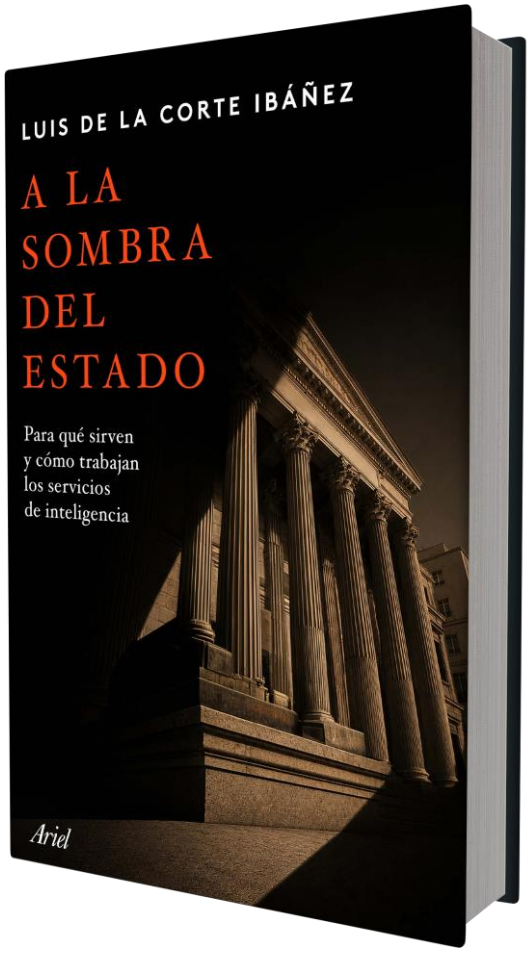
Ariel

LUIS DE LA CORTE IBÁÑEZ

A LA SOMBRA DEL ESTADO

PARA QUÉ SIRVEN Y CÓMO TRABAJAN LOS SERVICIOS DE INTELIGENCIA



Espionaje, operaciones encubiertas, guerra híbrida, desinformación y poder clandestino... una narración tensa y rigurosa para conocer cómo funcionan los servicios de inteligencia desde dentro

18 DE NOVIEMBRE A LA VENTA

AUTOR DISPONIBLE PARA ENTREVISTAS

PARA AMPLIAR INFORMACIÓN

Erica Aspas I RESPONSABLE DE COMUNICACIÓN ÁREA DE ENSAYO
689 77 19 80 I easpas@planeta.es

SINOPSIS

Sabemos que detrás de la política internacional se disputan conflictos invisibles. Pero ¿cómo funcionan realmente los servicios de inteligencia?

Luis de la Corte nos deja entrever el mundo secreto en el que los servicios de inteligencia tejen sus hilos a través de casos reales, operaciones legendarias, guerras encubiertas y errores históricos, para revelar cómo los Estados buscan reducir la incertidumbre y anticipar amenazas. *A la sombra del Estado* ofrece una visión sofisticada, humana y profundamente realista de cómo trabajan estas organizaciones, combinando historia, geopolítica y espionaje con episodios reales.

Rigor académico, tensión de *thriller* y enorme capacidad divulgativa se unen en este libro de referencia sobre servicios de inteligencia.

EL AUTOR



LUIS DE LA CORTE IBÁÑEZ

(@LuisdelaCorteIb) es profesor de Psicología social y pertenece al Consejo de Dirección del Instituto de Ciencias Forenses y de la Seguridad de la Universidad Autónoma de Madrid. Entre sus publicaciones destacan *La lógica del terrorismo* y *La yihad terrorista* (con Javier Jordán). Ha visitado diversos centros académicos extranjeros como el Centro para el Estudio del Terrorismo y la Violencia Política de la Universidad de St. Andrews (Reino Unido) y en España ha colaborado con el Centro Superior de Estudios de la Defensa Nacional, el Instituto Español de Estudios Estratégicos, la Guardia Civil, el Cuerpo Nacional de Policía, la Escuela Diplomática, el Real Instituto Elcano de Estudios Estratégicos e Internacionales y la Cátedra de Servicios de Inteligencia y Sistemas Democráticos de la Universidad Rey Juan Carlos.

ALGUNOS EXTRACTOS

«En este libro he procurado ofrecer una visión amplia y fidedigna de los servicios de inteligencia. Para ello he intentado reconstruir la génesis y evolución de esas organizaciones. De paso, también he suministrado diversas pruebas de su influencia en la historia reciente de las relaciones internacionales y las políticas de seguridad. Y, ante todo, me he ocupado de describir y explicar sus funciones, actividades y métodos».

¿Qué son y qué hacen los servicios de inteligencia?

«Los servicios de inteligencia, también conocidos como agencias de inteligencia, son organizaciones estatales que trabajan en secreto para **suministrar inteligencia al Gobierno de su país o a sus autoridades militares o mandos policiales**. Introducir a los mandos policiales en la definición es controvertido y muchos profesionales lo considerarán incorrecto. La razón es que en nuestro país los organismos o departamentos que proveen de inteligencia a los cuerpos policiales reciben la denominación alternativa de *servicios de información»*.

«La función principal de cualquier servicio de inteligencia que merezca tal nombre es **proporcionar conocimientos útiles**. Aunque no conocimientos sobre cualquier tema o cuestión, sino únicamente sobre aquellos asuntos o temas que afecten directamente a la seguridad y los intereses vitales o estratégicos de la propia nación y/o a la conducción de la guerra. A tales conocimientos específicos llaman los servicios "inteligencia".».

«La forma habitual de obtener informaciones confidenciales de manera secreta es una actividad a la que los *sapiens* han recurrido desde siempre: **el espionaje**».

