf, S. (Eds.). (2023). Routledge handbook of the future of warfare. Routledge.
29. National Geospatial-Intelligence Agency. (2006). Geospatial intelligence (GEOINT) basic doctrine. National Geospatial-Intelligence Agency.
30. Lowenthal, M. M. (2022). Intelligence: From secrets to policy (9th ed.). CQ Press.
31. Gruszczak, A., & Kaempf, S. (Eds.). (2023). Routledge handbook of the future of warfare. Routledge.
32. Haugstvedt, H. (2023). A flying reign of terror? The who, where, when, what, and how of non-state actors and armed drones. Journal of Human Security, 19(1), 1–7. https://doi.org/10.12924/johs2023.19010001
33. Bunker, R. J., & Sullivan, J. P. (2021, November 11). Mexican cartels are embracing aerial drones, and they're spreading. War on the Rocks. https://warontherocks.com/2021/11/mexican-cartels-are-embracing-aerial-drones-and-theyre-spreading/
34. Horowitz, M. C. (2018). The diffusion of military power: Causes and consequences for international politics. Princeton University Press.
35. Gruszczak, A., & Kaempf, S. (Eds.). (2023). Routledge handbook of the future of warfare. Routledge.
36. Parker, R. (2015, January 21). Drone loaded with meth crashes near Mexico-California border. Los Angeles Times. https://www.latimes.com/local/lanow/la-me-ln-drone-meth-crashes-tijuana-20150121-story.html
37. BBC News. (2015, May 2). Mexico drug gang shoots down military helicopter. BBC News. https://www.bbc.com/news/world-latin-america-32540648
38. ZETA. (2018, July 10). Con drones envían granadas a casa de Sosa Olachea. Semanario ZETA. https://zetatijuana.com/2018/07/con-drones-envian-granadas-a-casa-de-sosa-olachea/
39. Bunker, R. J., Sullivan, J. P., & Kuhn, D. A. (2020/2021). Use of weaponized consumer drones in Mexican crime war. Counter-IED Report, Winter 2020/2021, 69–77.
40. Ziemer, H. (2025, June 11). Illicit innovation: Latin America is not prepared to fight criminal drones. Center for Strategic and International Studies. https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones
41. Small Wars Journal Staff. (2026, January 29). How cartels are adopting drone tactics from Ukraine. Small Wars Journal. https://smallwarsjournal.com/2026/01/29/drug-cartel-operatives-snuck-

into-ukraine-for-drone-training-report-and-how-cartels-are-adopting-drone-tactics-from-ukraine
42. Höller, L. (2025, July 30). Drug cartel operatives snuck into Ukraine for drone training: Report. Defense News. https://www.defensenews.com/global/the-americas/2025/07/30/drug-cartel-operatives-snuck-into-ukraine-for-drone-training-report/
43. Ziemer, H. (2025, June 11). Illicit innovation: Latin America is not prepared to fight criminal drones. Center for Strategic and International Studies. https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones
44. Villegas, P. (2025, September 3). With drones and IEDs, Mexico's cartels adopt arms of modern war. The New York Times. https://www.nytimes.com/2025/09/01/world/americas/mexico-cartel-weapons.html
45. Kramer, G., Vivoda, V., & Davies, A. (2023). Narco drones: Tracing the evolution of cartel aerial tactics in Mexico's low-intensity conflicts. Small Wars & Insurgencies, 34(6), 1095–1129. https://doi.org/10.1080/09592318.2023.2226382
46. Kunertova, D. (2024). Learning from the Ukrainian battlefield: Tomorrow's drone warfare. ETH Zürich. https://doi.org/10.3929/ethz-b-000690448
47. Horowitz, M. C. (2018). The diffusion of military power: Causes and consequences for international politics. Princeton University Press.
48. Chaparro, L. (2021). Like a flying ant: An operative describes how Mexico's cartels use drones. Business Insider. https://www.businessinsider.com/how-mexico-cartels-use-drones-drug-smuggling-2021
49. Mendoza García, J. (2021). Organizaciones criminales y control territorial en México: Hacia un modelo analítico. Política y Gobierno, 28(2).
50. Grabo, C. M. (2010). Handbook of warning intelligence. Scarecrow Press.
51. Borch, O. J., & Heier, T. (Eds.). (2025). Preparing for hybrid threats to security: Collaborative preparedness and response. Routledge. https://www.routledge.com/Preparing-for-Hybrid-Threats-to-Security-Collaborative-Preparedness-and-Response/Borch-Heier/p/book/9781032627014
52. Ziemer, H. (2025, June 11). Illicit innovation: Latin America is not prepared to fight criminal drones. Center for Strategic and International Studies. https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones
53. Ziemer, H. (2025, June 11). Illicit innovation: Latin America is not prepared to fight criminal drones. Center for Strategic and International Studies. https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones
54. Rogers, J. P. (Ed.). (2024). De Gruyter handbook of drone warfare. De Gruyter.

55. Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilson, G. I. (1989). The changing face of war: Into the fourth generation. Marine Corps Gazette, 73(10), 22–26.
56. Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.
57. Mazarr, M. J. (2015). Mastering the gray zone: Understanding a changing era of conflict. U.S. Army War College Press. https://press.armywarcollege.edu/monographs/428
58. Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilson, G. I. (1989). The changing face of war: Into the fourth generation. Marine Corps Gazette, 73(10), 22–26.
59. Hammes, T. X. (2004). The sling and the stone: On war in the 21st century. Zenith Press.
60. Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.
61. Moghadam, A., Rauta, V., & Wyss, M. (Eds.). (2024). Routledge handbook of proxy wars. Routledge.
62. Felbab-Brown, V. (2017b). The extortion economy: Organized crime, corruption, and development. Brookings Institution Press.
63. Mazarr, M. J. (2015). Mastering the gray zone: Understanding a changing era of conflict. U.S. Army War College Press. https://press.armywarcollege.edu/monographs/428
64. Borch, O. J., & Heier, T. (Eds.). (2025). Preparing for hybrid threats to security: Collaborative preparedness and response. Routledge. https://www.routledge.com/Preparing-for-Hybrid-Threats-to-Security-Collaborative-Preparedness-and-Response/Borch-Heier/p/book/9781032627014
65. Rogers, J. P. (Ed.). (2024). De Gruyter handbook of drone warfare. De Gruyter.
66. Rogers, J. P. (Ed.). (2024). De Gruyter handbook of drone warfare. De Gruyter.
67. Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.
68. Felbab-Brown, V. (2017b). The extortion economy: Organized crime, corruption, and development. Brookings Institution Press.
69. Sullivan, J. P. (2012). From drug wars to criminal insurgency. Fondation Maison des Sciences de l'Homme.
70. National Geospatial-Intelligence Agency. (2006). Geospatial intelligence (GEOINT) basic doctrine. National Geospatial-Intelligence Agency.
71. Lowenthal, M. M. (2026). Intelligence: From secrets to policy (10th ed.). CQ Press.
72. Johnson, L. K. (Ed.). (2026). The Oxford handbook of national security intelligence (2nd ed.). Oxford University Press.
73. U.S. Department of Defense. (2020a). Joint concept for information advantage. U.S. Department of Defense.

