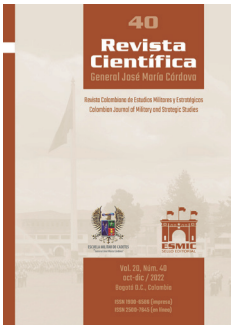
Revista Científica General José María Córdova
ISSN: 1900-6586
ISSN: 2500-7645
Escuela Militar de Cadetes "General José María Córdova"

Martínez-Sánchez, Juan Antonio
Una aproximación psicosocial a las causas de los fallos de inteligencia
Revista Científica General José María Córdova, vol. 20, núm. 40, 2022, Octubre-Diciembre, pp. 908-926
Escuela Militar de Cadetes "General José María Córdova"

DOI: https://doi.org/10.21830/19006586.977

Disponible en: https://www.redalyc.org/articulo.oa?id=476274912009



Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)
Bogotá D.C., Colombia

ISSN 1900-6586 (impreso), 2500-7645 (en línea)
Web oficial: https://www.revistacientificaesmic.com

Una aproximación psicosocial a las causas de los fallos de inteligencia

Juan Antonio Martínez-Sánchez
https://orcid.org/0000-0002-7696-5023
jamartsan@ea.mde.es
Ministerio de Defensa de España, Madrid, España

Citación APA: Martínez-Sánchez, J.A. (2022). Una aproximación psicosocial a las causas de los fallos de inteligencia. *Revista Científica General José María Córdova*, *20*(40), 909-926. https://dx.doi.org/10.21830/19006586.977

Publicado en línea: 1.º de octubre de 2022

Para enviar un artículo:
https://www.revistacientificaesmic.com/index.php/esmic/about/submissions

ESMIC
SELLO EDITORIAL
Miles Doctus

Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)
Bogotá D.C., Colombia

Volumen 20, número 40, octubre-diciembre 2022, pp. 909-926
https://dx.doi.org/10.21830/19006586.977

Una aproximación psicosocial a las causas de los fallos de inteligencia

A psychosocial approach to the causes of intelligence failures

Juan Antonio Martínez-Sánchez
Ministerio de Defensa de España, Madrid, España

Resumen. Este artículo aborda el concepto de *fallo de inteligencia*, sus rasgos y sus principales causas a partir de una perspectiva psicosocial. Desde este punto de vista, se plantea que los errores son inherentes a toda actividad humana y a la naturaleza de la inteligencia, de modo que su ocurrencia es normal e inevitable en sistemas complejos, como lo son los servicios, las agencias y las comunidades de inteligencia. Con todo, se argumenta que, si bien no se pueden evitar, es posible minimizar su ocurrencia y mitigar el impacto negativo que podrían tener. En ese sentido, se plantean algunas medidas y acciones que pueden contribuir a ese fin.

Palabras clave: fallo de inteligencia; inteligencia; psicología social; seguridad; teoría de los accidentes normales

Abstract. This article addresses the concept of intelligence failure, its features, and its main causes from a psychosocial perspective. From this point of view, it argues that errors are inherent to all human activity and the nature of intelligence. Therefore, their occurrence is normal and inevitable in complex systems, such as intelligence services, agencies, and communities. However, it contends that, although they cannot be avoided, it is possible to minimize their occurrence as much as possible and mitigate the negative impact they could have. In this sense, some measures and actions that can contribute to this end are proposed.

Keywords: intelligence failure; intelligence; social psychology; safety; normal accident theory

Sección: Dosier • Artículo de investigación científica y tecnológica
Recibido: 4 de mayo de 2022 • Aceptado: 7 de septiembre de 2022

Contacto: Juan Antonio Martínez-Sánchez ✉ jamartsan@ea.mde.es

Introducción

En el ámbito de la inteligencia los fallos son normales y existen desde que el ser humano sintió la necesidad de disponer de información sobre sus adversarios para, en última instancia, emplearla contra ellos. El siglo XX ofreció un sinnúmero de fallos y fracasos de inteligencia, algunos de los cuales tuvieron consecuencias trascendentales de tipo político y estratégico. Al respecto, cabe mencionar, a modo de ejemplos, el fallo de la inteligencia estadounidense al no advertir el ataque japonés contra Pearl Harbor, en 1941; el de los rusos al no prever la invasión alemana de 1940; y la "sorpresa" que causó en Israel el ataque árabe que desencadenó la denominada guerra de Yom Kippur, en 1973. La incapacidad de la inteligencia estadounidense para prevenir los ataques terroristas del 11 de septiembre de 2001 (11-S) es un ejemplo más reciente de fallos de inteligencia.