«Algunos expertos en el tema opinan que los únicos servicios de inteligencia que merecen la denominación de servicios secretos son aquellos cuya existencia es ella misma secreta. **Las autoridades del Reino Unido tardaron más de medio siglo en admitir la existencia de los dos servicios de inteligencia británicos más conocidos**. Aunque ambos fueron creados en la década de 1920, Londres solo reconoció pública y legalmente al MI5, su servicio de seguridad e inteligencia interior, en 1989, y no hizo lo propio con el MI6, su servicio de inteligencia exterior, hasta 1994».

¿Qué mueve a los espías?

«Stanislav Levchenko ingresó en el KGB en 1971 […]. Tras vivir algunos años en Estados Unidos, oculto y bajo protección del FBI, Levchenko empezó a colaborar con la CIA, a la que ayudó a desmantelar varias redes de agentes que los soviéticos habían establecido en Asia […]. En 1988 publicó sus memorias donde explicó por qué desertó de la URSS. En ese mismo libro, además, introdujo la primera referencia pública al acrónimo **MICE**, expresión inventada por los servicios estadounidenses durante la Guerra Fría para referirse a las cuatro técnicas principales empleadas para reclutar agentes y recabar información de fuentes humanas. A saber: **ofrecer**

dinero (M), apelar a razones o ideales políticos (I), coaccionar (C) y adular o masajear el ego (E)».

«Inteligente, atractiva e inquieta, [la neoyorquina] **Aline Griffith** contaba veintiún años y estaba a punto de terminar sus estudios universitarios cuando Japón atacó a Estados Unidos en Pearl Harbor, en diciembre de 1941. De inmediato, quiso emular a sus hermanos y alistarse para combatir en la guerra, pero su país todavía no admitía mujeres en el Ejército […]. En septiembre de 1943, Aline aceptó una propuesta para participar en una misión secreta en Europa. Después de un breve periodo de adiestramiento, a principios de 1944 fue enviada a España […].

El trabajo de Aline fue realmente productivo: entre 1944 y 1945 organizó toda una red de agentes principalmente reclutados entre antiguos partidarios del bando republicano durante la Guerra Civil, únicos candidatos fiables a trabajar como espías para los aliados, según el criterio fijado por la OSS, dado que el régimen de Franco mantenía buenas relaciones con la Alemania nazi […]. Su mayor contribución fue destapar una red de financiación nazi que permaneció activa hasta 1944 en la que participaron el príncipe Max von Hohenlohe, al que Aline conoció al hacerse íntima amiga de María Francisca von Hohenlohe, hija mayor del propio príncipe».

«**Mikel Lejarza, alias Lobo**, es el más conocido de todos los agentes infiltrados en ETA […]. Gracias al cúmulo de informaciones obtenidas por Lobo, el 18 de septiembre de 1975 la policía realizó varias redadas en Barcelona, Madrid, el País Vasco y Galicia que se saldaron con más de 150 detenidos, la incautación de abundante material y la destrucción temporal de toda la infraestructura de ETA-pm. Tras aquel golpe, los *polimilis* llenaron las calles del País Vasco de panfletos con la foto y el nombre de Mikel Lejarza y lo condenaron a muerte. El SECED le **aconsejó que pasara por el quirófano para cambiar los rasgos de su rostro y le proporcionó una nueva identidad** provisional. Lejarza recibió una compensación económica inferior a la que le habían prometido y se sintió abandonado, pero se mantuvo leal y continuó colaborando en otras operaciones de espionaje».

Intrusiones, cámaras y micrófonos

«Los primeros **duplicadores digitales portátiles** aparecieron a finales de los años noventa. Aunque permitían clonar discos duros completos en pocos minutos, su tamaño y diseño limitaban sus posibilidades operativas, que quedaban circunscritas a registros policiales e inspecciones forenses. A principios del siglo XXI surgieron dispositivos verdaderamente manejables para su uso por agentes de campo: fundamentalmente, **memorias USB con utilidades de extracción en vivo y programas de captura rápida de datos**. A partir de 2010 se empezó a trabajar con programas que, sin necesidad de clonar discos completos, podían sustraer en pocos minutos todos los datos volátiles de un equipo informático (claves de sesión, contraseñas activas y otros fragmentos de comunicaciones que se pierden al apagar los aparatos), junto con la información inmediata más valiosa. Aparecieron también las **plataformas de extracción de datos de teléfonos inteligentes**, dotadas de sistemas capaces de crear copias completas o copias lógicas que incluyesen toda la información visible de un teléfono».

«En marzo de 2017, el portal de internet **WikiLeaks**, especializado en difundir materiales secretos, publicó una serie de documentos bajo el nombre de Vault 7 que correspondían a varios miles de archivos donde se describía el desarrollo de un extenso muestrario de ingenios informáticos por parte de la CIA. Tales archivos contenían desde programas para infiltrarse en teléfonos y televisores hasta herramientas de extracción de información para su empleo en

situaciones operativas. Entre estas últimas figuraría el **software Dumbo, preparado para ser cargado en cualquier ordenador** mediante un pequeño dispositivo USB y capaz de detectar cámaras y micrófonos conectados, interrumpir grabaciones en curso y manipular memorias extraíbles».

Innovaciones técnicas

«Las innovaciones más recientes [en drones] han sido la **incorporación de sistemas de inteligencia artificial** que procesan datos durante el vuelo con mínima intervención humana y su empleo con propósitos ofensivos, del que hablaremos a continuación. En el futuro, los drones trabajarán en grupos formados por muchos aparatos pequeños coordinados a modo de enjambres y en cooperación con aeronaves con piloto […]

El conflicto armado donde se ha sacado un mayor partido al uso de los drones ha sido la guerra de Ucrania […]. Empleados en labores de reconocimiento y vigilancia (identificando trincheras, posiciones de tropas, corredores logísticos), para guiar la artillería y para lanzarlos contra objetivos a la manera de "drones suicidas". Su mayor utilidad, no obstante, ha sido la aportación de inteligencia. La información captada ha sido explotada por los ejércitos regulares, las brigadas de artillería y las tropas de defensa territorial».