https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf
74. Jackson, B. A., & Loidolt, B. (2013). Considering al-Qa'ida's Innovation Doctrine: From strategic texts to "innovation in practice." Terrorism and Political Violence, 25(2), 284–310. https://doi.org/10.1080/09546553.2012.662557
75. Coyne, J., Bassi, J., Taylor, C., Corera, J., Hughes, M., & Ciuffetelli, F. (2026). Strategic surprise in the 21st century: Complexity, systems failure, and national security. Australian Strategic Policy Institute.
76. Grabo, C. M. (2010). Handbook of warning intelligence. Scarecrow Press.
77. Kane, B. R., et al. (2024). Threats to critical infrastructure: A survey. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA2397-2.html
78. Guerra Hernández, V. H. (Ed.). (2024). Economías criminales: Enfoques multidimensionales. Editorial Diké.
79. López Portillo Vargas, E. (2019). La inteligencia en México: Reforma pendiente. Insyde.
80. Secretaría de Seguridad y Protección Ciudadana. (2022). Estrategia nacional de seguridad pública 2019–2024. Gobierno de México.
81. López Portillo Vargas, E. (2019). La inteligencia en México: Reforma pendiente. Insyde.
82. Secretaría de Seguridad y Protección Ciudadana. (2022). Estrategia nacional de seguridad pública 2019–2024. Gobierno de México.
83. Dávila, F. (2025, April 8). Sheinbaum rechaza incursión de EU con drones. Excélsior. https://www.excelsior.com.mx/nacional/sheinbaum-responde-reportes-de-que-eu-usara-drones-para-atacar-carteles/1709502
84. Zamarrón, I. (2023, September 25). Aumentan en México los ataques con drones equipados con explosivos. Forbes México. https://www.forbes.com.mx/aumentan-en-mexico-los-ataques-con-drones-equipados-con-explosivos/
85. Rodríguez, A. (2025, December 14). Cartels in Mexico take a leap forward with narco-drones. El País. https://english.elpais.com/international/2025-12-14/cartels-in-mexico-take-a-leap-forward-with-narco-drones-it-is-criminal-groups-that-are-leading-the-innovation-race.html
86. Lowenthal, M. M. (2022). Intelligence: From secrets to policy (9th ed.). CQ Press.
87. U.S. Joint Chiefs of Staff. (2022). Joint publication 2-0: Joint intelligence. U.S. Joint Chiefs of Staff.
88. Mendoza García, J. (2021). Organizaciones criminales y control territorial en México: Hacia un modelo analítico. Política y Gobierno, 28(2).
89. DroneSec. (2026). Global drone threat report 2026. DroneSec Intelligence Platform.
90. The War Zone. (2025, February 18). CIA MQ-9 Reaper drones are covertly spying on Mexican drug cartels: Reports. The War Zone.

https://www.twz.com/air/cia-mq-9-reaper-drones-are-covertly-spying-on-mexican-drug-cartels-reports
91. Office of the Director of National Intelligence (ODNI). (2025). Annual threat assessment of the U.S. intelligence community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf
92. Office of the Director of National Intelligence (ODNI). (2026). Annual threat assessment of the U.S. intelligence community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf
93. Gray, C. S. (2009). Modern strategy. Oxford University Press.
94. Gray, C. S. (2014). Strategy and defence planning: Meeting the challenge of uncertainty. Oxford University Press.
95. Coyne, J., Bassi, J., Taylor, C., Corera, J., Hughes, M., & Ciuffetelli, F. (2026). Strategic surprise in the 21st century: Complexity, systems failure, and national security. Australian Strategic Policy Institute. https://www.aspi.org.au/report/strategic-surprise-21st-century
96. U.S. Department of Defense. (2020b). Counter-small unmanned aircraft systems strategy. U.S. Department of Defense. https://media.defense.gov/2020/Jan/07/2002230619/-1/-1/1/COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF
97. Sayler, K., & Hoehn, J. R. (2021). Department of Defense counter-unmanned aircraft systems. Congressional Research Service.
98. Congressional Research Service. (2025, February 3). FY2025 NDAA: Countering uncrewed aircraft systems (Insight No. IN12418). https://www.congress.gov/crs-product/IN12418
99. Asia Today/UPI. (2026, April 16). South Korea to develop anti-drone defense strategy. UPI. https://www.upi.com/Top_News/World-News/2026/04/16/anti-drone-defense-capabilities/3101776372612
100. Ng, E. H. (2025, March 3). Speech by Minister for Defence, Dr. Ng Eng Hen, at the Committee of Supply 2025 [Speech transcript]. Ministry of Defence Singapore. https://www.mindef.gov.sg/news-and-events/latest-releases/04mar25_speech3/
101. Frantzman, S. J. (2024a). Drone wars: Pioneers, killing machines, artificial intelligence, and the battle for the future. Simon & Schuster. https://www.simonandschuster.com/books/Drone-Wars
102. Frantzman, S. J. (2024b, April 14). How Israel's layered air defense defeated Iran's massive drone and missile attack. The Jerusalem Post. https://www.jpost.com/israel-news/defense-news/article-797048
103. Kunertova, D. (2023). Learning from the Ukrainian battlefield: Tomorrow's drone warfare. ETH Zürich. https://doi.org/10.3929/ethz-b-000690448
104. Borch, O. J., & Heier, T. (Eds.). (2025). Preparing for hybrid threats to security: Collaborative preparedness and response. Routledge. https://www.routledge.com/Preparing-for-Hybrid-Threats-to-Security-Collaborative-Preparedness-and-Response/Borch-Heier/p/book/9781032627014

