

**El expediente probatorio de la complicidad china en el ataque a la Base Muwaffaq Salti:
inteligencia de todas las fuentes y los límites de la denegabilidad plausible en el espacio
comercial de uso dual**

Michael Chong Pineda
Artificial Intelligence Academy
13 de septiembre de 2026

Índice

Marco teórico: inteligencia de todas las fuentes y el problema de la atribución estratégica	4
Contexto empírico: el ataque a Muwaffaq Salti y el ecosistema satelital comercial chino	6
Los cinco eslabones del expediente probatorio	9
Rastro forense digital y telemetría de descarga (CYBINT/SIGINT)	10
Trazabilidad de requisitos de misión y efemérides orbitales (GEOINT/IMINT)	12
Fusión de fichas de blanco y metadatos de navegación (TECHINT)	13
Vínculo jurídico y corporativo con el Estado chino (OSINT/FININT)	15
Fuentes humanas e interceptaciones estratégicas (HUMINT/COMINT)	18
Estudio de caso comparado: el patrón Chang Guang–Spacety, de Ucrania a Yemen y Jordania	19
Los límites de la denegabilidad plausible ante el derecho internacional	20
Discusión: implicaciones para la gobernanza espacial y la seguridad hemisférica	22
Conclusiones	25
Referencias	28

El 17 de julio de 2026, misiles balísticos y drones de ataque directo iraníes impactaron la Base Aérea Muwaffaq Salti, en las afueras de Azraq, Jordania, matando a tres militares estadounidenses e hiriendo a otros cuatro (Task & Purpose, 2026; The Aviationist, 2026). El ataque ocurrió en el marco de la guerra abierta entre Estados Unidos e Irán iniciada a finales de febrero de 2026, y la base —que aloja al 332.º Ala Expedicionaria Aérea de la Fuerza Aérea estadounidense— había sido blanco recurrente de la artillería de precisión iraní a lo largo del año, incluyendo un ataque documentado en marzo contra un radar de defensa antimisiles THAAD AN/TPY-2 (Defence Security Asia, 2026b). Lo que distingue el episodio del 17 de julio de los bombardeos anteriores no es solo su letalidad, sino la aparente sofisticación de la selección de blancos: el análisis de imágenes satelitales posteriores sugirió que las municiones iraníes impactaron con precisión estructuras de alojamiento de reciente construcción, un patrón que, según analistas de inteligencia de fuentes abiertas, implicaría una recolección previa capaz de vincular el avance de obra con los requerimientos operativos estadounidenses inferidos (Defence Security Asia, 2026b).

Esa precisión reabrió una pregunta que las agencias de inteligencia occidentales llevan más de un año investigando: ¿en qué medida la República Popular China, a través de su pujante sector satelital comercial, ha proporcionado a Irán y a sus representantes (proxies) la inteligencia geoespacial necesaria para sostener una cadena de reconocimiento y ataque de precisión? La pregunta no es hipotética ni retórica. En mayo de 2026 el Departamento de Estado de Estados Unidos sancionó a tres empresas satelitales chinas —Chang Guang Satellite Technology, The Earth Eye Co. y Meentropy Technology— por su presunta participación en la cadena de selección de blancos que habría sostenido los ataques iraníes contra fuerzas estadounidenses en la región (Defence Security Asia, 2026c; Oficina de Control de Activos Extranjeros [OFAC], 2026).

Sin embargo, entre la sospecha fundada y la certeza jurídicamente accionable —aquella que permitiría sustentar una acusación formal ante el Consejo de Seguridad de las Naciones Unidas o justificar represalias en el marco del derecho internacional— existe una distancia probatoria considerable. Beijing opera de manera deliberada a través de un ecosistema de empresas nominalmente privadas y de marcos espaciales de uso dual diseñados para preservar lo que la literatura de inteligencia denomina denegabilidad plausible: la capacidad de un Estado de beneficiarse de una operación encubierta sin dejar un rastro jurídico que le sea directamente

atribuible (Kasapoglu, 2026). Este ensayo sostiene que cerrar esa distancia exige abandonar el análisis de fuente única y adoptar un estándar de inteligencia de todas las fuentes (All-Source Intelligence) que integre simultáneamente cinco eslabones probatorios independientes: el rastro forense digital y de telemetría; la trazabilidad de las órdenes de apuntamiento orbital; la fusión de metadatos de los sistemas de guía recuperados; el vínculo jurídico-corporativo entre las empresas satelitales y el aparato de seguridad del Estado chino; y las fuentes humanas y las interceptaciones estratégicas. El argumento central es que, si bien ningún eslabón aislado basta para atribuir responsabilidad estatal de manera inequívoca, la convergencia de los cinco —evaluada contra el patrón ya documentado de Chang Guang en apoyo al Grupo Wagner en Ucrania y a los hutíes en el mar Rojo— constituye un umbral probatorio razonable para sostener la complicidad material china en el ataque a Muwaffaq Salti.



Figura 1. Síntesis del expediente probatorio de la complicidad china en el ataque a la Base Muwaffaq Salti.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

Marco teórico: inteligencia de todas las fuentes y el problema de la atribución estratégica

La distancia entre la sospecha técnica y la imputación política

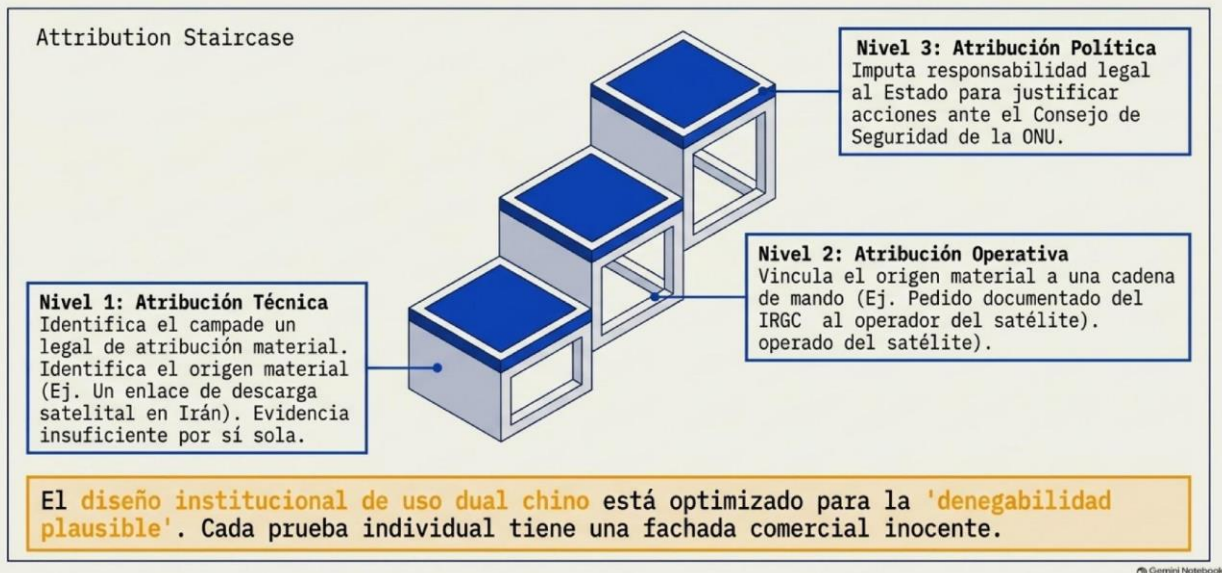


Figura 2. La distancia entre la sospecha técnica y la imputación política: la escalera de atribución (técnica, operativa, política).

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

La inteligencia de todas las fuentes parte de una premisa metodológica exigente: ninguna disciplina de recolección aislada —ya sea de señales (SIGINT), de imágenes (IMINT), geoespacial (GEOINT), técnica (TECHINT), de fuentes abiertas (OSINT), financiera (FININT) o humana (HUMINT)— produce por sí sola una imagen jurídicamente robusta de la intencionalidad estatal detrás de una operación encubierta. Esta limitación se agrava en el dominio espacial comercial, donde la frontera entre actividad civil legítima y apoyo militar encubierto es, por diseño, ambigua. El propio concepto de uso dual —tecnologías y activos que sirven simultáneamente a fines civiles y militares— constituye el mecanismo estructural que China ha empleado para insertar activos de inteligencia estatal dentro de un mercado aparentemente competitivo y globalizado de observación terrestre (Kasapoglu, 2026).