«La inteligencia de medición y firmas (MASINT) suministra **información sobre fenómenos físicos como vibraciones, sonidos, calor, radiación o reflejos de la luz que no generan emisiones electromagnéticas** ni ningún rastro visible, pero que pueden captarse a través de dos procedimientos. El primero ("medición") consiste en registrar y traducir a datos cuantificables la huella física que un objeto o una actividad deja en el mundo material. Puede tratarse de las ondas sísmicas provocadas por una explosión subterránea, el calor residual o la radiación emitidos por un reactor en marcha o el rumor mecánico de un submarino en movimiento. El segundo procedimiento consiste en comparar cada medición con otras anteriores para obtener una "firma" que permita reconocer el objeto o la actividad registrados […].

La inteligencia de señales y firmas ha servido para **vigilar pruebas atómicas**, distinguir entre explosiones convencionales y nucleares, controlar el cumplimiento de tratados de desarme, vigilar submarinos y seguir su actividad en zonas sensibles, detectar la actividad de reactores nucleares e instalaciones vinculadas a programas de armamento que trataban de pasar inadvertidas, y **localizar artefactos enterrados** como minas, explosivos o depósitos ocultos».

Web, Deep Web, Dark Web

«Internet es como abrir una o varias ventanas o puertas de una casa ubicada en **un barrio lleno de vecinos curiosos y ladrones**».

«El nivel básico de exploración [de internet] se realiza en la capa más superficial y visible de la WWW, constituida por páginas públicas indexadas por grandes motores de búsqueda (Google, Bing, DuckDuckGo, etc.), pero las exploraciones también se extienden a la **Deep Web** o internet profunda, a la que no llegan los buscadores públicos y que **contiene cerca del 90 por ciento de la información en línea**, hasta alcanzar la zona más opaca del ciberespacio, conocida como internet oscura o **Dark Web**, únicamente accesible mediante programas que garanticen el anonimato de los usuarios (Tor, I2P, Tails). En ese nivel, la recolección digital ya es

ciberespionaje, ya que **se busca información escondida en espacios virtuales** como foros cerrados de grupos extremistas, puntos de compraventa ilegal de armas, drogas, programas maliciosos o identidades falsas, repositorios que almacenan datos robados o canales de comunicación empleados por redes criminales y actores estatales. Las investigaciones realizadas en esta última capa, a menudo mediante *software* especializado (*crawlers*, *scrapers*, herramientas de análisis *blockchain*), pueden aportar información sobre operaciones financieras opacas, rutas logísticas sospechosas, contratos y adquisiciones de material estratégico, intercambios de tecnología o datos sensibles, campañas de propaganda, planes de atentados y otras acciones hostiles».

«En 2007, la NSA desplegó **Upstream**, un programa de interceptación de comunicaciones internacionales encuadrado en la iniciativa Rampart-A, un proyecto más amplio para explotar el flujo de datos vinculado a las redes mundiales de comunicación que contaría **con el respaldo de servicios británicos, alemanes, suecos y daneses y de varias compañías internacionales de telecomunicaciones.** Mientras otras partes de ese macroproyecto se centraron en acceder a datos almacenados en servidores privados, Upstream intervendría cables terrestres y submarinos, grandes enrutadores y equipos de canalización del tráfico de señales que unen las principales redes transnacionales de fibra óptica».

«En 2013, la filtración pública de los documentos robados a la NSA por el contratista **Edward Snowden** sacó a la luz la existencia de Eikonal, Upstream y Tempora, descubriéndose también que los sistemas de filtrado de datos utilizados por esos programas no siempre distinguían entre comunicaciones procedentes del extranjero y otras provenientes de los países responsables de los proyectos. La consiguiente tormenta política reavivó el debate abierto en la década anterior a raíz de la red ECHELON. En palabras de un comentarista británico, aquellas revelaciones demostraron que **internet se había convertido en "la mejor máquina de vigilancia del mundo**"».

Pegasus

«Creado y comercializado por NSO Group, una empresa tecnológica fundada en 2010 por dos antiguos miembros de la Unidad 8200, principal unidad de inteligencia de señales de Israel, y un tercer socio que sirvió en el Mossad, el *spyware* **Pegasus es un "troyano de vigilancia"** capaz de tomar el control de cualquier teléfono inteligente y convertirlo en una fuente permanente de información […] y **solo puede ser comprado por organismos estatales, previa autorización del Ministerio de Defensa israelí**».

«Diversas noticias supuestamente basadas en "fuentes de la inteligencia española" señalaron que **los servicios de inteligencia marroquíes llevaban tiempo usando Pegasus**, advirtiendo asimismo que las infecciones de los teléfonos del Gobierno coincidieron con la crisis diplomática con Marruecos de abril-mayo de 2021. El juez instructor consideró plausible la hipótesis de una operación de espionaje marroquí y **solicitó varias comisiones rogatorias a Israel** para obtener información de la empresa propietaria de Pegasus, si bien la falta de respuestas llevó a archivar provisionalmente el caso en julio de 2023. Se reabrió algunos meses después, al recibirse nuevos indicios técnicos remitidos por Francia, pero el juez terminó admitiendo que, **sin cooperación internacional ni pruebas rastreables, la autoría del espionaje no podría esclarecerse**».