105. Calder, G. (2025, December 16). Building Europe's "drone wall": Embracing and scaling cheap defensive technologies. European Leadership Network. https://europeanleadershipnetwork.org/commentary/building-europes-drone-wall-embracing-and-scaling-cheap-defensive-technologies/
106. Defense One. (2026, April). How Ukraine's defense industry innovates at the speed of modern war. Defense One. https://www.defenseone.com/ideas/2026/04/ukraine-defense-industry-innovates-modern-war/412594/
107. European Commission. (2022). A drone strategy 2.0 for a smart and sustainable unmanned aircraft eco-system in Europe (COM(2022) 652 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022DC0652
108. European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2025, October 16). Defence readiness roadmap 2030 [Communication]. European Commission. https://defence-industry-space.ec.europa.eu/commission-and-high-representative-present-new-defence-roadmap-strengthen-european-defence-2025-10-16_en
109. North Atlantic Treaty Organization. (2025, September 12). NATO launches "Eastern Sentry" to bolster posture along eastern flank [News release]. https://www.nato.int/cps/en/natohq/news_237601.htm
109b. Congressional Research Service. (2025). Department of Defense counter unmanned aircraft systems: Background and issues for Congress (Report No. R48477). https://www.congress.gov/crs-product/R48477
110. Zoldi, D. M. K. (2025, June 8). Counter-drone laws under fire: The real danger is constitutional confusion, not C-UAS technology. Lawfire. https://sites.duke.edu/lawfire/2025/06/08/dawn-zoldi-on-counter-drone-laws-under-fire-the-real-danger-is-constitutional-confusion-not-c-uas-technology/
111. Betts, R. K. (1982). Surprise attack: Lessons for defense planning. Brookings Institution Press.
112. Gray, C. S. (2009). Modern strategy. Oxford University Press.
113. Gray, C. S. (2014). Strategy and defence planning: Meeting the challenge of uncertainty. Oxford University Press.
114. Kane, B. R., et al. (2024). Threats to critical infrastructure: A survey. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA2397-2.html
115. Coyne, J., Bassi, J., Taylor, C., Corera, J., Hughes, M., & Ciuffetelli, F. (2026). Strategic surprise in the 21st century: Complexity, systems failure, and national security. Australian Strategic Policy Institute. https://www.aspi.org.au/report/strategic-surprise-21st-century
116. Reeves, T. (2025, December 17). EU takes first steps to create drone wall on eastern flank. National Defense Magazine. https://www.nationaldefensemagazine.org/articles/2025/12/17/eu-takes-first-steps-to-create-d

RIS
Revista de Inteligencia y Seguridad

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C.

Inteligencia Estratégica: El Pilar de Seguridad Nacional del Estado Mexicano ante los Riesgos y Amenazas del Siglo XXI

Eduardo de Jesús Sayavedra Ruiz*

Resumen: En un mundo donde las fronteras físicas se desvanecen ante la explosión de la dataesfera y los conflictos ya no se libran sólo en campos de batalla tradicionales, ¿cómo puede el Estado Mexicano proteger a 133.3 millones de personas y un territorio de más de 5 millones de kilómetros cuadrados? Este artículo desentraña la compleja realidad de un país con una riqueza natural y económica excepcional, pero que enfrenta amenazas híbridas y asimétricas surgidas con potencial de explotar sus vulnerabilidades más profundas. Desde el impacto global de una pandemia hasta la resiliencia tecnológica del crimen organizado, el autor analiza por qué la inteligencia estratégica ha dejado de ser una opción para convertirse en una herramienta de supervivencia del Estado. A través de una visión prospectiva y multidimensional, esta obra propone transformar la inteligencia en la brújula que guíe las decisiones nacionales, permitiendo que México no sólo reaccione a las crisis; sino que las anticipe en defensa de su soberanía y bienestar.

Palabras clave: Inteligencia estratégica, Seguridad Nacional, Amenazas híbridas, Amenazas asimétricas, Riesgos, Dataesfera, Vulnerabilidad y Estado Mexicano.

Abstract: In a world where physical borders fade before the explosion of the datasphere and conflicts are no longer fought solely on traditional battlefields, how can the Mexican State protect 133.3 million people and a territory spanning over 5 million square kilometers? This article unravels the complex reality of a nation with exceptional natural and economic wealth,

* Licenciado en Inteligencia para la Seguridad por la Universidad Anáhuac, Especialista en Análisis en Seguridad Nacional y Regional por la Escuela de Inteligencia para la Seguridad Nacional, Maestro en Inteligencia Policial y Seguridad Nacional por el Centro de Prácticas Universitarias Lucía Botín, Maestro en Análisis, Seguimiento y Lucha contra el Narcotráfico por el Centro de Prácticas Universitarias Lucía Botín y Maestro en Analítica e Inteligencia de Negocios por la Universidad Tecnológica de México. Actualmente, se desempeña como analista de inteligencia en el sector privado y como docente sobre temas relacionados con Inteligencia y Seguridad Nacional en la Universidad Anáhuac y en el Centro de Estudios de Defensa de la Secretaría de la Defensa Nacional.

yet one that faces hybrid and asymmetric threats with the potential to exploit its deepest vulnerabilities. From the global impact of a pandemic to the technological resilience of organized crime, the author analyzes why strategic intelligence has ceased to be an option and has become a vital tool for state survival. Through a prospective and multidimensional vision, this work proposes transforming intelligence into the compass that guides national decisions, allowing Mexico not only to react to crises but to anticipate them in defense of its sovereignty and well-being.

Key Words: Strategic intelligence, National Security, Hybrid threats, Asymmetric threats, Risks, Datasphere, Vulnerability and Mexican State.

1. Introducción: La tarea de velar por la seguridad de un ente de 133 millones de habitantes y una extensión de 5,121,136 km2

La tarea de velar por la integridad, estabilidad y permanencia del Estado Mexicano es una actividad compleja que requiere de un enfoque multifactorial y multidisciplinario, la cual debe ser realizada dentro de un marco jurídico específico y puntual de la materia. Dicha tarea, constituye un reto permanente que demanda colaboración, coordinación, profesionalización, compromiso, capital humano, recursos materiales y económicos que sean guiados por el pilar e insumo indispensable para la Seguridad Nacional: La Inteligencia Estratégica.

El Estado Mexicano, constituye un ente jurídico, político y social complejo que acorde con estimaciones del Consejo Nacional de Población, para el 2025, cuenta con una población aproximada de 133.3 millones de personas la cual se encuentra asentada en un territorio que abarca 5,121,136.7 km2 (1,960,646.7 km2 corresponden a la superficie continental, 10,570 km2 corresponden a la plataforma continental extendida y 3,149,920 km2 corresponden a la superficie marítima).(Gobierno de México, 2024)

El componente demográfico del Estado Mexicano es diverso; ya que abarca una gran variedad de culturas, entre las cuales destaca la presencia de 68 pueblos indígenas cada uno con su propia lengua, las cuales se extienden hasta 364 variantes. (Gobierno de México, 2023). Estas comunidades cuentan con usos y costumbres definidas, las cuales se encuentran protegidas por diversos ordenamientos del marco jurídico del Estado Mexicano.