El problema de la atribución estratégica, tal como se ha desarrollado en la literatura sobre conflictos híbridos y guerra cibernética, distingue entre tres niveles de certeza: la atribución técnica (identificar el origen material de una acción), la atribución operativa (vincular ese origen con una cadena de mando) y la atribución política (imputar responsabilidad al Estado como tal). Aplicado al caso satelital, un solo enlace de descarga (downlink) hacia territorio iraní constituye, en el mejor

de los casos, atribución técnica; solo la convergencia de evidencia jurídico-corporativa, financiera y de mando permite ascender hacia la atribución política que exigiría un foro como el Consejo de Seguridad. Es este tránsito —de la sospecha técnica a la imputación política— el que estructura la arquitectura probatoria propuesta en este ensayo.

Un segundo elemento del marco teórico, tomado de la literatura sobre guerra híbrida, es la distinción entre evidencia corroborante y evidencia dispositiva. La evidencia corroborante aumenta la probabilidad de una hipótesis sin descartar explicaciones alternativas; la evidencia dispositiva la establece más allá de una duda razonable. En el caso del espacio comercial de uso dual, casi ningún elemento individual alcanza el estatus de evidencia dispositiva, precisamente porque el diseño institucional chino —empresas nominalmente privadas, contratos comerciales formalmente lícitos, marcos legales de confidencialidad— está optimizado para que cada elemento, tomado aisladamente, admita una lectura inocente. La función metodológica de la inteligencia de todas las fuentes no es, entonces, producir un elemento dispositivo único, sino demostrar que la probabilidad conjunta de que los cinco eslabones converjan de manera simultánea por pura coincidencia comercial es estadísticamente marginal, incluso cuando cada eslabón individual permanece, en rigor, corroborante y no dispositivo.

Resulta pertinente subrayar que el estándar probatorio no es homogéneo según el foro. Ante un tribunal doméstico, el umbral puede ser relativamente bajo si se trata de sanciones administrativas —como demuestra la facilidad relativa con la que la Oficina de Control de Activos Extranjeros del Tesoro estadounidense ha designado a Chang Guang Satellite Technology bajo distintos regímenes de sanciones desde 2023 (OFAC, 2026)—. Pero ante el Consejo de Seguridad, o como justificación de una represalia armada bajo el artículo 51 de la Carta de las Naciones Unidas, el estándar se aproxima al de la certeza razonable más allá de toda duda político-diplomática, dado que una acusación errónea contra una potencia con asiento permanente y capacidad de veto tiene costos estratégicos desproporcionados. De ahí que el expediente deba construirse como un sistema de corroboración cruzada, y no como una acumulación de indicios de una sola disciplina.

Contexto empírico: el ataque a Muwaffaq Salti y el ecosistema satelital comercial chino

La anomalía de precisión del 17 de julio de 2026

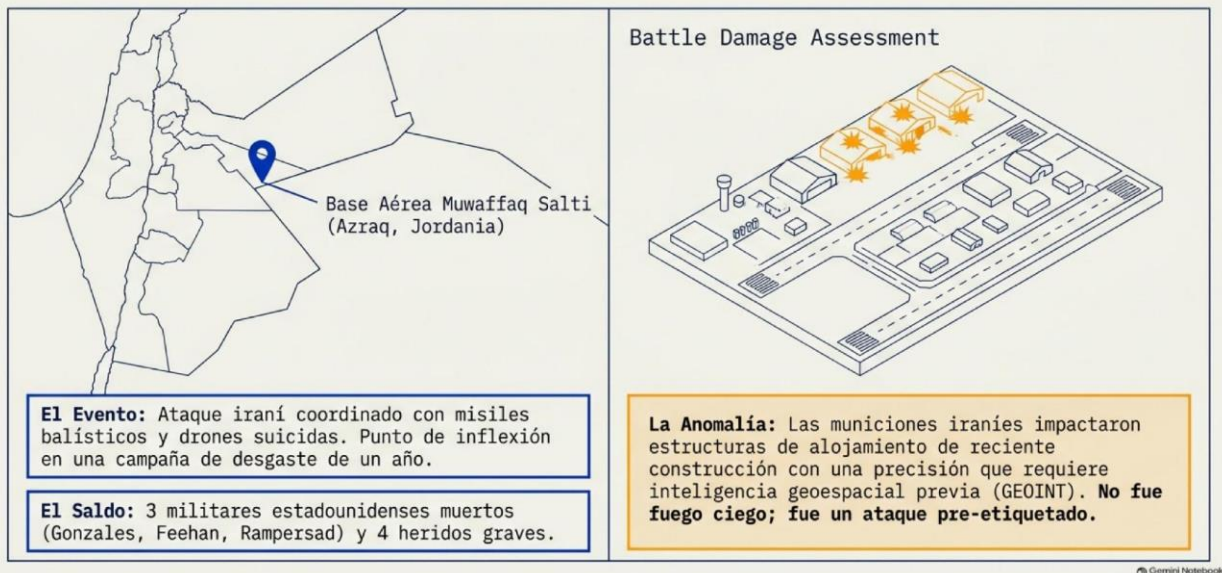


Figura 3. La anomalía de precisión del ataque del 17 de julio de 2026 contra la Base Aérea Muwaffaq Salti.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

Muwaffaq Salti, cuyo nombre honra a un piloto de la Real Fuerza Aérea Jordana caído en combate en 1966, es una base jordana —no estadounidense— situada en el desierto oriental cerca de Azraq, a unos ochenta kilómetros de Amán (Migflug, 2026; Radio Free Europe/Radio Liberty [RFE/RL], 2026). Su relevancia estratégica radica en que ha servido como plataforma de lanzamiento para las operaciones aéreas estadounidenses contra Irán, lo que la convirtió en blanco recurrente durante 2026. El ataque del 17 de julio, ejecutado con misiles balísticos y municiones merodeadoras de un solo uso, costó la vida a la soldado Isabella Gonzales, al teniente Tyler James Feehan y al sargento Angel S. Rampersad, además de dejar a otros cuatro efectivos heridos y evacuados a hospitales jordanos (Task & Purpose, 2026).

De manera paralela a la escalada militar, analistas de fuente abierta documentaron que la constelación Jilin-1, operada por Chang Guang Satellite Technology y compuesta por más de un centenar de satélites de observación terrestre, habría estado observando en tiempo casi real elementos clave del conflicto: patrones de ataque, despliegues de aeronaves, trayectorias de misiles y ciclos logísticos estadounidenses, en lo que un análisis describió como la generación de un conjunto de datos de guerra estadounidense en tiempo real para uso militar futuro de Beijing (Defence Security Asia, 2026a). Funcionarios estadounidenses, incluido el entonces subasesor de

Seguridad Nacional Jon Finer, acusaron públicamente a China de habilitar los ataques iraníes mediante inteligencia derivada de monitoreo satelital comercial, acusación que Beijing rechazó calificando la actividad de sus empresas como observación terrestre estrictamente comercial (Defence Security Asia, 2026a).

El nodo específico señalado por la investigación periodística y de inteligencia abierta es el satélite TEE-01B, construido por Chang Guang Satellite Technology por encargo de The Earth Eye Co. —un intermediario de exportación con sede en Beijing especializado en mercados de la Franja y la Ruta— y lanzado en junio de 2024 bajo la descripción oficial de "levantamientos de tierra, monitoreo de desastres y cartografía geográfica" (Kharon, 2026). Según documentos de la Fuerza Aeroespacial del Cuerpo de la Guardia Revolucionaria Islámica (IRGC) filtrados y citados por el Financial Times, Teherán habría adquirido acceso operativo a ese satélite desde septiembre de 2024, dieciocho meses antes del inicio del conflicto abierto, lo que sugiere una relación de suministro de inteligencia geoespacial preexistente y no una improvisación de guerra (China in Space, 2026b). En mayo de 2026 el Departamento de Estado formalizó estas sospechas al sancionar a Chang Guang por la probable recolección de imágenes de activos estadounidenses a través de Jilin-1, a Meentropy Technology por el presunto etiquetado automatizado mediante aprendizaje automático de aeronaves, refugios reforzados, depósitos de combustible y sistemas de radar en el Medio Oriente, y a The Earth Eye Co. por el suministro directo de imágenes a Irán (China in Space, 2026a; Defence Security Asia, 2026c).