Por qué el CESID se convirtió en CNI

«El CESID no aparece mencionado en la Constitución aprobada en 1978, pese a que así lo habían solicitado sus directores, de modo que la normativa que regularía sus actividades se concretó en una colección de reglamentos (reales decretos y órdenes ministeriales). Esta circunstancia no fue completamente anómala (en Europa solo las constituciones alemana y austriaca mencionan expresamente a sus servicios de inteligencia) […]. Lo que sí sería una anomalía es que **su propia normativa reguladora no reconociera al CESID la posibilidad de solicitar y obtener autorización judicial para interceptar llamadas telefónicas o practicar registros domiciliarios**, como sí podían hacer el Cuerpo Nacional de Policía, la Guardia Civil y los órganos de información de las policías autonómicas.

Los problemas creados por una regulación tan poco sofisticada se hicieron evidentes a raíz de dos escándalos surgidos entre mediados y finales de la década de 1990. El primer escándalo saltó en junio de 1996, mes en que el diario *El Mundo* denunció que "el CESID lleva más de diez años **espiando y grabando a políticos, empresarios y periodistas**" […]. El segundo, en marzo de 1998, cuando **Herri Batasuna (HB),** partido político controlado por ETA, presentó una denuncia por espionaje después de que trabajadores de su sede en Vitoria descubrieran unos cables conectados a la centralita telefónica que subían al siguiente piso del edificio».

«Los problemas no se resolvieron hasta que **una nueva ley aprobada en 2002 decretó la sustitución del CESID por el Centro Nacional de Inteligencia**, dotando al nuevo servicio de una cobertura legal completa y de criterios claros sobre los controles de sus actividades por el Congreso y el Poder Judicial».

Sorpresas, fracasos y aciertos

«Los servicios de inteligencia no son infalibles. Por otro lado, **los juicios sobre su eficacia están claramente sesgados** por tres razones: el carácter secreto de la inteligencia suministrada, las expectativas exageradas sobre las opciones reales de anticipar eventos futuros y el hecho de que los fallos de inteligencia son más evidentes y conocidos que los aciertos».

"Un servicio de inteligencia puede cosechar fracasos en cualquiera de sus tres funciones típicas: **la inteligencia, la contrainteligencia y las acciones encubiertas**».

«La incapacidad alemana para parar a los aliados en Normandía fue consecuencia de decisiones basadas en una inteligencia equivocada. A la vez, tan decisivo fallo no se habría producido sin la actuación de **Juan Pujol**, a quien el MI5 todavía califica como **el mejor agente doble de la Segunda Guerra Mundial**, y del resto de los agentes dobles que alimentaron a la Abwehr con informaciones falsas».

«Es evidente que la CIA erró [en 1961] al enviar una fuerza paramilitar improvisada a combatir contra unidades de un ejército con dos años de guerra revolucionaria a sus espaldas: entre los 1.500 exiliados cubanos enviados a **Bahía de Cochinos**, solo 135 habían sido militares profesionales. También falló su previsión sobre un levantamiento popular que no se produjo. Quizá las expectativas generadas por los partidarios del plan quedaron distorsionadas por las informaciones sobre la isla, no siempre rigurosas, suministradas por la disidencia cubana».

«El informe de la Comisión que investigó los **ataques del 11-S** dejó claro que la comunidad de inteligencia estadounidense desaprovechó múltiples oportunidades que podrían haber llevado a descubrir los preparativos de los ataques. Los errores de la CIA fueron gravísimos, pero la agencia que desperdició más ocasiones fue el FBI.

La mayoría de los fallos del FBI se debieron a un equivocado marco de prioridades, así como a algunos problemas organizativos. Pese a haber realizado importantes misiones de inteligencia durante el pasado siglo, la obligación primordial del FBI desde su creación en 1908 había sido investigar delitos contra las leyes federales en territorio estadounidense. Al término de la Guerra Fría, casi todos sus agentes veteranos se habían dedicado a perseguir esa clase de crímenes».

Israel, 7 de octubre de 2023

«La relativa calma reinante en Gaza después de la guerra concluida en 2021 y la inteligencia sobre los líderes políticos de Hamás afincados en Catar **parecían confirmar [que la organización islamista estaba menos interesada en agredir a Israel que en seguir gobernando Gaza**], si bien indujeron la conclusión de que los mandos operativos de Hamás que permanecían en la Franja tenían las mismas prioridades que los dirigentes políticos que vivían fuera de Gaza, cuando no era el caso. Para los líderes militares como Yahya Sinwar y Mohamed Deif, los cerebros del ataque del 7-O, los Acuerdos de Abraham y la esperada incorporación de Arabia Saudí estaban haciendo olvidar a los árabes y al mundo entero la cuestión palestina, lo que añadía una razón más para escalar el conflicto contra Israel. A su vez, la **confianza del Gobierno de Netanyahu y los mandos militares israelíes en que podían contener a Hamás** ofrecía, de hecho, una oportunidad para preparar un gran ataque».

«¿Por qué falló un sistema construido precisamente para advertir y contener la amenaza procedente de Gaza? Una primera respuesta apunta a las contramedidas empleadas por Hamás como parte de los preparativos del ataque. En las semanas y días previos al 7 de octubre, la organización islamista usó los canales de comunicación que sabía intervenidos por los servicios israelíes para enviar mensajes que sugerían que su liderazgo no tenía ningún interés en cometer ataques que pudieran precipitar una nueva guerra con Israel. Al mismo tiempo, su dirección operativa **redujo al máximo el número de militantes que supieron de la existencia del plan**, compartimentó la información al respecto (de modo que muy pocos operativos conocieran todos los detalles) y protegió las conversaciones sobre el plan y los preparativos, privilegiando el uso de mensajeros y las reuniones presenciales frente a las comunicaciones diferidas y limitando estas a la red de teléfonos cableados instalada dentro de túneles bajo Gaza, mientras se evitaban los teléfonos móviles y la radio».