Aunado a lo anteriormente expuesto, y para dimensionar la complejidad demográfica del Estado Mexicano, resulta imperioso mencionar que México es el décimo primer país más poblado del mundo, concentrando al 1.6% de la población mundial, teniendo una distribución demográfica del 88.30% en entornos urbanos y del 11.70% en entornos rurales. (Worldometers, 2026)

En cuanto al ámbito geográfico, México cuenta con fronteras amplias, teniendo una frontera de 3,141 kilómetros con los Estados Unidos (Magaña et al. 2018) (siendo una de las fronteras terrestres más activas y dinámicas del mundo en cuanto al traslado de mercancías y cruce de personas), 959 kilómetros con Guatemala y 288 kilómetros con Belice. (Gobierno de México, 2024) En cuanto a los litorales del país, éstos tienen una longitud de 11,122 kilómetros en su parte continental. (Gobierno de México, 2018), evidenciando la gran extensión marítima que tiene México. En cuanto a la orografía del país, el 70% corresponde a sistemas montañosos. (Gobierno de México, 2026), lo cual supone un enorme reto en materia de conectividad, seguridad y desarrollo.

En cuanto a su riqueza natural, México es uno de los 17 países megadiversos del mundo. (Centro Mesoamericano, 2020), ocupando la quinta posición en plantas vasculares, la tercera en mamíferos, la décimo primera en aves, la segunda en reptiles y la quinta en anfibios. (Gobierno de México, 2023) Lo anterior, supone que México concentra entre el 10 y el 12 porciento de la biodiversidad mundial en apenas el 1.31 porciento de la superficie terrestre mundial. (Georank, 2026)

En cuanto a recursos naturales, México ocupa la vigésima primera posición de las reservas de petróleo del mundo, con 5,901,800,000 barriles (representando el 0.33 porciento de la cuota mundial de petróleo). (Worldometer, 2025) México ha sido durante varios años consecutivos el mayor productor de plata del mundo, concentrando el 23% de la producción mundial, ocupando también la octava posición en producción de oro, novena posición en producción de cobre y la sexta posición en producción de zinc. (Santillán, 2024)

En el ámbito económico, México se encuentra entre las 20 economías más grandes del mundo, ocupando la décimo tercera posición en tamaño, así como el sexto lugar en materia de exportaciones totales, así como la vigésima sexta economía más compleja acorde con el Índice de Complejidad Económica. (Datawhel, 2026) México

sobresale como un importante exportador de autopartes, autos, camiones, tractores, monitores, pantallas, computadoras, electrodomésticos, minerales, cerveza, tequila, tomates rojos, frutos rojos, aguacate y muchos otros alimentos.

Los datos anteriormente expuestos, evidencian la grandiosidad de México como país en cuanto a su riqueza y diversidad cultural y natural; sin embargo, también suponen una vulnerabilidad inherente a sus dimensiones demográficas y territoriales. Un país tan amplio y complejo como lo es México, requiere de un insumo esencial para poder asegurar su estabilidad, integridad y permanencia en el tiempo: la inteligencia estratégica.

Habiendo descrito brevemente el objeto de referencia de interés para la Seguridad Nacional del Estado Mexicano, es posible transitar a describir la naturaleza de los nuevos antagonismos y riesgos inherentes del siglo XXI.

2. El entorno de los riesgos y amenazas del siglo XXI

Actualmente, resulta innegable negar el hecho de que los Estados y las sociedades se encuentran fuertemente interrelacionados unos de otros en distintos ámbitos tales como el económico, migratorio, militar, comercial, energético, tecnológico, logístico, sanitario y hasta cultural.

Esta interdependencia e interrelación forma parte de las nuevas dinámicas de conformación, integración y funcionamiento de los Estados y sociedades alrededor del mundo. Lo anterior se debe a una multiplicidad de fenómenos, actores y procesos con múltiples aristas. Aunque especialmente el mundo no se encogió, la ventana temporal para atravesarlo espacialmente se redujo sustancialmente en el ámbito del intercambio de mercancías y el flujo de personas, por no decir del intercambio de ideas e información, la cual está creciendo y fluyendo como nunca en la historia de la humanidad.

Esta reducción en la percepción del tamaño espacial del mundo está aparejada a una expansión innegable del mundo de los datos, en donde ya se habla de la "dataesfera", entendida como el ecosistema o el entorno en donde se crean, almacenan e intercambian los datos entre una multiplicidad de plataformas, actores y softwares que trascienden cualquier frontera tanto física como digital. (Iglesias, 2023)

Para ejemplificar este fenómeno en la expansión en la creación, almacenamiento y difusión de datos, se comparte el siguiente gráfico:

Fuente: Statista (Iglesias, 2023)

Esta predicción en el crecimiento de la dataesfera refleja que en el futuro no sólo habrá más datos; sino que se requerirán mayores soluciones de almacenamiento, procesamiento y análisis de datos. Este ecosistema de datos creciente, constituye una enorme oportunidad para el análisis de datos para la elaboración de inteligencia estratégica, operativa y táctica para el Estado, orientada a la prevención más que a la reacción; pero también constituye una enorme amenaza que pudiese ser explotada por actores estatales y no estatales antagonistas al Estado Mexicano.

Habiendo visto la prospectiva, en cuanto a la cantidad de datos que se están generando, es importante hacer una retrospectiva sobre el mismo tema, permitiéndonos contar con un panorama completo sobre la cuestión de la dataesfera pasada, actual y futura.
A continuación, se adjunta una tabla que ejemplifica el crecimiento exponencial de los datos desde 1986 hasta el 2020.

Año	Capacidad de Almacenamiento Mundial (Exabytes)
1986	2.6 EB
1993	15.8 EB
2000	54.5 EB
2007	295 EB
2014	5000 EB
2020	6800 EB

Fuente: Rivery (Bartley, 2025)

Como es posible vislumbrar, el crecimiento de los datos ha sido exponencial, lo cual está aparejada con otro de los elementos que conforman al entorno en el cual se gestan, desarrollan y materializan los riesgos y amenazas del siglo XXI.

La generación, distribución, almacenamiento y análisis de datos no es una cuestión de ninguna manera exclusiva de los actores estatales; sino que la gran parte de la dataesfera ha sido erigida por y para actores no estatales, lo cual es reflejo de un cambio en la expansión de los actores dentro del sistema internacional.

El sistema internacional ha transitado de un esquema en el que únicamente existían actores estatales en el telón internacional, a integrar otro tipo de actores tales como lo son las organizaciones no gubernamentales, las organizaciones internacionales, las empresas multinacionales (también llamadas corporaciones) y hasta la opinión pública internacional. (Restrepo, 2013) Este cambio en la integración de actores que componen el sistema internacional supone una transformación en los procesos y las dinámicas bajo las cuales se vislumbran, desarrollan y materializan los riesgos y amenazas a los actores estatales, contribuyendo a aumentar la complejidad en su respectiva prevención y mitigación.

La conjunción de un crecimiento desbordado de datos y el incremento en la relevancia de los actores no estatales dentro del sistema internacional suponen un entorno propicio en el cual muchas de los antagonismos modernos se desarrollan y materializan.

De igual modo, es posible vislumbrar una transición hacia un sistema internacional complejo multipolar en donde es posible identificar polos de poder muy marcados con una clara ausencia de liderazgo

mundial, en la que cualquier materia se vuelve un instrumento de negociación en el marco de la realpolitik. (Fiocchi, 2025), lo cual se ha materializado en una erosión de las normas de Derecho Internacional.