Conviene precisar, además, el contexto más amplio del conflicto dentro del cual se inscribe el ataque a Muwaffaq Salti, ya que la magnitud del costo humano estadounidense acumulado ayuda a explicar la urgencia política de resolver la pregunta de atribución. Según cifras del Departamento de Defensa citadas por Task & Purpose (2026), un total de dieciocho militares estadounidenses habían muerto en apoyo a las operaciones contra Irán desde el inicio del conflicto a finales de febrero de 2026, incluyendo trece efectivos en marzo —seis de ellos en el accidente de un avión cisterna LC-135 en el occidente de Irak— y una muerte adicional en Erbil durante la detonación controlada de municiones de un dron iraní derribado. Este acumulado de bajas, sumado al hecho de que las tropas estadounidenses en Jordania estuvieron defendiéndose activamente de ataques con misiles balísticos y drones el mismo día del 17 de julio (RFE/RL, 2026), sitúa al caso Muwaffaq Salti no como un incidente aislado sino como el punto de inflexión de una campaña de

desgaste sostenida, en la que la calidad de la inteligencia de selección de blancos disponible para Irán adquiere una relevancia estratégica directamente proporcional al número de vidas estadounidenses en juego.



Figura 4. El espacio comercial de uso dual como arma estratégica: cobertura satelital convergente sobre el área del ataque.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

Los cinco eslabones del expediente probatorio

Cerrar la brecha requiere cinco eslabones probatorios concurrentes

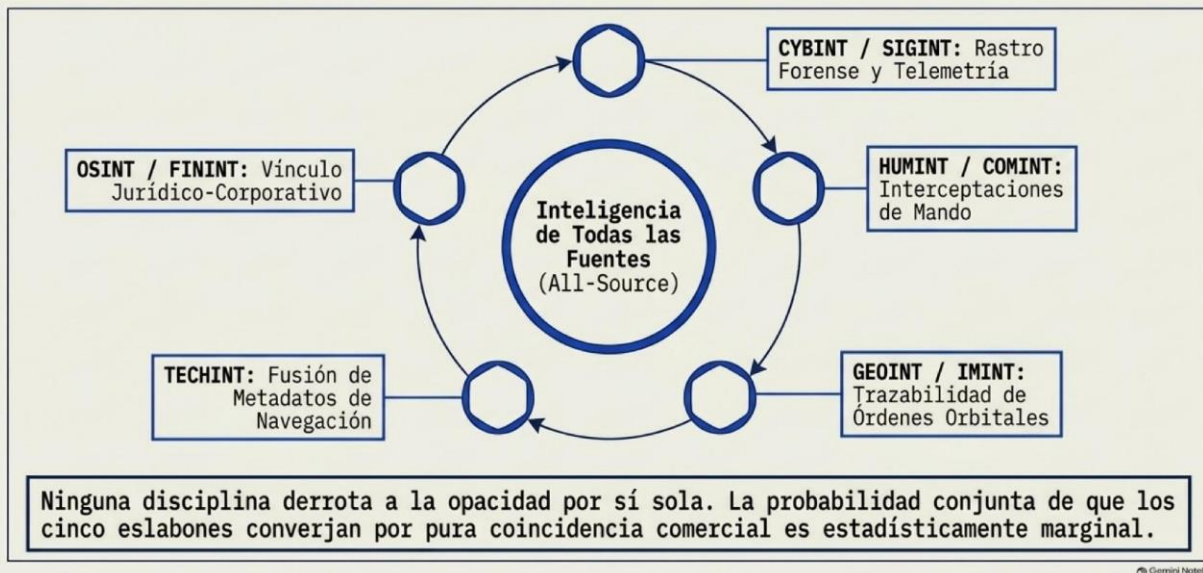


Figura 5. Los cinco eslabones probatorios concurrentes que exige la inteligencia de todas las fuentes.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

Construir un caso que resista el escrutinio de un foro internacional exige romper la separación artificial entre el Estado chino, sus constelaciones comerciales y los operadores de misiles iraníes mediante cinco líneas de evidencia complementarias, cada una anclada en una disciplina de inteligencia distinta.

Rastro forense digital y telemetría de descarga (CYBINT/SIGINT)

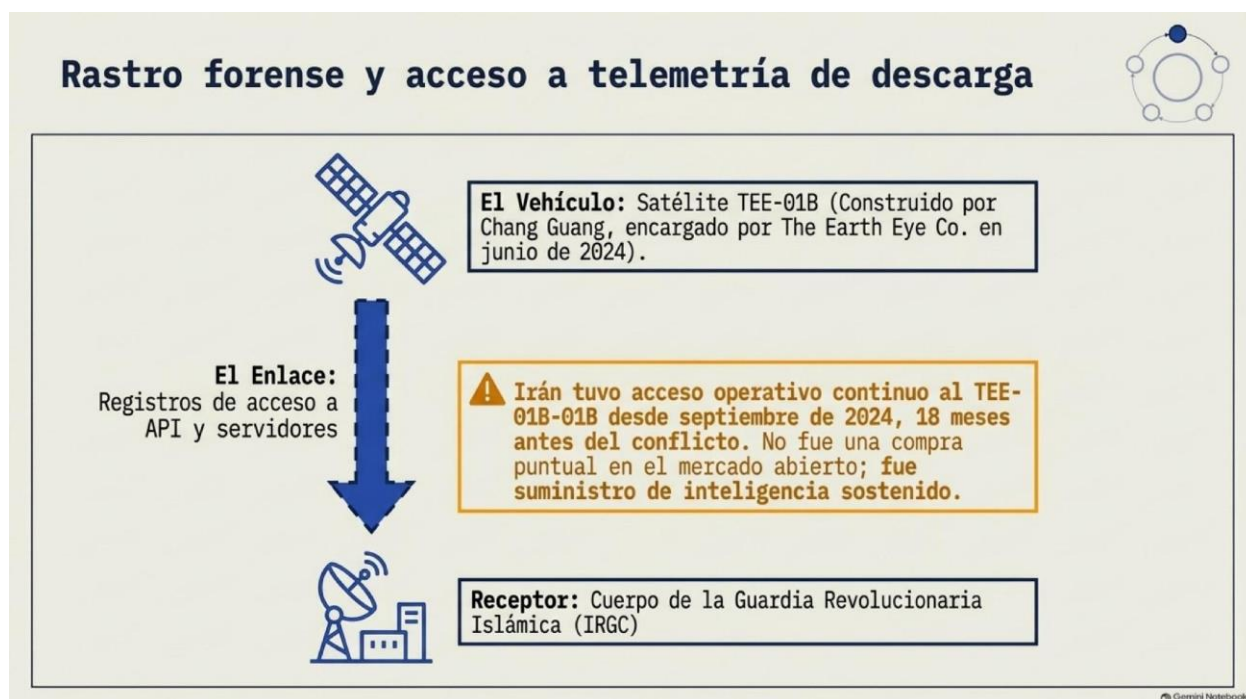


Figura 6. Rastro forense y acceso a telemetría de descarga: la cadena satélite TEE-01B–IRGC.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

El primer eslabón es la evidencia técnica más directa: conectar los servidores del operador satelital chino con las estaciones terrenas iraníes. Esto requiere, en primer lugar, registros de acceso a interfaces de programación de aplicaciones (API) y a servidores comerciales que demuestren que terminales asociadas al IRGC o a intermediarios como The Earth Eye Co. descargaron imágenes de alta resolución de Muwaffaq Salti en fechas inmediatamente previas al ataque. En segundo lugar, exige telemetría de enlaces descendentes que documente la transmisión de datos brutos desde un satélite óptico o de radar de apertura sintética (SAR) chino hacia estaciones receptoras dentro de territorio iraní durante ventanas orbitales específicas. La revelación de que Irán habría tenido acceso operativo continuo al satélite TEE-01B desde 2024 —y no un acceso puntual coincidente con el ataque— constituye precisamente el tipo de patrón temporal sostenido que la telemetría de descarga permitiría corroborar de manera forense (China in Space, 2026b; Kharon, 2026).

La dificultad práctica de este eslabón es que la infraestructura de descarga de datos satelitales comerciales rara vez es accesible a investigadores externos, y su reconstrucción depende casi por completo de capacidades de inteligencia de señales estatales —es decir, de fuentes que, por definición, los servicios de inteligencia occidentales no divulgan públicamente incluso cuando

existen—. Esto explica por qué las sanciones del Departamento de Estado de mayo de 2026, pese a nombrar específicamente a las tres empresas y describir sus roles diferenciados en la cadena de selección de blancos, no fueron acompañadas de la publicación de los registros de acceso o telemetría subyacentes (OFAC, 2026).