Proteger secretos

«La mayoría de las fugas de información procedentes de los servicios de inteligencia no se deben a la intrusión de agentes externos, sino a acciones del propio personal. Algunas pérdidas de información son consecuencia de la **actitud descuidada o imprudente de funcionarios leales**. Llevarse a casa documentos clasificados o "pasearlos" fuera de las instalaciones es una mala práctica que ha acarreado más de un disgusto a todos los servicios de inteligencia».

«Existen **dos clases de filtradores**: los que intentan ocultar su identidad —que lo consigan es otra cuestión— y los que prefieren revelarla. Llamemos **susurradores** a los primeros y **denunciantes**, a los segundos. Algunos denunciantes son personas. Así ocurre con el filtrador que no oculta su identidad, el periodista que publica lo que aquel le ha contado o cualquier otra persona que divulga una información filtrada. En cambio, otros denunciantes son organizaciones: medios de comunicación o portales web que permiten a sus periodistas publicar una filtración proveniente de un susurrador o de un filtrador con nombre y apellidos. Todas estas variantes han tenido representación en las dos series de filtraciones más impactantes de principios del presente siglo.

En 2010, **WikiLeaks**, el portal de internet fundado en 2006 por el *hacker* australiano Julian Assange, inició la publicación de los *Diarios de la guerra de Afganistán y de Irak*, una filtración masiva de mensajes del Departamento de Estado (más de 250.000) e informes del Ejército de Estados Unidos (cerca de 500.000). Entre otros muchos secretos, los Diarios documentaron diversos incidentes armados protagonizados por soldados y unidades militares estadounidenses en Afganistán e Irak, maltratos a terroristas recluidos en la base militar de Guantánamo y polémicas opiniones de diplomáticos norteamericanos. **El primer responsable de la filtración fue un cabo del Ejército estadounidense que había desempeñado funciones de analista de inteligencia**».

Agentes extranjeros y traidores

«Las **actividades promovidas en España por servicios extranjeros** han sido de muy diversa naturaleza: espionaje económico, empresarial, científico y tecnológico; colaboración con organizaciones terroristas (en la década de 1970, agentes **argelinos** apoyaron a ETA); vigilancia de extranjeros afincados en España (una especialidad de los servicios **marroquíes, cubanos y chinos**); e incluso reclutamiento de miembros de los servicios españoles: en 2010 Roberto Flórez, miembro del CNI, fue condenado por haber ofrecido documentación clasificada al **servicio de inteligencia exterior ruso** (SVR) y, en 2023, se descubrió que otros dos miembros del CNI, uno de ellos jefe del área de análisis sobre Rusia, llevaban años pasando información a la CIA.

Con todo, el caso español solo confirma una regla universal de la inteligencia: **ningún país es un coto vedado para los servicios de otras naciones**, aunque todos lo procuren. Así como no hay malla que un furtivo no pueda romper para cazar donde no tiene permiso, no hay sistema de seguridad nacional capaz de eliminar de raíz el riesgo de que sus propios órganos de inteligencia sean penetrados por otros servicios. Por eso, el segundo objetivo de la contrainteligencia es detectar la presencia de agentes extranjeros y traidores y poner fin a cualquier actividad suya que amenace la seguridad y los intereses nacionales».

Los servicios de inteligencia y la invasión de Ceuta

«La invasión de la ciudad autónoma de Ceuta y la controversia suscitada a continuación sobre el papel desempeñado por el CNI en dicho episodio vienen a reafirmar varias de las ideas expuestas y argumentadas en este libro. La primera es la **conveniencia de contar con servicios de inteligencia**. Esta conveniencia se pone de manifiesto incluso en algunas de las ocasiones en las que los propios servicios fracasan en sus cometidos, pues al hacerlo muestran que su actuación eficaz habría proporcionado un "servicio" inestimable a su país, valga la redundancia. De todos modos, ya se ha dicho que, en el caso de la invasión de Ceuta, **el fracaso no fue del CNI, ya que**

este organismo alertó en varias ocasiones de que algún hecho grave podía producirse en la frontera ceutí el mismo día en que comenzó la invasión. Realidad que avala un segundo argumento desarrollado en este libro: muchos presuntos errores atribuidos a los servicios de inteligencia no son verdaderos fallos de inteligencia, sino **errores políticos que son fruto de una mala interpretación o comprensión de las informaciones** y valoraciones que los servicios suministran a las autoridades o derivados en otros casos del simple menosprecio de esas mismas informaciones y valoraciones».

A la caza del mentiroso

«Aparte de métodos reprobables como la **tortura y del empleo de drogas psicoactivas**, generalmente ineficaz, otras técnicas desarrolladas para descubrir a los mentirosos pasan por identificar indicios de engaño en el curso de una entrevista o un interrogatorio a partir de **respuestas verbales, conductas no verbales** y ciertas señales fisiológicas».

«Numerosos estudios científicos han sembrado **dudas fundadas acerca de la utilidad de las pruebas poligráficas**. Según una de las investigaciones más exhaustivas sobre el tema, si un servicio de inteligencia compuesto por 10.000 miembros escondiera a diez traidores y todos ellos pasaran por el polígrafo, conseguiría identificar a ocho de los diez traidores verdaderos, pero a la vez también tomaría por traidores a 1.598 empleados leales. Alternativamente, si el mismo servicio recurriera al polígrafo para acabar con las sospechas sobre la existencia de traidores, una prueba que reconociese la veracidad del 95 por ciento de los testimonios sinceros, solo permitiría descubrir a dos de los diez traidores».

¿Confiar o no confiar?

«Confiar o no confiar: en las fuentes, en la información recolectada, en la sinceridad y el buen criterio de los compañeros, camaradas, amigos, jefes o subordinados. En definitiva, confiar o no confiar. He aquí el eterno dilema con el que deben lidiar permanentemente los profesionales de la inteligencia. Más aún, los oficiales de contrainteligencia.