Lo anterior permite advertir que las amenazas y los riesgos a los que el Estado Mexicano se enfrenta, han evolucionado y mutado hacia problemáticas multifactoriales que requieren de soluciones basadas en inteligencia estratégica, acompañada de una voluntad política férrea, así como de la canalización de recursos materiales y capital humano especializado.

Habiendo descrito el entorno en el cual se gestan los nuevos riesgos y amenazas del siglo XXI, es posible transitar a realizar una descripción y un análisis de la naturaleza de éstas.

3. La naturaleza de los riesgos y amenazas del siglo XXI

Las amenazas emergentes inherentes al siglo XXI, y su probabilidad de ocurrencia expresada en los riesgos, cuentan con características muy particulares que las diferencian de aquellas del pasado, volviendo a la Seguridad Nacional una disciplina actual, más necesaria que nunca y con especiales requerimientos de inteligencia estratégica para su debida salvaguardia.

Los nuevos antagonismos y amenazas son producto de una realidad difícilmente predecible debido a una multiplicidad de actores que ya trascienden a los Estados, con una pluralidad de escenarios inciertos con posibilidades infinitas de mutabilidad en donde intervienen una conjunción de pugnas por intereses de diversa índole.

Dicho lo anterior, resulta conveniente enumerar algunas de las características que distinguen a las amenazas del siglo XXI, las cuales evidencian su naturaleza, siendo las siguientes:

1. Trascienden sus respectivos ámbitos de origen.
2. Tienen múltiples causas.
3. Se mimetizan y ocultan dentro de la complejidad de las dinámicas nacionales y globales.
4. Se interrelacionan entre sí para potencializar sus efectos.
5. Tienen potencial y capacidades de escalamiento, pudiendo pasar de ser una problemática nacional a una regional e inclusive a una global.

6. La tecnología cataliza sus capacidades de expresión y expansión.
7. Se caracterizan por su incertidumbre en cuanto a patrones y tendencias, pudiendo reinventarse para adaptarse al entorno.
8. Pueden tener un alto impacto en el objeto de referencia a custodiar, aún con pocos recursos o medios a su disposición.
9. Explotan y aprovechan la interdependencia del sistema internacional y las relaciones de sus respectivos actores.
10. Tienen altas capacidades resilientes en contra de estrategias y/o planes destinados a combatirlas.

Habiendo descrito algunas de las características de las amenazas a las que se enfrenta el Estado Mexicano y muchos otros actores estatales y no estatales dentro del sistema internacional, resulta imperioso ahondar en cada una de ellas para tener una mejor comprensión de la naturaleza de las mismas.

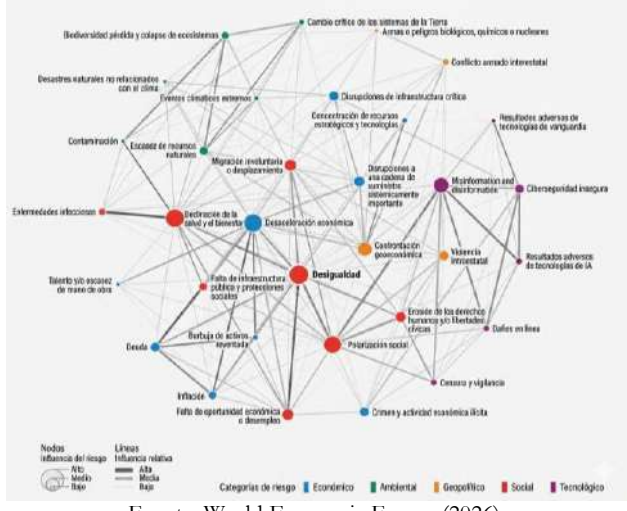
La característica que hace alusión a que las amenazas trascienden a sus respectivos ámbitos de origen, está íntimamente relacionada con otra de sus características, la cual hace referencia a su potencial y capacidad de escalamiento, pudiendo pasar de ser una amenaza local a ser una amenaza nacional, para posteriormente ser una amenaza regional y finalmente una amenaza global. Un ejemplo puntual de una amenaza con dichas características fue la amenaza sanitaria de la pandemia provocada por el virus del coronavirus SARS-CoV-2, la cual inició en noviembre del 2019 en la provincia de Wuhan, China. Transcurrirían 4 meses para que la Organización Mundial de la Salud la declarara una pandemia (enfermedad de alcance global), puntualmente el 11 de marzo del 2020.(OMS, 2020) En el caso puntual de México, el arribo de un padecimiento respiratorio a más de 12,000 kilómetros de distancia, que cobró la vida de 334,336 personas acorde con cifras oficiales del Gobierno de México (Gobierno de México, 2023) y 833,473 vidas según la Comisión Independiente de Investigación sobre la Pandemia de Covid-19 en México, evidencia la capacidad de las amenazas del siglo XXI de trascender de sus respectivos ámbitos de origen y de escalar en cuanto a su magnitud y manifestación.

Las características de las amenazas concernientes a la mimetización y ocultamiento dentro de la complejidad de las dinámicas nacionales y globales, la multiplicidad de causas que les dan origen, su resiliencia ante estrategias o planes destinadas a combatirlas y la capacidad de reinventarse están ligadas estrechamente, dándoles ventajas sobre

estructuras burocráticas y formales que se oponen a su existencia y funcionamiento, tal como el Estado Mexicano. Un ejemplo sobre esta característica, es la resiliencia que tienen algunos grupos criminales para el mantenimiento de sus operaciones a pesar de fuertes golpes estructurales y operativos destinados a desmantelarlos, incluso con esfuerzos internacionales, tal como el Cártel Jalisco Nueva Generación o el Cártel de Sinaloa en el escenario mexicano. (Manzi, Calderoni, 2024)

Las características de interrelación entre sí para la potencialización de sus efectos y el aprovechamiento de la interdependencia del sistema internacional tiene que ver con las características inherentes al entorno en el cual se desarrolla el escenario global. El Reporte de Riesgos Globales 2026 del Foro Económico Mundial, evidencia perfectamente estas características, mostrando una clara correlación entre los tipos de riesgos según su naturaleza.

A continuación, se muestra un mapa de interconexiones de riesgos globales:



Fuente: World Economic Forum (2026)

Como es posible ver en el mapa de interconexiones de riesgos globales, hay una clara interrelación entre riesgos de índole económico, ambiental, geopolítico, social y tecnológico. Esta interrelación es posible advertirla en cadenas logísticas, transacciones

financieras, elaboración de determinados productos y satisfacción de necesidades energéticas por parte de Estados y regiones enteras.