Trazabilidad de requisitos de misión y efemérides orbitales (GEOINT/IMINT)

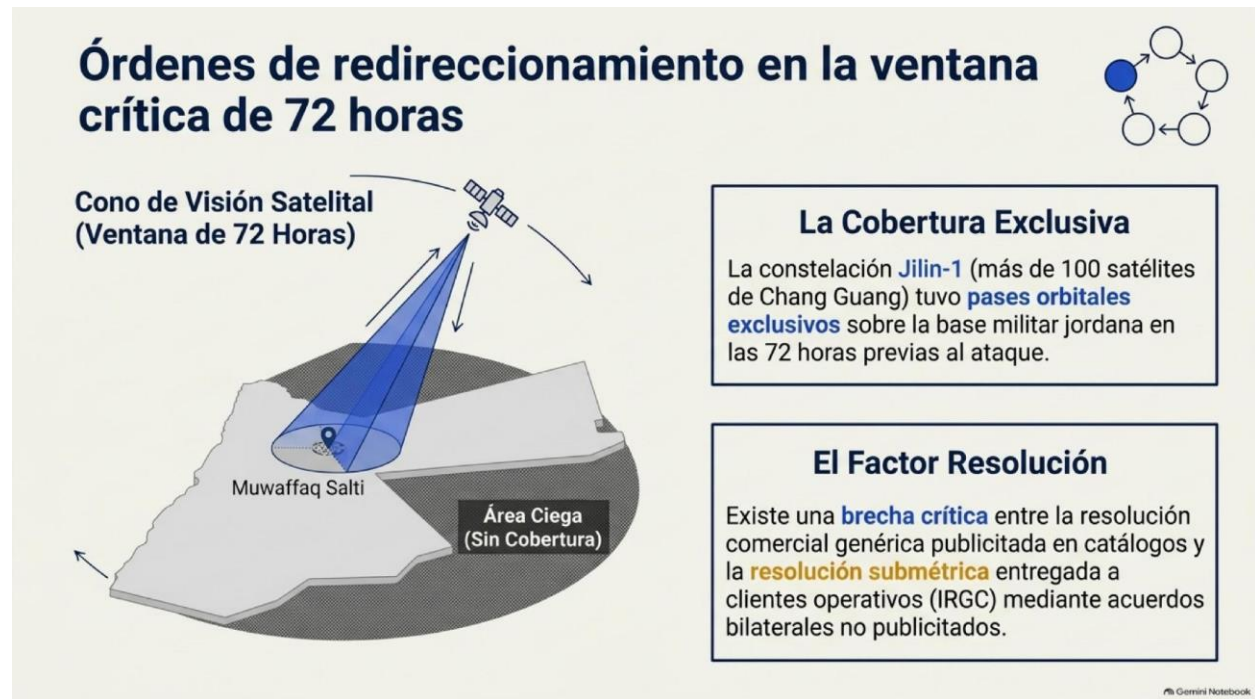


Figura 7. Órdenes de redireccionamiento orbital en la ventana crítica de setenta y dos horas previas al ataque.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

Los satélites comerciales de observación submétrica no fotografían la totalidad de la superficie terrestre de manera continua; operan bajo demanda, mediante órdenes de tasking que reorientan sensores ópticos o maniobran la plataforma hacia coordenadas específicas. El segundo eslabón probatorio consiste en demostrar que existió una orden de redireccionamiento prioritaria sobre las coordenadas de Muwaffaq Salti en la ventana de setenta y dos horas previas al ataque del 17 de julio, y que ese redireccionamiento no puede explicarse por un patrón comercial rutinario. Complementariamente, la exclusividad del pase orbital —es decir, que ninguna otra constelación aliada u comercial abierta sobrevoló el área con el ángulo y la resolución necesarios durante la ventana crítica— reforzaría la inferencia de que el vector de inteligencia geoespacial fue, en efecto, chino.

El análisis de Defence Security Asia (2026b) sobre lo que denominó la "mancha oscura" en las imágenes satelitales de Muwaffaq Salti ilustra la relevancia práctica de este eslabón: la reconstrucción del daño estructural mediante tasking de mayor resolución posterior al ataque —contrastando el registro del daño confirmado a hangares, refugios de aeronaves y alojamientos con las imágenes disponibles antes del impacto— permite, en principio, extrapolar hacia atrás qué constelaciones tuvieron línea de visión directa sobre el objetivo en las horas previas. La existencia de más de un centenar de satélites en la constelación Jilin-1 (Defence Security Asia, 2026a; China in Space, 2026a) aumenta sustancialmente la probabilidad estadística de cobertura persistente sobre cualquier instalación de interés estratégico en el Levante, lo que a su vez facilita —aunque no garantiza— la reconstrucción retrospectiva de las órdenes de misión.

Un elemento adicional de este eslabón, con frecuencia subestimado en el debate público, es la diferencia entre la resolución nominal publicitada por el operador comercial y la resolución efectivamente entregada al cliente final. Los contratos comerciales de observación terrestre suelen ofrecer distintos niveles de resolución según el nivel de pago y la relación con el cliente, lo que significa que una misma constelación puede vender imágenes de calidad genérica al mercado abierto mientras entrega productos de resolución submétrica y con menor latencia a clientes privilegiados mediante acuerdos bilaterales no publicitados. La denuncia de que Irán habría mantenido acceso operativo continuo al satélite TEE-01B desde 2024 es congruente con este tipo de arreglo preferencial, distinto de una simple compra puntual en el mercado abierto de imágenes (China in Space, 2026b), y su verificación técnica —mediante la comparación de metadatos de resolución entre el catálogo comercial público de Chang Guang y los productos efectivamente recuperados de los restos de los vectores de ataque— constituye un procedimiento de verificación forense relativamente accesible para agencias con capacidad técnica adecuada.

Fusión de fichas de blanco y metadatos de navegación (TECHINT)

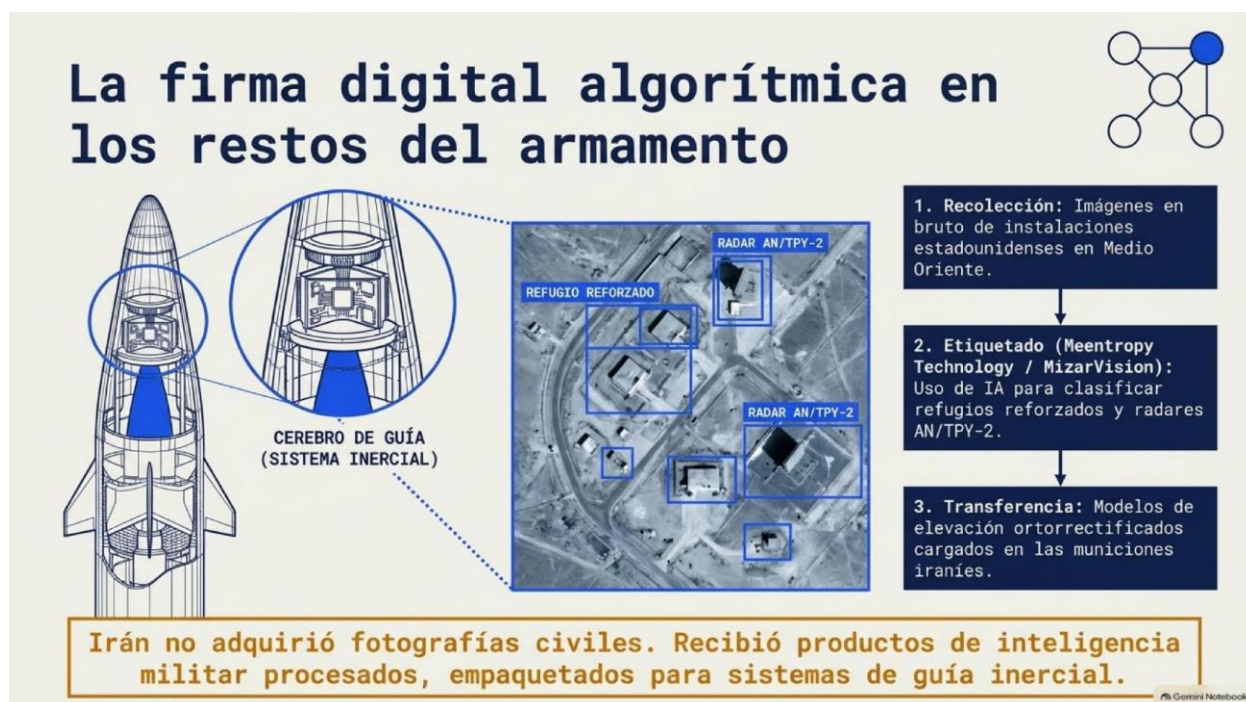


Figura 8. La firma digital algorítmica en los restos del armamento recuperado.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

El tercer eslabón se deriva del análisis forense de los restos de los vectores de ataque o de los sistemas de guía recuperados. Las armas de precisión guiadas por sistemas inerciales y de posicionamiento global requieren paquetes de datos de puntería que incluyen modelos digitales de elevación y matrices ortorrectificadas; la resolución, el formato y los metadatos propietarios de dichos modelos pueden, en principio, coincidir de manera única con los algoritmos de procesamiento de firmas satelitales chinas. El hecho de que Meentropy Technology, bajo su marca comercial MizarVision, haya sido señalada por el uso de algoritmos de aprendizaje automático entrenados sobre imágenes de origen comercial —incluyendo proveedores occidentales— para etiquetar automáticamente aeronaves, refugios reforzados, depósitos de combustible y sistemas de radar en el Medio Oriente, es directamente pertinente a este eslabón: un producto de inteligencia ya procesado y clasificado, y no una fotografía civil en bruto, es lo que dejaría una firma algorítmica identificable en el paquete de datos de puntería recuperado de los restos de un misil (Defence Security Asia, 2026c).