Los fallos de los servicios de inteligencia han atraído siempre más la atención que sus éxitos, lo que justifica el interés académico en el tema durante las últimas décadas (G. Díaz, 2005). Dicho interés se inició con la extensa investigación que Roberta Wohlstetter (1962) desarrolló sobre el fallo de los Estados Unidos para pronosticar o alertar sobre el ataque japonés contra Pearl Harbor el 7 de diciembre de 1941, investigación que tuvo el acierto de trascender la mera búsqueda de culpables para analizar las causas del error (Marrin, 2004). A partir de entonces, y debido a las repercusiones políticas, históricas, económicas e incluso sociales de este tipo de errores, proliferaron los estudios sobre fallos de inteligencia. Como es lógico, la principal motivación de estos estudios era práctica: la necesidad de evitar que dichos errores se repitieran en el futuro (Duffy, 2003).

A principios del siglo XXI, la investigación sobre fallos de inteligencia tuvo un impulso aún mayor, a raíz de los ataques del 11-S y del "fiasco" de las supuestas armas de destrucción masiva de Irak. El 11-S marcó un antes y un después para los servicios de inteligencia (Esteban & Navarro, 2003). La tormenta política y académica que se desató incluyó feroces críticas contra los servicios de inteligencia estadounidenses. Dichas críticas comprendieron duros calificativos, como "ineficacia desconocida" o "fallo estrepitoso" (Navarro, 2004, p. 32), y propusieron soluciones drásticas, como la reorganización y redefinición de las funciones, estructuras y objetivos de los servicios de inteligencia (Laqueur, 2003).

Igualmente criticada fue la actuación de la comunidad de inteligencia estadounidense a propósito de la supuesta existencia del programa de armas de destrucción masiva de Irak. Estas críticas incluyeron múltiples acusaciones de politización, de inadecuación de los métodos de obtención y análisis de la información y de falta de preparación de analistas. Al respecto, el informe final del Comité de Inteligencia del Senado de los Estados Unidos encontró al menos 71 fallos en la actuación de sus servicios de inteligencia, con lo cual ofreció una imagen muy negativa de su actuación (United States Senate Select Committee on Intelligence, 2004).

Frente a estas críticas se alzaron voces especializadas que defendieron posturas contrarias (Betts, 2002; Heuer, 2005; Hedley, 2005; Lefebvre, 2004). Para la que fuera directora

del servicio de inteligencia británico MI5 entre 1992 y 1996, Stella Rimington, culpar a los servicios de inteligencia occidentales de no haber hecho nada por prevenir los ataques del 11-S es no entender nada de la naturaleza de los servicios secretos (Navarro, 2004). Idéntico argumento fue utilizado por Richards Heuer (2005), que acusó a los miembros del Comité de Inteligencia del Senado de sufrir de una grave falta de comprensión de la dinámica del análisis de inteligencia y del trabajo de los analistas. Asimismo, Richard J. Kerr, ex director adjunto de la Agencia Central de Inteligencia (CIA) y encargado de dirigir la investigación interna sobre la actuación de la agencia en este tema, culpó al Comité del Senado de no comprender el trabajo de los servicios de inteligencia, la dinámica de obtención y análisis de información y las limitaciones del proceso (Corera, 2004). Hedley (2005) fue más allá, al acusar a quienes hicieron este tipo de críticas de poseer expectativas poco realistas sobre el trabajo y el funcionamiento de los servicios de inteligencia.

Tras estos argumentos parece subyacer una premisa incuestionable en el ámbito de la inteligencia: *los fallos y fracasos de inteligencia son inevitables* (Berkowitz, 2001; Betts, 1978; Brady, 1993; Handel, 1977, 1984; Herman, 1996; Hedley, 2005; Kuhns, 2003; Marrin, 2004). Así, para Richard Betts (1978), los fallos de inteligencia son normales y, como afirma Michael Herman (1996), no solo *pueden* ocurrir, sino que *deben* ocurrir. Más contundente resulta la opinión de Hollister (2005, pp. 435-436), que concluye que "la afirmación de que los fallos de la inteligencia son inevitables tiene la certeza de una ley de la física". Sin embargo, a pesar del consenso académico sobre la inevitabilidad de los fallos de inteligencia, la mayoría de estudios se ha centrado en el análisis de acontecimientos históricos que supusieron importantes fracasos, mientras que los trabajos que han tratado de profundizar en cuáles son las causas de dicha inevitabilidad son más bien escasos.