Los más graves fallos de contrainteligencia siempre se deben a una mala gestión del dilema de la confianza. En inteligencia, la confianza ciega es un lujo inasumible. Aunque mantener la guardia alta en todo momento y frente a todos no es sencillo. Existen múltiples factores que pueden animar a confiar más de la cuenta en informaciones y personas. Los protocolos de seguridad, la clasificación de documentos, las medidas de compartimentación de la información y protección de las comunicaciones tienden a rebajar las estimaciones sobre el riesgo de acabar siendo infiltrados o manipulados por agentes extranjeros. Lo mismo sucede con los sentimientos de camaradería, admiración profesional y amistad forjados por años de trabajo compartidos y el espíritu de misión que acompaña al trabajo de campo».

¿Un poder en la sombra?

«Pese a que los servicios de inteligencia siempre han trabajado a la sombra y bajo la protección de los Estados, su habitual subordinación a autoridades superiores suele menospreciarse a menudo. **Las interpretaciones de corte conspirativo que los pintan como una especie de Estados paralelos que no rinden cuentas a ninguna instancia superior solo han encontrado respaldo empírico en casos bastante excepcionales**. Conviene tener presente que la mayoría

de los abusos y delitos cometidos por servicios de inteligencia han sido y son ordenados, alentados o consentidos por los Gobiernos a los que esos organismos deben obediencia».

«Las acciones encubiertas han sido una ocupación habitual o esporádica de muchos servicios de inteligencia, aunque no de todos. Su incorporación al repertorio de actividades de los servicios puede entenderse como una consecuencia del interés de los Estados y Gobiernos en convertir a esos organismos en herramientas de poder y complemento de la diplomacia y la acción militar, con las que puede llegar a mezclarse. **La atención dedicada a esas acciones por escritores, guionistas de cine y periodistas ha exagerado su importancia, pero tampoco conviene subestimarlas**. Inherentemente controvertidas, las acciones encubiertas cumplieron un papel relevante durante la Guerra Fría y han reemergido en los últimos años como un reflejo de la nueva etapa de intensa rivalidad geopolítica que ha transformado las relaciones internacionales».

Una mirada al futuro inmediato

«Nadie duda de que **en los próximos años el sistema internacional acentuará su tendencia natural a la anarquía** y veremos aumentar (todavía más) la rivalidad entre Estados. Los expertos en asuntos militares y de seguridad están convencidos de que las amenazas y los conflictos híbridos continuarán mutando y diversificándose y auguran un protagonismo creciente de las actividades hostiles en la zona gris. En paralelo, **tecnologías emergentes como la inteligencia artificial avanzada, la computación y los sensores cuánticos, las neurotecnologías** (técnicas para registrar, estimular y condicionar la actividad cerebral), las nuevas generaciones de robots y vehículos no tripulados y las biotecnologías (que permitirán manipular organismos y patógenos con mucha más precisión, creando riesgos biológicos muy difíciles de detectar y atribuir) **generarán entornos operativos más complejos, inciertos y dinámicos**. En un mundo atravesado por esas tendencias, los servicios de inteligencia deberán promover cambios sustantivos en su manera de trabajar. De hecho, algunos de esos cambios fueron identificados hace ya algunos años».

«Todo invita a pensar que **la nueva herramienta principal será la inteligencia artificial** (IA). Aunque las actuales previsiones sobre los futuros desarrollos de la IA podrían resultar exageradas, la combinación de capacidades ya disponibles y desarrollos plausibles transformará el trabajo ordinario de los servicios».

PARA AMPLIAR INFORMACIÓN

Erica Aspas I RESPONSABLE DE COMUNICACIÓN ÁREA DE ENSAYO
689 77 19 80 I easpas@planeta.es

ÍNDICE DESARROLLADO

Prólogo 11
Introducción: ¿Qué son y qué hacen
los servicios de inteligencia? 17
La noticia oculta de las cosas 17
Los servicios de inteligencia como
organizaciones e instituciones 21
¿Servicios secretos o servicios de inteligencia? 24
No solo inteligencia 25

Primera parte
ORIGEN DE LOS SERVICIOS Y FUNDAMENTOS DE LA INTELIGENCIA

1 . Genealogía de la inteligencia 29
Un largo pasado 30
Los imperativos 31
Del espionaje antiguo a las primeras
estructuras de inteligencia 32
Al servicio de los Estados 35
Razón y secretos de Estado 36
La inteligencia de monarcas,
ministros y secretarios 37
La información secreta del siglo XVIII al XIX 39
Los servicios modernos 41
Primeros hitos institucionales 42
La Guerra Fría y la consolidación definitiva
de los servicios 46
Hacia el siglo XXI: del antiterrorismo al
espionaje digital 52
Las estructuras de inteligencia en España 54
La Guerra Civil y la dictadura 54
Del CESID al CNI 58

2 . Para qué sirve y cómo se hace la inteligencia 61
Una guerra contra la ignorancia y
la incertidumbre 61
Usos y funciones 63
Sobre las armas nucleares chinas 65
¿Cuántos tipos de inteligencia existen? 66
La inteligencia como proceso: el ciclo 68
Fijar el rumbo (dirección y planificación) 70
Buscando información (obtención) 71
De lo crudo a lo cocido (elaboración) 73
Sherman Kent, maestro de analistas 74
Entrega dirigida (difusión) 78
De la teoría a la práctica 79
Inteligencia accionable: a la caza de Bin Laden 80