De manera análoga, si se demostrara que los ataques contra activos móviles o buques utilizaron vectores derivados de algoritmos chinos de detección automática de blancos —fusionando datos de identificación automática (AIS) con imágenes de radar de apertura sintética—

, ello evidenciaría la transferencia de un producto de inteligencia procesado, elevando sustancialmente el umbral de complicidad más allá de la mera venta de imágenes comerciales sin procesar.

Vínculo jurídico y corporativo con el Estado chino (OSINT/FININT)



Figura 9. El ecosistema corporativo como extensión del aparato de defensa: arquitectura de la fusión civil-militar.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

El cuarto eslabón es, argumentablemente, el más sólido y el mejor documentado hasta la fecha, porque no depende de inteligencia clasificada sino de arquitectura legal e institucional pública. Escalar la responsabilidad de una empresa nominalmente privada al gobierno de Beijing exige demostrar, primero, el marco normativo que obliga a la cooperación; segundo, la integración corporativa real de la empresa en el aparato de defensa; y tercero, la ruta financiera del beneficio obtenido.

En el plano normativo, el artículo 7 de la Ley de Inteligencia Nacional de la República Popular China, vigente desde 2017 y enmendada en 2018, establece que toda organización y ciudadano chino debe apoyar, asistir y cooperar con las labores de inteligencia nacional conforme a la ley, y mantener en secreto el trabajo de inteligencia nacional del que tenga conocimiento

(China Law Translate, 2018). Esta disposición ha sido objeto de un debate académico genuino: mientras analistas como Murray Scot Tanner sostienen que la ley transformó la obligación legal de los ciudadanos chinos de una postura "defensiva" a una de cooperación activa y potencialmente ofensiva, juristas como Gu Bin, de la Universidad de Estudios Extranjeros de Beijing, han argumentado en sentido contrario que el artículo 7 no autoriza el espionaje preventivo y que el trabajo de inteligencia nacional debe entenderse como fundamentalmente defensivo (Wikipedia, 2026a). Este ensayo no pretende zanjar esa controversia interpretativa; lo relevante para el expediente probatorio es que, exista o no una obligación de cooperación activa, el artículo 7 sí establece —de manera no controvertida— una obligación legal de confidencialidad que impediría a cualquier empresa china divulgar voluntariamente el uso que el Estado o sus intermediarios hacen de su infraestructura, lo que en la práctica blinda jurídicamente la opacidad operativa denunciada en el caso Chang Guang.

En el plano de la integración institucional, la doctrina de fusión civil-militar (Military-Civil Fusion, MCF) —elevada a estrategia nacional hacia 2014 y consolidada en 2017 con la creación del Comité Central de Desarrollo de la Fusión Militar-Civil, presidido directamente por Xi Jinping— constituye el marco estructural que explica por qué la distinción entre "empresa comercial" y "activo de defensa" resulta, en el caso chino, en gran medida nominal (Centro para una Nueva Seguridad Americana [CNAS], 2026; Oficina Nacional de Investigación Asiática [NBR], s.f.). El sector espacial ha sido identificado de manera reiterada como uno de los dominios emergentes prioritarios de la fusión civil-militar, en el cual empresas formalmente privadas desarrollan tecnologías de uso dual bajo la coordinación de comités provinciales y municipales de fusión civil-militar establecidos en casi todo el territorio chino (Instituto de Políticas de Seguridad y Desarrollo [ISDP], 2025). Chang Guang Satellite Technology encaja de manera casi paradigmática en este patrón: la empresa está incrustada institucionalmente en la Academia de Ciencias de China y respaldada por el gobierno provincial de Jilin, lo que la convierte, según análisis del Instituto Hudson, en una extensión del aparato de defensa chino antes que en una entidad comercial verdaderamente independiente (Kasapoglu, 2026). El caso del sistema de navegación satelital BeiDou —descrito por altos mandos militares chinos como un "modelo de fusión civil-militar" y como un hito para la construcción de la defensa nacional junto con el desarrollo económico y social— ofrece un precedente adicional de cómo Beijing articula

explícitamente sus activos espaciales de doble uso dentro de su propia doctrina militar (Fundación para la Defensa de las Democracias [FDD], 2021).

En el plano financiero, la ruta de pagos y el régimen de sanciones ofrecen la evidencia más verificable y ya parcialmente pública. La Oficina de Control de Activos Extranjeros del Tesoro estadounidense sancionó a Chang Guang Satellite Technology en 2023 por el suministro de imágenes al Grupo Wagner en la Ucrania ocupada, y posteriormente la vinculó, bajo distintos regímenes de sanciones —incluidos los relacionados con Irán y con la Orden Ejecutiva 14024 sobre Rusia—, a redes de intermediarios comerciales y militares (OFAC, 2026). Una investigación de la firma de inteligencia de riesgo Kharon documentó que, entre 2021 y 2025, al menos tres empresas de lanzamiento chinas —Galactic Energy, CAS Space y LandSpace— colocaron en órbita más de veinte satélites para operadores posteriormente sancionados por su vínculo con el esfuerzo bélico ruso, así como para clientes vinculados al aparato militar iraní, en lanzamientos realizados sistemáticamente desde el Centro de Lanzamiento de Satélites de Jiuquan, bajo control de facto del Ejército Popular de Liberación (Kharon, 2026). Ese mismo informe documentó que al menos tres de los cinco clientes recurrentes de dichas empresas de lanzamiento fueron posteriormente sancionados por su papel en el conflicto ruso-ucraniano, y que continuaron recibiendo servicios de lanzamiento tanto antes como después de sus respectivas designaciones (Kharon, 2026). Este patrón de reincidencia comercial —contratar y volver a contratar con clientes ya sancionados— constituye, en sí mismo, un indicio de que la relación comercial no responde a un desconocimiento genuino del uso final de los activos, sino a una tolerancia institucional consistente con el marco de fusión civil-militar descrito.

Vale la pena señalar, adicionalmente, que la propia arquitectura institucional de la fusión civil-militar china prevé mecanismos formales de coordinación que trascienden la simple disposición legal del artículo 7 de la Ley de Inteligencia Nacional. La creación en 2017 del Comité Central de Desarrollo de la Fusión Militar-Civil, presidido por Xi Jinping y compuesto por altos mandos tanto de la Comisión Militar Central como del aparato del Partido-Estado, tuvo el propósito explícito de superar las resistencias de las empresas estatales de defensa establecidas y de articular objetivos militares y de mercado dentro de un mismo instrumento de planificación (Oficina Nacional de Investigación Asiática [NBR], s.f.). Hoy, prácticamente todos los gobiernos provinciales y municipales chinos cuentan con comités locales de fusión civil-militar dirigidos por

funcionarios del Partido (NBR, s.f.), lo que significa que una empresa como Chang Guang, radicada en la provincia de Jilin y respaldada institucionalmente por su gobierno provincial, opera dentro de una cadena de coordinación política que existe independientemente de que cualquier orden específica de recolección de imágenes sobre Muwaffaq Salti pueda o no rastrearse documentalmente hasta Beijing.