Desde una perspectiva psicosocial, este artículo pretende responder a la cuestión de por qué los fallos y errores de inteligencia son inevitables. Este propósito exige analizar el concepto de *fallo de inteligencia,* sus principales rasgos definitorios y sus principales causas. Esta perspectiva permite, además, proponer algunas medidas cuyo objetivo es minimizar al máximo la ocurrencia de fallos y errores en el proceso de inteligencia.

Para analizar el concepto y sus principales causas, se usó una metodología cualitativa. En ese sentido, se llevó a cabo una revisión de la literatura y un análisis documental que partió de una búsqueda bibliográfica en distintas bases de datos e índices. Las bases de datos consultadas fueron SCOPUS, EBSCOhost Research Platform, CSA Worldwide Political Science Abstract (WPSA), The Lancaster Index to Defence and International Security Literature y Taylor and Francis Online.

Se utilizaron los descriptores "intelligence failure AND analyst" como palabras clave. En el proceso, se descartaron los documentos desactualizados, los pertenecientes a publicaciones sin factor de impacto y aquellos artículos cuyo contenido no se circunscribía al ámbito del análisis de inteligencia. De esta manera, el número final de documentos examinados fue de 103.

El concepto de *fallo de inteligencia*

Existen múltiples definiciones de *fallo de inteligencia* en la literatura, aunque la mayoría de autores toman como referencia las de Mark Lowenthal (1985) y Abram Shulsky y Gary Schmitt (2002).

Para Lowenthal (1985), fallo de inteligencia es la incapacidad de una o varias partes del proceso para producir inteligencia oportuna y exacta sobre una cuestión o acontecimiento de importancia para el interés nacional. Por su parte, Shulsky y Schmitt (2002) ponen el énfasis en los destinatarios de la inteligencia y en las consecuencias negativas que provocan los fallos, al definirlos como todo malentendido de una situación que conduce a un Gobierno o a sus fuerzas armadas a emprender acciones inapropiadas y contraproducentes para sus propios intereses.

El Diccionario LID de Inteligencia y Seguridad considera fallo de inteligencia toda situación no deseada por el decisor político o militar y provocada por la incapacidad de los servicios y agencias para suministrar inteligencia adecuada (A. Díaz, 2013). Además, desde una perspectiva teórica del estudio del término, para G. Díaz (2005) consiste tanto en el fallo del proceso de inteligencia como en el de los decisores al utilizar la información que se les suministra.

En resumen, y conjugando todas las anteriores definiciones, cabe concluir que un fallo de inteligencia es todo error que se presente en cualquiera de las fases del ciclo de inteligencia y que impide al decisor político o militar disponer de la información adecuada para la toma de decisiones. Pero, dentro de tales errores, también se encuentra y se destaca el fallo de los decisores políticos y militares consistente en *ignorar o utilizar de manera inapropiada* la inteligencia adecuada o correcta que es proporcionada por los servicios de inteligencia.

Varios rasgos definen la naturaleza de los fallos de inteligencia, entre ellos sus múltiples causas, sus consecuencias para la seguridad nacional, su estrecha relación con la denominada sorpresa estratégica y, como ya se ha mencionado, el hecho de ser inevitables.

Sus múltiples causas

Frente al punto de vista tradicional, que defiende que los fallos de inteligencia poseen una sola causa, hoy en día predomina la idea de que *sus causas son múltiples* (G. Díaz, 2005; Lefebvre, 2004). Desde este punto de vista, el interés de los investigadores ha sido determinar cuáles son esas causas. Entre otras, han señalado las siguientes: los errores en los procesos y métodos de análisis; las limitaciones tecnológicas en la obtención y procesamiento de la información; las dificultades de comunicación y coordinación; ciertos defectos organizacionales propios de las agencias y servicios de inteligencia; la mala praxis y actuación de políticos y consumidores de inteligencia; y las limitaciones psicológicas y cognitivas de los analistas (relacionadas con procesos psicológicos como la atención, la

memoria, el procesamiento de información, el razonamiento, la motivación, etc.) y entre las que se encuentran los sesgos cognitivos y el empleo de reglas o estrategias heurísticas o atajos mentales.