Una disrupción en un determinado componente del sistema puede provocar una falla sistémica que afecte distintos ámbitos. La interrelación que existe en múltiples campos es una vulnerabilidad de gran envergadura en el sistema internacional actual; por lo que no es posible vislumbrar un componente del sistema como una unidad aislada.

La característica del uso de la tecnología como catalizador de sus capacidades de expresión y expansión y el uso de pocos recursos, se encuentran relacionadas, en cuanto a que la tecnología permite llegar a más personas en menor tiempo para la transmisión de mensajes, los cual puede permitirle a determinados actores antagonistas el robustecimiento de sus operaciones y/o la expansión en el número de sus simpatizantes o colaboradores. Un ejemplo de este tipo de característica ha sido el uso de las redes sociales y videojuegos por parte de grupos criminales para el reclutamiento de niños y jóvenes. (Bledsoe, 2025) Otro ejemplo de esta característica es la ampliación de las capacidades de los actores criminales en materia tecnológica, innovando en el uso de la inteligencia artificial para la comisión de una amplia variedad de ilícitos digitales, así como el uso de criptomonedas para el financiamiento de sus operaciones, la venta de mercancía ilegal en línea, el establecimiento de comunicaciones cifradas y seguras para asegurar sus operaciones, entre otras. (El Khoury, 2025)

Habiendo revisado las características y la naturaleza de las nuevas amenazas, es posible transitar a describir dos conceptos que cambian por completo la visión de la Seguridad Nacional: las amenazas híbridas y las amenazas asimétricas.

4. Las amenazas híbridas

Las amenazas híbridas son aquellas en las que un actor, pudiendo ser estatal o no estatal, despliega métodos que se encuadran en espacios "grises", combinando medios convencionales y no convencionales para causar daños a los intereses nacionales de Estados. Las amenazas híbridas replantean el panorama de la Seguridad Nacional en cuanto a su capacidad de evolución, su velocidad, escalabilidad en intensidad y cobertura. Este tipo de amenazas son potenciadas por la rápida

incorporación de nuevas tecnologías y por la innegable conectividad global de la cual hablamos algunos párrafos atrás. (North Atlantic Treaty Organization, 2026)

Las amenazas híbridas se caracterizan por una ausencia marcada de autoría en los ataques que despliegan, en donde no es fácilmente establecer responsabilidades ante una afectación directa. Adicionalmente, se caracterizan por operar en un espacio intermedio entre la paz y la guerra, causando daños sin existir una condición de guerra abierta o total. De igual modo, se caracterizan por actuar de manera coordinada y en multidominios, pudiendo tener afectaciones físicas, digitales y hasta psicológicas sobre los Estados objetivo. Este tipo de amenazas suelen aprovechar todas las vulnerabilidades de un Estado, bien pudiendo aprovechar su propio territorio, poner a su población contra su gobierno o generar disrupciones en su infraestructura crítica. Un elemento verdaderamente peligroso, es que pueden desestabilizar Estados con costos relativamente bajos en comparación con los presupuestos que las instituciones de seguridad pueden destinar a combatirlos, pudiendo tener actividades de alto impacto con costos muy bajos. Finalmente, este tipo de amenazas se mantiene en constante evolución para resistir los embates de sus adversarios, sean actores estatales o no estatales, siempre manteniéndose a la vanguardia al no tener reglas, políticas o marcos jurídicos burocráticos y poco flexibles.

5. Amenazas asimétricas

Por otro lado, los Estados se enfrentan hoy a las amenazas asimétricas, las cuales como su nombre lo indica, son aquellas en las que hay una desigualdad en los actores que se enfrentan. En el marco de las amenazas asimétricas, el actor más débil adoptará tácticas y estrategias que le permitan explotar las vulnerabilidades del actor más fuerte. (Center for International Relations & International Security, 2024)

Este tipo de amenazas se caracterizan por haber una desproporción en los recursos, capital humano y capacidades, siendo usualmente la que se encuentra en una aparente desventaja. Las amenazas asimétricas se aprovechan de la rigidez estructural de mando, la obligación de actuación bajo el cobijo de la legalidad y la falta de flexibilidad en las actuaciones.

Otra característica de las amenazas asimétricas es el marcado aprovechamiento del terreno en el cual realizan sus operaciones, teniendo muchas veces un conocimiento pleno del campo de operaciones en el cual se desarrollan. Este dominio del terreno es difuso; pues no versa sobre tener un control físico completo del mismo mediante el establecimiento de una base de operaciones fija; sino que implica contar con el apoyo de la población local, el establecimiento de centros de mando clandestinos e itinerantes desde donde puedan coordinar y lanzar sus operaciones. Su capacidad de mimetización, las vuelve difíciles de distinguir de la población civil y al aprovechar tanto el terreno como la demografía local, anula casi por completo la ventaja táctico-operativa del enemigo más poderoso.

Este tipo de amenazas suelen hacer uso de estrategias de dominio cognitivo y de operaciones psicológicas; ya que los actores que representan una amenaza asimétrica, tal como el crimen organizado, no busca derrotar ni destruir a su enemigo por completo, sino anular su voluntad de combatir en un determinado territorio. El objeto de la amenaza asimétrica es vencer a su adversario mediante el desgaste del mismo, aprovechando su tamaño y capacidades para hacerlo caer por sus propios medios.

Una de las características más emblemáticas es la ausencia de un uniforme, la falta de una cadena de mando rígida o la inexistencia de lineamientos o políticas que deban seguirse, las tácticas innovadoras y de bajo costo para la realización de sus operaciones, así como el uso de la tecnología para magnificar sus acciones en contra del adversario más fuerte. La derrota del actor más fuerte viene muchas veces por la opinión pública al ser cuestionada sobre sus capacidades para enfrentar a dicha amenaza "menor".

Al haber abordado brevemente las características de las amenazas a las cuales se enfrentan los actores estatales en la actualidad, es posible transitar hacia el entendimiento del uso de la inteligencia como herramienta imprescindible para mantener la integridad, estabilidad y permanencia del Estado Mexicano.

6. La inteligencia estratégica como el pilar de la Seguridad Nacional

Habiendo visto el objeto de referencia tan complejo y amplio con el que cuenta la Seguridad Nacional en nuestro país, resulta innegable el hecho de que la inteligencia estratégica es un elemento que ya no es

sólo necesario; sino imprescindible para asegurar la integridad, estabilidad y permanencia del Estado Mexicano.

Si en el pasado, durante el apogeo de las amenazas y riesgos tradicionales, el uso de la inteligencia era crucial, hoy en día, con la aparición de las amenazas asimétricas y las amenazas híbridas de las que hablamos líneas atrás, resulta un ejercicio de supervivencia Estatal.

La inteligencia estratégica debe ser el pilar de la Seguridad Nacional del Estado Mexicano con las siguientes características:

1. Contar con una visión prospectiva de largo plazo (entre 20 y 50 años) que permee y sobreviva a las visiones de los gobiernos que vayan asumiendo el poder, imponiendo las necesidades del Estado sobre las necesidades de los gobiernos.