Fuentes humanas e interceptaciones estratégicas (HUMINT/COMINT)

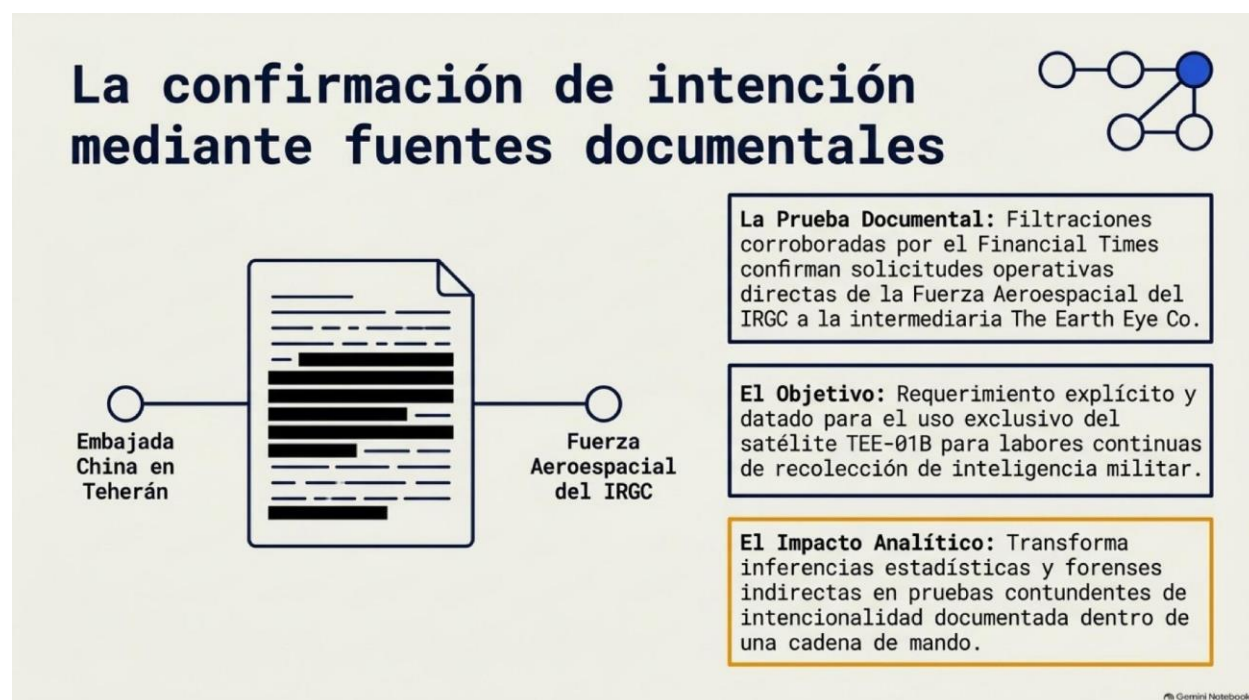


Figura 10. La confirmación de intención mediante fuentes documentales filtradas.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

El quinto y último eslabón —interceptaciones de comunicaciones de mando entre agregadurías militares chinas en Teherán y el IRGC, así como directivas internas filtradas del Ministerio de Comercio o de la Administración Espacial Nacional China que autoricen exenciones de control de exportación para telemetría sensible con destino a Irán— es, por su propia naturaleza, el más difícil de corroborar mediante fuentes abiertas. No obstante, la filtración de documentos de la Fuerza Aeroespacial del IRGC citada por el Financial Times, en la que se solicitaba explícitamente a The Earth Eye Co. el uso de su satélite TEE-01B para labores de recolección de imágenes, constituye un ejemplo concreto del tipo de evidencia documental que este eslabón busca sistematizar: no una inferencia técnica indirecta, sino una solicitud operativa directa y datada,

atribuible a una unidad militar identificada (China in Space, 2026b). La existencia de este único documento filtrado sugiere que, contrariamente a la percepción de opacidad total, el expediente HUMINT/COMINT no es inaccesible en principio, sino que su disponibilidad pública depende de filtraciones ocasionales y de la voluntad de las agencias de inteligencia de desclasificar interceptaciones cuyo valor de fuente probablemente sigue vigente.

Estudio de caso comparado: el patrón Chang Guang–Spacety, de Ucrania a Yemen y Jordania



Figura 11. Un patrón de política exterior estatal, no un error comercial aislado: Ucrania, Yemen y Jordania.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

La solidez del expediente contra Chang Guang Satellite Technology en el caso de Muwaffaq Salti no puede evaluarse de manera aislada: debe leerse como la tercera iteración documentada de un mismo patrón operativo, lo que fortalece sustancialmente la inferencia de intencionalidad frente a la hipótesis alternativa de negligencia comercial no intencionada. La primera iteración se remonta a comienzos de 2023, cuando Spacety Co. se convirtió en la primera empresa satelital comercial china sancionada por Estados Unidos, acusada de proporcionar imágenes sobre Ucrania que, según funcionarios estadounidenses, habrían habilitado operaciones de combate del Grupo Wagner (Kharon, 2026). Meses después, en 2023, Chang Guang fue

sancionada por el mismo tipo de conducta —suministro de imágenes en apoyo a operaciones militares rusas—, sanción a la que se sumó posteriormente la Unión Europea en junio de 2024 (Kharon, 2026).

La segunda iteración se produjo en 2024-2025, cuando, según el Instituto Hudson, Chang Guang habría proporcionado a los hutíes yemeníes —representantes del IRGC en la región— inteligencia de imágenes derivada de la constelación Jilin-1 para operar contra la navegación comercial y las fuerzas navales estadounidenses en el estrecho de Bab el-Mandeb, apoyo que según fuentes de inteligencia abierta habría continuado incluso después de que Washington planteara formalmente el problema ante Beijing (Kasapoglu, 2026). Es significativo que ese mismo período coincidiera con el primer ataque antibuque balístico exitoso de la historia militar, ejecutado por los hutíes en febrero de 2024, en el marco de un programa de misiles antibuque que la literatura especializada atribuye directamente al ecosistema de misiles del IRGC (Kasapoglu, 2026).

La tercera iteración es la que ocupa a este ensayo: el apoyo presunto de Chang Guang, The Earth Eye Co. y Meentropy Technology a la campaña de selección de blancos iraní contra fuerzas estadounidenses en Jordania e Irak durante 2026, formalizada en las designaciones del Departamento de Estado de mayo de ese año (OFAC, 2026). La consecuencia comercial de esta reincidencia ha sido tangible: Chang Guang retiró su solicitud de oferta pública inicial en diciembre de 2024, citando en medios locales tanto las sanciones estadounidenses como pérdidas financieras acumuladas (Kharon, 2026), lo que sugiere que el patrón de apoyo a actores sancionados no ha sido cost-free ni siquiera dentro del propio sistema chino, pero tampoco ha sido disuasivo al punto de interrumpir la conducta.

Leído en conjunto, este patrón de tres episodios —Ucrania, Yemen y Jordania— desplaza la carga argumentativa: la hipótesis de una venta comercial aislada, sin conocimiento del uso final, se vuelve estadísticamente menos plausible con cada repetición documentada del mismo comportamiento por parte de la misma empresa, incrustada institucionalmente en el mismo marco de fusión civil-militar y protegida por el mismo régimen jurídico de confidencialidad de inteligencia nacional.

Los límites de la denegabilidad plausible ante el derecho internacional

Anatomía del escudo de denegabilidad plausible

	Fachada Legal/Comercial (Beijing)	Realidad Operativa (Inteligencia)
Naturaleza de los Activos	Observación terrestre pacífica para cartografía y clima.	Fusión Civil-Militar (MCF) dirigida y orquestada por el Estado.
Responsabilidad del Cliente	Ventas legítimas en el mercado abierto a terceros independientes.	Suministro persistente y contratos recurrentes con actores bajo sanciones internacionales.
Mecanismo de Transparencia	Protección habitual de secretos comerciales estándar de la industria.	Blindaje legal e impedimento de auditorías mediante el Artículo 7 de la Ley de Inteligencia.

Gemini Notebook

Figura 12. Anatomía del escudo de denegabilidad plausible.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

Pese a la convergencia de evidencia descrita, es indispensable reconocer los límites reales que enfrenta cualquier intento de traducir este expediente en una acusación formal ante el Consejo de Seguridad de las Naciones Unidas o en una justificación de represalia bajo el derecho internacional. En primer lugar, China cuenta con capacidad de veto en el Consejo de Seguridad, lo que convierte cualquier resolución formal en una imposibilidad práctica independientemente de la solidez probatoria; el foro relevante, en consecuencia, tiende a desplazarse hacia mecanismos unilaterales o plurilaterales de sanción —como los ya aplicados por el Tesoro estadounidense y la Unión Europea— antes que hacia una condena multilateral vinculante (OFAC, 2026).