Segunda parte
DESAFÍOS DE LA OBTENCIÓN

3 . Robar secretos 89
Perfiles a través del tiempo 90
Espías en las primeras guerras del siglo XX 90
El proceso de espiar 95
Los hombres del Circus (o el espionaje
como obra colectiva) 96
Cómo preparar y ejecutar una operación
de espionaje 98
Penetraciones e infiltraciones 100
Tres héroes del Mossad 101
Philby: un topo casi perfecto 107

4 . ¿Qué mueve a los espías? 111
Intereses 112
Codicia: John Walker 112
Dinero y deudas: Tong Daning 113
El ego herido y afán de reconocimiento:
Robert Hanssen 114
Amor al riesgo y sed de aventuras:
Sidney Reilly 116
Pasiones 117
Resentimiento, odio y venganza:
Ibrahim Yassin 118
Miedo, trampas de miel y otras formas
de chantaje: John Vassall 119
La voluntad de agradar: los agentes Romeo 121
Un idilio poco común: el caso Boursicot 122
Ideas e ideales 123
I de ideología 124
Dos leyendas soviéticas 124
Desengaños políticos: Penkovsky, Vetrov
y los traidores a la URSS 127
Patriotismo y espionaje en tiempos de guerra 128
Louise de Bettignies: la reina de las espías 128
Aline Griffith: modelo, espía y condesa 130
Los altruistas 132
Juan Pujol contra los nazis 132
Omar Nasiri: del GIA a Al Qaida 135

5 . Dirigir fuentes y agentes 141
El ciclo HUMINT 141
Cómo reclutar una fuente 141
Así se captó a Mikel Lejarza 144
Funciones y reglas en la dirección de
fuentes y agentes 148
Y así se dirigió a Lobo 152
Las fuentes no reclutadas y la
inteligencia de contactos 157
La Transición y las entrevistas del SECED 159

6 . Destrezas y artilugios 163
Coberturas y tapaderas 164
Vivir otra vida: agentes durmientes
y los ilegales del KGB 166
Organizaciones pantalla 169
Brewster Jennings y Asociados:
la tapadera de Valerie Plame 170
Escondites, intercambios y reuniones secretas ....., 172
Comunicaciones técnicas encubiertas 174
De las radios a las telecomunicaciones 174
Intrusiones, cámaras y micrófonos 176
De los USB chinos a «Dumbo» (extracciones
Digitales sobre el terreno) 177

7 . Posibilidades de la técnica 181
Sobre señales y mensajes:
SIGINT, COMINT, ELINT, FISINT 182
Escuchando al enemigo: un siglo
de inteligencia de señales 183
La alianza de los Cinco Ojos 185
De la inteligencia de imágenes a la geoespacial 188
Espiar desde el cielo y el espacio 190
La evolución del reconocimiento aéreo espacial 190
A vista de pájaro: las naves aéreas no tripuladas ... 193
Drones desde Yemen a Rusia 195

Más allá de señales e imágenes 197
Cómo se descubrió la bomba soviética 199

8 . Inteligencia digital y ciberespionaje 203
La intuición de Turing 203
La revolución digital y sus consecuencias
para los servicios de inteligencia 205
Patrullando el ciberespacio: de las fuentes
abiertas al espionaje informático 206
Interceptando comunicaciones y mensajes digitales.. 207
Los programas de interceptación digital:
de Eikonal a Tempora 209
Intrusiones informáticas 211
Los equipos no conectados 212
Los servicios como hackers 212
Pegasus, el CNI, el Catalangate y
la sombra de Rabat 216
Infiltrados virtuales 220
Yihadistas en internet: la historia de
Cole James Bridges 224

Tercera parte
FALLOS DE INTELIGENCIA

9 . Sorpresas, fracasos y aciertos 229
Fallos de inteligencia y fracasos de los servicios 230
Sorpresas y falsas alarmas 230
Inteligencia defectuosa, contrainteligencia
y operaciones encubiertas 231
La Operación Fortaleza y los engaños de Garbo 232
Bahía de Cochinos 234
Inteligencia desaprovechada 236
Arrogancia y miedo: cuando Stalin confió en
Hitler (y se equivocó) 238
¿Son inútiles los servicios de inteligencia?
La hipótesis del gran engaño 241
Múltiples formas de subestimar
el valor de la inteligencia 242
Un libro sobre la CIA 244
Balance tentativo de la inteligencia *made in USA* .. 245
Buscando un criterio 249
¿Por qué los servicios de inteligencia
no pueden predecirlo todo? 249
El Muro de Berlín 252
¿Cómo valorar la inteligencia? 252

10 . La información como problema 255
Déficits informativos y sus causas 255
La ley de la escasez 255
Entornos opacos, barreras y obstáculos 257
Espiar en democracia 258
La Comisión McDonald 259
Controles sobre las actividades de obtención..... 260
Escándalos y vacíos legales (o por qué
el CESID se convirtió en CNI) 262
Inundados de información 268
Cuando Japón atacó Hawái 270

11 . La mente del analista 275
En busca de la verdad y la objetividad 276
Influencias externas y entorno operativo 277
Racionales e irracionales 278
La intuición humana y sus límites: sesgos en análisis.. 279
La lección de Nosenko (Richards J . Heuer) 281
Primar y sobrestimar informaciones 282
Conectar puntos, buscar patrones, atribuir causas 284
El problema de explicar lo ocurrido 285
Establecer hipótesis y estimar probabilidades 287
El síndrome del espejo: errores sobre el mundo
islámico, la URSS y la India 289
La tiranía de las ideas 291
Corrientes de opinión y la prevista/imprevista
invasión de Ucrania 294
La guerra de Yom Kipur, el «concepto»
y otros problemas 295