2. Ser una prioridad para los tomadores de decisiones de los tres órdenes de gobierno, debiendo basar la ejecución de sus proyectos políticos en datos.

3. Adoptar una naturaleza multidimensional en la función de inteligencia al ser una actividad inherente a todas las instituciones del Estado, no únicamente las relacionadas con la Seguridad Pública o la Defensa Nacional.

4. Servir como herramienta para adaptar el marco jurídico nacional a las necesidades del Estado Mexicano y a su población, teniendo por objeto asegurar el bienestar y el desarrollo de los mismos.
5. Integrar la inteligencia proveniente del sector privado con la del Estado Mexicano para la reducción de la incertidumbre y hacerle frente a las amenazas de índole antropológico y naturales.

6. Ampliar las capacidades instaladas de inteligencia del Estado Mexicano para prevenir amenazas y no reaccionar ante los embates de las mismas.

7. Fortalecer la cultura de la inteligencia, promoviendo y ampliando la oferta académica en instituciones públicas y

privadas para la conformación de futuros científicos de datos, analistas de inteligencia y expertos en la materia.

El término de inteligencia estratégica ha ido ganando notoriedad en la sociedad mexicana; sin embargo, falta mucho camino por recorrer para aprovechar todo el potencial de la misma para la conducción y desarrollo de las decisiones con impacto nacional e internacional.

Como se vio anteriormente en el presente escrito, la explosión en la generación, almacenamiento y distribución de datos, supone una oportunidad inmejorable para fortalecer las capacidades de lo que la inteligencia estratégica puede ofrecer para el Estado Mexicano.

La inteligencia estratégica es el pilar de la Seguridad Nacional del Estado Mexicano por excelencia debido a que suministra alertas tempranas que transforman datos en información y ésta a su vez se convierte en conocimiento accionable para hacerle frente a riesgos y amenazas de diversa índole.

Es el pilar de la Seguridad Nacional debido a que permite reducir la incertidumbre en entornos altamente complejos e inciertos para la toma de decisiones, garantizando condiciones de certeza, estabilidad, desarrollo y bienestar, logrando con ello la continuidad del Estado Mexicano.

La inteligencia estratégica, en conclusión, dota a los líderes de una ventaja competitiva y cognitiva que garantiza que la política pública no sea sólo reactiva; sino una herramienta de planeación estratégica que le permite al Estado Mexicano garantizar condiciones dignas en un entorno global volátil e incierto.

7. Conclusiones

El Estado Mexicano cuenta con características geográficas, demográficas, económicas, energéticas y geológicas que lo vuelven un actor estatal relevante en el escenario global; sin embargo, cuenta con vulnerabilidades muy marcadas con respecto a su demografía (133.3 millones de habitantes) y una geografía estratégica pero conflictiva (4,388 kilómetros de fronteras, un territorio de 5,121,136 km2 y un litoral de 11,122 kilómetros). Como es posible vislumbrar, el objeto de referencia de la Seguridad Nacional es un ente amplio y complejo que requiere de atención táctica, operativa y sobre todo, estratégica.

Las amenazas a las cuales se enfrenta el Estado Mexicano son más complejas, variadas y numerosas que en antaño, cuando se concebían las amenazas tradicionales. Hoy en día, México se enfrenta a antagonismos que se interrelacionan, que se adaptan, que son resilientes, que no portan un uniforme o bandera particular, que se aprovechan de la interdependencia del sistema internacional, que no siguen ningún marco jurídico, que innovan y que explotan las vulnerabilidades propias del Estado.

Las amenazas híbridas y asimétricas son realidades ante las cuales el Estado Mexicano debe estar listo para enfrentar, al tenerlas plenamente identificadas, analizadas, y así, poder prevenir, mitigar y reducir la influencia de éstas; habilitando un espacio de acción basado en la prevención más allá de una reacción descoordinada.

La Seguridad Nacional en el siglo XXI implica una visión multidimensional, de enfoque estratégico que trascienda problemáticas de Seguridad Pública, que le permitan garantizar la integridad, estabilidad y permanencia al Estado Mexicano. En el marco de lo anterior, es donde la inteligencia estratégica juega un papel protagónico al advertir amenazas y riesgos para la prevención de crisis nacionales y regionales. La inteligencia estratégica debe ser la brújula para la conducción del país, siendo una herramienta de Estado y no de gobierno.

Los riesgos y amenazas del siglo XXI a los que se enfrenta el Estado Mexicano requieren de consideraciones técnicas aparejadas con voluntad política para prevenirlas, enfrentarlas y superarlas, siendo que sólo de esta forma se podrá garantizar la supervivencia del Estado en un sistema internacional donde este concepto ha ido cediendo espacios a otro tipo de actores.

8. Referencias

Armstrong, Martin. (16 de abril del 2019). *La Creación global de datos está a punto de explotar*. Statista, consultado el 9 de abril del 2026 en: https://www.statista.com/chart/17727/global-data-creation-forecasts/

Bartley, Kevin. (28 de mayo del 2025). *Big data statistics: How much data is there in the world?* Rivery, consultado el 9 de abril del 2026 en: https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world/#:~:text=According%20to%20IDC%2C%20the%20overall,segment%2C%20followed%20by%20social%20media

Bledsoe, Rubi. (28 de mayo del 2025). *The Role of Social Media in Cartel Recruitment*. Center for Strategic & International Studies, consultado el 11

de abril del 2026 en: https://www.csis.org/analysis/role-social-media-cartel-recruitment#:~:text=Beyond%20social%20media%2C%20cartels%20are,any%20type%20of%20video%20game

Center for International Relations & International Security. (2024). *Asymmetric Warfare*. Center for International Relations & International Security, consultado el 12 de abril del 2026 en: https://www.ciris.info/learningcenter/asymmetric-warfare/#:~:text=Disparity%20in%20Power:%20At%20its,disrupting%20stability%20and%20exerting%20influence

Centro Mesoamericano para el Intercambio de Conocimientos y Experiencias Forestales. (2020). *México*. Centro Mesoamericano para el Intercambio de Conocimientos y Experiencias Forestales, consultado el 8 de abril del 2026 en: https://cmicef.org/mexico/

Comisión Independiente de Investigación sobre la Pandemia de Covid-19 en México. (2023). *Impacto de la pandemia en México: consecuencias fundamentales (2020-2023)*. Comisión Independiente de Investigación sobre la Pandemia de Covid-19 en México, consultado el 10 de abril del 2026 en: https://www.comisioncovid.mx/

Datawheel. (2026). *Economía México*. Observatorio de Complejidad Económica, consultado el 8 de abril del 2026 en: https://oec.world/es/profile/country/mex