En segundo lugar, la propia arquitectura de la Ley de Inteligencia Nacional china, al obligar a la confidencialidad sin necesariamente exigir cooperación activa según la lectura más restrictiva del artículo 7, permite a Beijing sostener con cierta consistencia jurídica interna la posición de que sus empresas operan de manera comercial y que cualquier uso militar del producto por parte de terceros escapa a su control directo (Wikipedia, 2026a). Esta ambigüedad interpretativa —documentada incluso en el propio debate académico occidental sobre el alcance de la norma— es, en sí misma, funcional a la estrategia de denegabilidad plausible: Beijing no necesita que la

interpretación defensiva sea la correcta, sino simplemente que exista suficiente incertidumbre jurídica genuina como para impedir un consenso internacional sobre su responsabilidad directa.

En tercer lugar, el estándar de enforcement de las sanciones ya impuestas ha demostrado ser limitado en la práctica, precisamente por la naturaleza distribuida y globalizada del mercado de observación terrestre: como han señalado analistas especializados, la naturaleza comercial de la industria de imágenes satelitales y la distribución internacional de los datos de observación terrestre dificultan sustancialmente la aplicación efectiva de sanciones dirigidas a empresas individuales, incluso cuando estas ya han sido formalmente designadas (Defence Security Asia, 2026a). Ello sugiere que, incluso en el escenario más favorable de atribución probatoria completa, el problema de la disuasión efectiva frente a Beijing permanece parcialmente sin resolver.



Figura 13. Los límites estructurales del derecho internacional y del régimen de sanciones.
Nota. Elaboración propia a partir de las fuentes citadas en el texto.

Discusión: implicaciones para la gobernanza espacial y la seguridad hemisférica

El precedente doctrinal: Implicaciones directas para América Latina

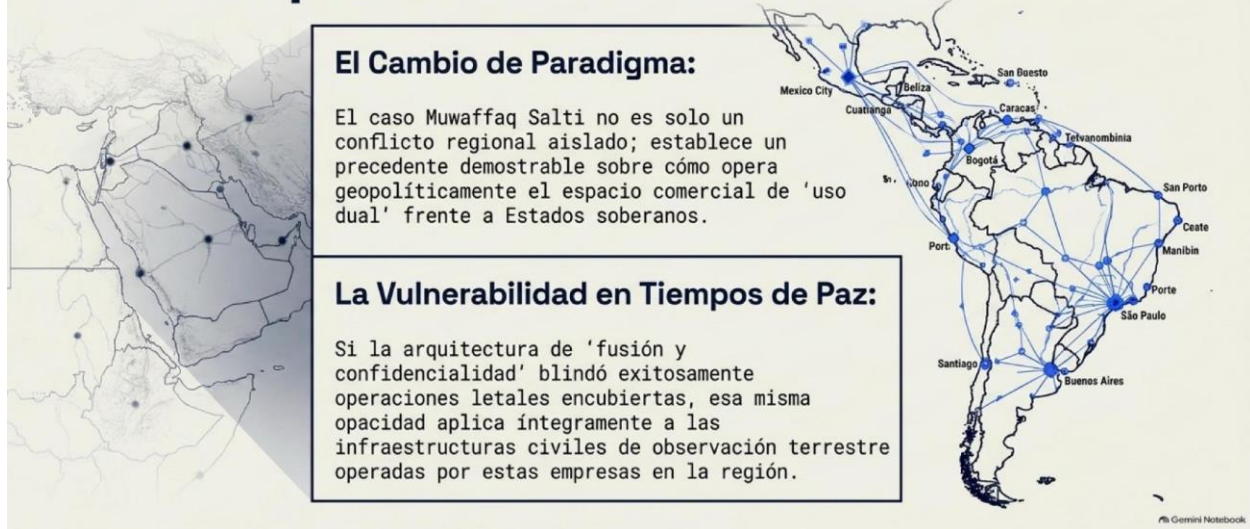


Figura 14. El precedente doctrinal: implicaciones directas para América Latina.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

El caso Muwaffaq Salti no es relevante únicamente para la relación triangular entre Washington, Teherán y Beijing; constituye también un precedente doctrinal con implicaciones directas para regiones que, como América Latina, dependen crecientemente de infraestructura espacial y de observación terrestre de origen chino en programas de seguridad ciudadana, gestión de desastres y vigilancia fronteriza. Si la arquitectura de fusión civil-militar y confidencialidad de inteligencia nacional que blindó a Chang Guang Satellite Technology durante casi tres años de apoyo documentado a actores sancionados es replicable en cualquier contrato de observación terrestre suscrito por un Estado latinoamericano con un proveedor chino, entonces la pregunta relevante para los gobiernos de la región deja de ser exclusivamente comercial —el costo y la resolución de las imágenes— y pasa a ser una pregunta de soberanía sobre el propio flujo de datos generado por esa infraestructura.

Esta dimensión conecta directamente con la literatura sobre dependencia tecnológica y extractivismo de datos en la región: la misma opacidad jurídico-corporativa que impide una atribución rápida y verificable en el caso de un ataque militar en Jordania es, estructuralmente, la misma opacidad que dificulta auditar de manera independiente qué ocurre con los flujos de datos generados por sistemas de videovigilancia, observación satelital o gestión de emergencias

operados con tecnología china en países de la región. El expediente probatorio de cinco eslabones propuesto en este ensayo, diseñado originalmente para un escenario de conflicto armado interestatal, ofrece por extensión un marco metodológico transferible para que analistas y autoridades regulatorias latinoamericanas evalúen, de manera más rigurosa, el nivel real de soberanía tecnológica que conservan sus propios acuerdos de cooperación espacial y de observación terrestre con proveedores chinos, en lugar de asumir a priori tanto la inocuidad comercial como la complicidad automática de dichos proveedores.

Adicionalmente, el caso ilustra una asimetría estructural entre la velocidad de la innovación comercial espacial china y la velocidad de las capacidades regulatorias y de contrainteligencia disponibles en la mayoría de los países receptores de esta tecnología, incluidos los de América Latina. Mientras que constelaciones como Jilin-1 han superado el centenar de satélites operativos con ciclos de revisita cada vez más cortos (Defence Security Asia, 2026a), la capacidad institucional de los organismos reguladores latinoamericanos para auditar contratos de observación terrestre, exigir cláusulas de trazabilidad de datos o establecer requisitos de procesamiento local de la información recolectada permanece, en la mayoría de los casos, incipiente. Esta brecha no es meramente técnica: es la misma brecha de gobernanza que, en el plano internacional, ha permitido que Chang Guang opere durante casi tres años bajo sanciones sucesivas sin que ello haya bastado para interrumpir su patrón de conducta documentado.

Extractivismo de datos y la ilusión del abaratamiento tecnológico

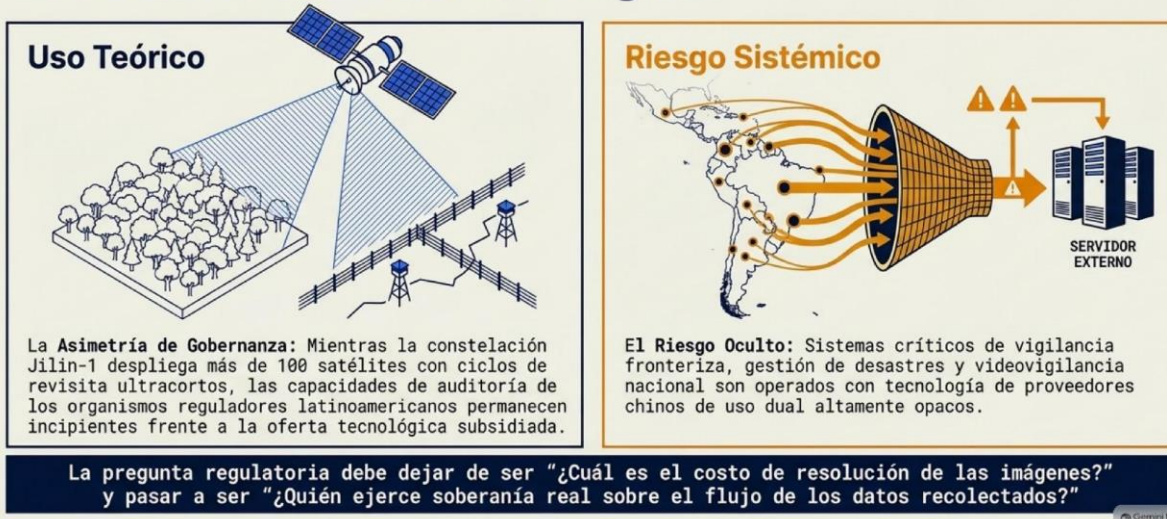


Figura 15. Extractivismo de datos y la ilusión del abaratamiento tecnológico.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

Conclusiones

Agenda estratégica: Elevando el costo del secretismo



1. Metodologías Forenses Abiertas

Desarrollar estándares OSINT internacionales para auditar y comparar las resoluciones comerciales publicitadas versus las verdaderas capacidades operativas entregadas (GEOINT civil).