12 . Fracasos organizativos 299
La impronta burocrática 299
Peso y precio de las jerarquías 300
Reglas y compartimentos 301
Sesgos y vicios institucionales 303
Cultura y clima 303
Casandra y el lobo (patologías de la alerta) 305
Inercia y resistencia al cambio 307
Comunidades descoordinadas,
agencias que compiten 310
El 11-S como fallo organizacional y sistémico 312
Los antecedentes: adaptaciones aplazadas 313
Errores de enfoque, informaciones ambiguas,
indicios tardíos 315
Una comunidad incomunicada 316
El papel del FBI 317

13 . Cuando todo falla (Irak 2003, Israel 2023) 323
Irak y las armas que nunca existieron 325
Mucho más que mentiras 325
Una hipótesis plausible 326
La dimensión política 327
Una endeble base informativa 329
Fabricadores 331
Fallos analíticos múltiples 334
Matanza del 7-O y fracaso de la inteligencia israelí ... 337
Los antecedentes 338
Los fallos de alerta temprana y las
contramedidas de Hamás 339
Las señales 341
«Concepto» sobre Hamás y desprecio de alertas 342
Arrogancia tecnológica 345
Las alertas finales 347

Cuarta parte
CONTRAINTELIGENCIA Y CONTRAESPIONAJE

14 . Proteger secretos 351
Mensajes y códigos 352
Tintas invisibles, microfilms, micropuntos y más .. 352
Criptógrafos contra criptoanalistas 353
Un telegrama para entrar en guerra:
el caso Zimmermann 355
Entran las máquinas 357
Cosmic Top Secret: clasificación y
control de las materias reservadas 358
Factor humano y políticas de personal 360
Selección y alistamiento 360
Supervisar y vigilar 361
Aldrich Ames: una brecha de seguridad andante ... 363
El problema de las filtraciones 366
Indiscreciones sobre la batalla de Midway
y los Papeles del Pentágono 367
Susurradores y denunciantes: De WikiLeaks a
Snowden..... 368

15 . Cómo atrapar a un agente 373
Inteligencia a la contra 374
VENONA: señales, criptoanálisis y contrainteligencia 375
Investigaciones 377
Trampas y provocaciones 378
Atrapar a un traidor (de nuevo, Ames) 379
Aportaciones analíticas 381
El agente 8882: ¿y si Marruecos plantara un topo en el CNI? 382
Testimonios y confesiones 383
Klaus Fuchs: científico, espía y delator 384
De la tortura al suero de la verdad 385
El «detector de mentiras» 389
¿Qué hacer con los agentes de otros? 392

16 . Sobre topos y dobles 397
Contrainteligencia ofensiva 397
¿Qué es, en verdad, un agente doble? 398
Joaquín Madolell contra el GRU 400
Los topos 404
Oleg Gordievski: el sentido de una traición 406
Ventajas e inconvenientes de las operaciones con agentes dobles y topos 409
Las oportunidades 410
Complicaciones y costes 411
Espiando a la Stasi (lo que todo agente espera y no siempre consigue) 412
Tal vez una agente triple: Katrina Leung 415

17 . Una jungla de espejos 421
Decepción y contradecepción 422
Para confundir y engañar a un servicio 423
Decepción en la guerra: tres muestras 425
El ardid de la mochila: engaño táctico en la Primera Guerra Mundial 425
Desinformar por varias vías: la ocultación del ataque a Pearl Harbor 426
Un cadáver en Punta Umbría 428
Contradecepción 430
Los misiles que llegaron a Cuba (contradecepción tardía) 432
¿Confiar o no confiar? 435
El túnel de Berlín (sobreconfianza en la inteligencia técnica) 435
La paranoia en los servicios 437
Las obsesiones de Angleton 438

Quinta parte
LAS ACCIONES ENCUBIERTAS

18 . El imperativo de la acción 445
¿Qué son las acciones encubiertas? 445
Institucionalización de actividades encubiertas..... 448
El espectro de lo clandestino 450
La pugna entre Occidente y la URSS y las operaciones secretas 453
Propaganda y política clandestina en la Europa de posguerra 454
Del Tíbet a la guerra de Vietnam 455
América Latina: políticas de patio trasero y revoluciones 456
Oriente Próximo y África: golpes de Estado y guerras civiles 459
Reactivación de los teatros europeo y latinoamericano 461
Últimos éxitos de la CIA 463

19 . Sombras y luces de las acciones encubiertas ... 465
Dilemas morales y zonas de sombra 466
¿Hasta qué punto son útiles?..... 469
Afganistán, la Operación Ciclón y las consecuencias no previstas 470
Otras misiones secretas 473
Dos rescates de película (mar Rojo, Irán) 474
Diplomacia secreta y procesos de paz tras la Guerra Fría 477
Negociando con criminales 479
Conversaciones con ETA 480
Rescatados por el CNI 482

20 . Desinformación, injerencias y guerras clandestinas en el siglo XXI 485
¿Por qué han vuelto las acciones encubiertas? 486
Estados Unidos e Israel contra el terrorismo internacional y el Eje de la Resistencia 488
Afganistán, otoño de 2001 489
Objetivo: el programa nuclear iraní 491
Los buscas asesinos y la peor derrota de Hizbulá .. 493
Influencias e injerencias 494
Operaciones digitales 495
Herramientas para desinformar y manipular 497
Algunas campañas 500
El modelo de influencia chino 501
El regreso de las medidas activas 504
Desinformación, injerencias y acciones hostiles en Estados Unidos y Europa 506
De la zona gris a las guerras híbridas 508
Objetivo Taiwán 509
Crimea y Donbás (2014) 511
Una operación especial 514
La guerra encubierta en Ucrania 516

Final 519
Ideas para llevar 519
La reinvención de los servicios (epílogo futurista) 523
Posdata: Los servicios de inteligencia y la invasión de Ceuta 529
Agradecimientos 533
Notas 539
Bibliografía mínima 557
Bibliografía completa 561
Índice desarrollado 563