El Khoury, Chady. (Septiembre del 2025). *Combatir la criminalidad facilitada por la tecnología*. Fondo Monetario Internacional, consultado el 11 de abril del 2026 en: https://www.imf.org/es/publications/fandd/issues/2025/09/fighting-tech-fueled-crime-chady-el-khoury

Fiocchi, María Antonieta. (28 de noviembre del 2025). *The shift in the world's balances: the return of Realpolitik*. ESCP International Politics Society, consultado el 10 de abril del 2026 en: https://pppescp.com/2025/11/28/the-shift-in-the-worlds-balances-the-return-of-realpolitik/

Georank. (2026). *Superficie terrestre de México: rango de tamaño y tipos de territorio*. Georank, consultado el 8 de abril del 2026 en: https://georank.org/size/mexico#:~:text=Mexico's%20land%20area%20is%20750%2C563,1.62%25%20of%20the%20world's%20forests

Gobierno de México. (11 de octubre del 2018). *Mares mexicanos*. Secretaría de Medio Ambiente y Recursos Naturales, consultado el 8 de abril del 2026 en: https://www.gob.mx/semarnat/articulos/mares-mexicanos#:~:text=Los%20litorales%20de%20M%C3%A9xico%20tienen,Mar%20Caribe%20(INEGI%202002)

Gobierno de México. (2023). *México Megadiverso*. Comisión Nacional para el Conocimiento y Uso de la Biodiversidad, consultado el 8 de abril del 2026 en: https://www.biodiversidad.gob.mx/pais/quees

Gobierno de México. (2024). *Extensión Territorial de México*. Instituto Nacional de Estadística y Geografía, consultado el 8 de abril del 2026 en: https://cuentame.inegi.org.mx/descubre/geografia/extension_territorial/

Gobierno de México. (2024). *Fronteras de México*. Instituto Nacional de Estadística y Geografía, consultado el 8 de abril del 2026 en: https://cuentame.inegi.org.mx/descubre/geografia/fronteras/#:~:text=%C2%

BFCu%C3%A1les%20son%20las%20fronteras%20naturales,M%C3%A9xico%20de%20los%20Estados%20Unidos?&text=En%20la%20frontera%20sur%2C%20los,una%20frontera%20de%20959%20kil%C3%B3metros

Gobierno de México. (2025). *La Situación Demográfica de México*. Consejo Nacional de Población, consultado el 8 de abril del 2026 en: https://www.gob.mx/cms/uploads/attachment/file/1019967/Libro_LSDM_2025_02sep2025-1-10.pdf

Gobierno de México. (25 de junio del 2023). *Covid-19 México*. Gobierno de México, consultado el 10 de abril del 2026 en: https://datos.covid-19.conacyt.mx/

Gobierno de México. (9 de agosto del 2023). *Día Internacional de los Pueblos Indígenas*. Comisión Nacional de Zonas Áridas, consultado el 8 de abril del 2026 en: https://www.gob.mx/conaza/articulos/dia-internacional-de-los-pueblos-indigenas-341934

Gobierno de México. *El relieve de México*. Secretaría de Educación Pública, consultado el 8 de abril del 2026 en: https://nuevaescuelamexicana.sep.gob.mx/contenido/coleccion/el-relieve-en-mexico/

Iglesias, Carlos. (5 de mayo del 2023). *La datasfera en la que vivimos: el sistema de datos interconectado.* Gobierno de España, Ministerio para la Transformación Digital y de la Función Pública, consultado el 9 de abril del 2026 en: https://datos.gob.es/es/blog/la-dataesfera-en-la-que-vivimos-el-sistema-de-datos-interconectado

Magaña et al. (2018) *Panorama actual de la frontera de México y Estados Unidos*. Centro de Estudios Internacionales Gilberto Bosques del Senado de la República, consultado el 8 de abril del 2026 en: https://centrogilbertobosques.senado.gob.mx/analisisinvestigacion/contexto/ni-fronteramx-eeuu-010617#:~:text=La%20frontera%20entre%20M%C3%A9xico%20y%20Estados%20Unidos%20tiene%20una%20extensi%C3%B3n,flujos%20comerciales%20y%20de%20personas

Manzi, Deborah & Calderoni, Francesco. (2024). *The resilience of drug trafficking organizations: Simulating the impact of police arresting key roles*. Universita Cattolica del Sacro Cuore, consultado el 10 de abril del 2026 en: https://publicatt.unicatt.it/retrieve/05eb2f91-c80c-49d7-9b9f-e5b1b9e4a3b4/Manzi%20%26%20Calderoni%20%282024%29%20-%20The%20resilience%20of%20drug%20trafficking%20organizations.%20Simulating%20the%20impact%20of%20police%20arresting%20key%20roles.pdf

North Atlantic Treaty Organization. (29 de enero del 2026). *Countering hybrid threats*. North Atlantic Treaty Organization, consultado el 12 de abril del 2026 en: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

Organización Mundial de la Salud. (27 de abril del 2020). *COVID-19: cronología de la actuación de la OMS*. Organización Mundial de la Salud, consultado el 10 de abril del 2026 en: https://www.who.int/es/news/item/27-04-2020-who-timeline---covid-19

Restrepo Vélez, Juan Camilo. (Diciembre del 2013). *La globalización en las relaciones internacionales: Actores internacionales y sistema internacional contemporáneo*. Revista de la Facultad de Derecho y Ciencias Políticas de la

Universidad Pontificia Bolivariana, consultado el 9 de abril del 2026 en:http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-38862013000200005#:~:text=En%20conclusi%C3%B3n%2C%20la%20perspectiva%20realista,las%20firmas%20multinacionales%20y%20la

Santillán, Aldo. (2024). *Recursos y reservas minerales en México*. Mining México, consultado el 8 de abril del 2026 en: https://miningmexico.com/recursos-y-reservas-minerales-de-mexico/

World Economic Forum. (2026). *The Global Risk Report 2026*. World Economic Forum, consutado el 11 de abril del 2026 en: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf

Worldometer. (2025). *Reservas de petróleo por país*. Worldometer, consultado el 8 de abril del 2026 en: https://www.worldometers.info/es/petroleo/reservas-de-petroleo-por-pais/

Worldometers. (2026). *Población de México.* Worldometers, consultado el 8 de abril del 2026 en: https://www.worldometers.info/es/poblacion-mundial/poblacion-mexico/#:~:text=La%20densidad%20de%20poblaci%C3%B3n%20en%20M%C3%A9xico%20es,mediana%20en%20M%C3%A9xico%20es%20de%2030%20a%C3%B1os

RIS
Revista de Inteligencia y Seguridad

NÚMERO 5
(ENERO-JUNIO 2026)

"ESTUDIOS DE INTELIGENCIA EN EL SIGLO XXI: EVOLUCIÓN DEL CAMPO Y RETOS PARA LA SEGURIDAD"