2. Vigilancia Comercial Predictiva

Crear bases de datos longitudinales sobre los clientes de lanzadores comerciales chinos para detectar patrones de reincidencia antes de que faciliten un conflicto activo.



3. Defensa Regulatoria (Sur Global)

Redactar marcos contractuales modelo que exijan auditorías estrictas de trazabilidad de datos y garanticen el procesamiento local de información frente a todo proveedor de uso dual.

La denegabilidad plausible no se destruye con un solo dato aislado, sino desmantelando incrementalmente su viabilidad estructural.

Figura 16. Agenda estratégica: elevando el costo del secretismo.

Nota. Elaboración propia a partir de las fuentes citadas en el texto.

Este ensayo sostuvo que demostrar la complicidad material china en el ataque iraní a la Base Muwaffaq Salti exige un expediente de inteligencia de todas las fuentes que integre cinco eslabones probatorios independientes: el rastro forense digital y de telemetría, la trazabilidad de las órdenes de tasking orbital, la fusión de metadatos de los sistemas de guía recuperados, el vínculo jurídico-corporativo con el Estado chino, y las fuentes humanas e interceptaciones estratégicas. El análisis de la evidencia disponible en fuentes abiertas sugiere que, si bien ningún eslabón individual alcanza por sí solo el umbral de certeza necesario para una acusación formal ante el Consejo de Seguridad, la convergencia de al menos tres de los cinco eslabones —el vínculo jurídico-corporativo, la ruta financiera y sancionatoria, y el patrón repetido de conducta documentado entre 2023 y 2026— configura un caso circunstancial sustancialmente más sólido que el de una simple coincidencia comercial.

El precedente de Chang Guang Satellite Technology, sancionada de manera sucesiva por su apoyo al Grupo Wagner en Ucrania, a los hutíes en el mar Rojo y presuntamente a la campaña iraní de selección de blancos en Jordania, ilustra con particular claridad cómo la doctrina china de fusión civil-militar y el marco jurídico de la Ley de Inteligencia Nacional operan conjuntamente para producir una arquitectura de denegabilidad plausible que resulta difícil de desmontar mediante evidencia de una sola disciplina, pero que se erosiona de manera apreciable ante la repetición sistemática del mismo patrón de conducta. En última instancia, el problema que plantea este caso trasciende la atribución de un ataque específico: revela cómo el sector espacial comercial de uso dual se ha convertido en un instrumento de proyección de poder estatal que opera deliberadamente en los intersticios del derecho internacional, y cuya regulación efectiva —tanto para foros de seguridad internacional como para gobiernos que dependen de esa misma infraestructura en tiempos de paz— constituye uno de los desafíos regulatorios más urgentes y menos resueltos de la actual competencia geopolítica en el dominio espacial.

Como agenda de investigación futura, este ensayo sugiere tres líneas complementarias que excederían el alcance de un análisis basado exclusivamente en fuentes abiertas. La primera es el desarrollo de metodologías forenses estandarizadas para comparar metadatos de resolución y formato entre catálogos comerciales publicitados y productos de inteligencia recuperados de restos de armamento, de manera que el tercer eslabón —hoy dependiente casi por completo de

capacidades clasificadas— pueda volverse parcialmente verificable mediante análisis técnico abierto. La segunda es la construcción de bases de datos longitudinales sobre clientes recurrentes de lanzadores comerciales chinos, en la línea de lo iniciado por Kharon (2026), que permitan identificar patrones de reincidencia antes de que una empresa alcance el nivel de visibilidad pública que motivó las sanciones contra Chang Guang. La tercera, de particular relevancia para la región latinoamericana, es la elaboración de marcos contractuales modelo que incorporen explícitamente cláusulas de auditoría de trazabilidad de datos y de responsabilidad corporativa ante terceros, aplicables a los acuerdos de cooperación espacial y de observación terrestre que los Estados de la región suscriben cada vez con mayor frecuencia con proveedores chinos. Ninguna de estas tres líneas resuelve por sí sola el problema estructural de la denegabilidad plausible, pero cada una reduce, de manera incremental, el costo de vigilancia que Beijing puede externalizar hacia sus socios comerciales y hacia los Estados que dependen de su infraestructura espacial.

Referencias

- Centro para una Nueva Seguridad Americana. (2026). Myths and realities of China's military-civil fusion strategy. <https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy>
- China Law Translate. (2018). National Intelligence Law of the People's Republic of China (as amended in 2018). <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>
- China in Space. (2026a, 12 de mayo). U.S. sanctions three Chinese space firms over alleged Iran ties. <https://www.china-in-space.com/p/us-sanctions-three-chinese-space>
- China in Space. (2026b, 20 de abril). Iran allegedly using Chinese satellite images, surprising U.S. Space Force. <https://www.china-in-space.com/p/iran-allegedly-using-chinese-satellite>
- Defence Security Asia. (2026a, 11 de marzo). China's Jilin-1 spy satellite network is watching the U.S.–Iran war in real time. <https://defencesecurityasia.com/en/china-jilin1-satellites-monitor-us-iran-war-pla-intelligence-surveillance/>
- Defence Security Asia. (2026b, agosto). Dark patch over Muwaffaq Salti: Satellite imagery reignites the US–Iran battle-damage war over Jordan. <https://defencesecurityasia.com/en/muwaffaq-salti-satellite-dark-patch-iran-missile-strike-jordan-hormuz/>
- Defence Security Asia. (2026c, 19 de julio). Iran's missiles are learning: How China's satellites and Russia's intelligence are defeating US air defenses in the Middle East. <https://defencesecurityasia.com/en/iran-china-russia-satellite-intelligence-defeats-us-patriot-thaad-missile-defense-2026/>
- Fundación para la Defensa de las Democracias. (2021, 26 de mayo). Defusing military-civil fusion. <https://www.fdd.org/analysis/2021/05/26/defusing-military-civil-fusion/>
- Instituto de Políticas de Seguridad y Desarrollo. (2025). China's military-civil fusion in space: Strategic transformations and implications for Europe. <https://www.isdp.eu/wp->

content/uploads/2025/07/files_chinas-military-civil-fusion-in-space-strategic-transformations-and-implications-for-europe.pdf

Kasapoglu, C. (2026, 30 de mayo). The war above the war: How Chinese satellites support Iran. Hudson Institute. <https://www.hudson.org/national-security-defense/war-above-war-how-chinese-satellites-support-iran-mena-defense-can-kasapoglu>

Kharon. (2026, 4 de junio). China's space mercenaries: How the commercial rocket economy is arming Iran and Russia. <https://www.kharon.com/brief/china-space-military-intelligence-iran-russia-rocket-satellite>

Migflug. (2026, 20 de julio). What happened at Muwaffaq Salti. <https://migflug.com/jetflights/muwaffaq-salti-air-base-iran-attack-us-service-members-2026/>

Oficina Nacional de Investigación Asiática. (s.f.). Commercialized militarization: China's military-civil fusion strategy. <https://www.nbr.org/publication/commercialized-militarization-chinas-military-civil-fusion-strategy/>

Oficina de Control de Activos Extranjeros. (2026, 8 de mayo). Non-proliferation and Iran-related designations and designations updates. Departamento del Tesoro de Estados Unidos. https://ofac.treasury.gov/recent-actions/20260508_33

Radio Free Europe/Radio Liberty. (2026, 19 de julio). 2 US service members killed, 1 missing in Jordan as Iran steps up attacks, threats. <https://www.rferl.org/a/centcom-soldiers-killed-jordan-iran-missile-attack/33806519.html>

Task & Purpose. (2026, 22 de julio). These are the 3 soldiers killed by Iran's attack on a base in Jordan. <https://taskandpurpose.com/news/jordan-iran-feehan-gonzales-rampersad/>

The Aviationist. (2026, 18 de julio). Two U.S. service members killed, one missing in Iranian attack on Jordanian base. <https://theaviationist.com/2026/07/18/iranian-attack-muwaffaq-salti/>

Wikipedia. (2026a, 2 de mayo). National Intelligence Law of the People's Republic of China. https://en.wikipedia.org/wiki/National_Intelligence_Law_of_the_People%27s_Republic_of_China

Wikipedia. (2026b, 23 de enero). Military-civil fusion. https://en.wikipedia.org/wiki/Military-civil_fusion