A menudo, se ha recalcado la influencia de uno u otro factor, mientras que se ha minimizado o ignorado la de los demás. Pero los fallos de inteligencia no deben analizarse desde el supuesto de que existe un solo culpable, sino desde la perspectiva del ciclo de inteligencia completo, pues este conforma una realidad global y cualquier disfunción en una de sus fases provoca que todo el proceso deje de funcionar correctamente (G. Díaz, 2005). Un ejemplo claro de esto se tiene en los numerosos errores que se presentaron en todas las fases del ciclo de inteligencia que impidieron predecir y evitar los ataques del 11-S (Betts, 2007; Steele, 2002).

Sus múltiples consecuencias

Así como tienen múltiples causas, los fallos y errores de inteligencia provocan *múltiples y variadas consecuencias*, tanto sobre la seguridad nacional de los Estados en general como sobre la comunidad de inteligencia en particular.

En determinados casos, estos fallos tienen un alto impacto en la seguridad nacional, con consecuencias muy negativas, incluso "apocalípticas" (Betts, 1978, p. 62). Un ejemplo este tipo de consecuencias lo representan los fallos de la inteligencia estadounidense que le impidieron alertar el ataque japonés contra Pearl Harbor, en 1941, y la instalación de misiles soviéticos en Cuba, en 1962, o el fallo en la estimación de las capacidades de Sadam Huseín, que desencadenó la ocupación militar de Irak, en 2003. Sin embargo, en la mayoría de las ocasiones, los errores de inteligencia tienen un mínimo impacto en la seguridad de un país y pasan completamente inadvertidos para la opinión pública (Marrin, 2004).

En cualquier caso, es la gran trascendencia que algunos fallos de inteligencia tienen para la seguridad y la necesidad de evitar su futura repetición lo que ha provocado, como ya se dijo, un fuerte interés en su estudio y análisis. En este sentido, y como aspecto positivo, los fallos de inteligencia dan lugar a comités y comisiones de investigación y propician la desclasificación de información, lo que moviliza a la comunidad académica e impulsa el desarrollo de modelos teóricos (G. Díaz, 2017). Otros efectos directos de los fallos de inteligencia son las continuas reformas y restructuraciones que padecen los servicios y agencias de inteligencia.

Su relación con el factor sorpresa

Una de las principales funciones de los servicios de inteligencia es proteger de lo inesperado a aquellos a los que sirve (Laqueur, 1985), lo que lleva a la íntima relación que existe entre los conceptos de *fallo de inteligencia* y *sorpresa estratégica.* Tradicionalmente se ha considerado a la sorpresa como un tipo específico de error de inteligencia (Betts, 1978),

aunque frecuentemente suele ser conceptualizada como el resultado de algún fallo en alguna de las fases del ciclo de inteligencia (George, 2004; Marrin, 2004)[1].

La equiparación entre ambos términos viene motivada en parte por el hecho de que los primeros avances teóricos sobre fallos de inteligencia se realizaron gracias al estudio de acontecimientos bélicos de relevancia mundial que tomaron desprevenido al adversario, es decir, de sorpresas estratégicas. Además, hay que considerar que, en cuanto órganos asesores de los Gobiernos en política exterior, uno de los objetivos de las agencias y servicios de inteligencia es la anticipación de acontecimientos. De ahí que, cuando, a pesar de los esfuerzos de la comunidad de inteligencia, ocurre la sorpresa, se tiende a hablar de fallo de inteligencia.

Otro aspecto que puede llevar a equiparar ambos términos es el hecho de que, al igual que el fallo de inteligencia, la sorpresa estratégica también es inevitable (Betts, 2002; Heuer, 2005; Marrin, 2004). De hecho, nada ni nadie puede evitar que un adversario emprenda una acción súbita e inesperada contra otro. Es más, aunque los servicios de inteligencia de un país conozcan las intenciones del adversario de llevar a cabo un ataque contra sus intereses, el factor sorpresa siempre va a estar presente. Por ejemplo, en lo que respecta a cuándo y cómo se producirá el ataque (Betts, 2002).

Por último, no se puede olvidar que la ocurrencia de acontecimientos súbitos e inesperados constituye una constante en las relaciones internacionales (Heuer, 2005), tal como sucede con los denominados eventos espontáneos imprevisibles, como los *cisnes negros* y los *enigmas* o *misterios*[2].

Su inevitable inevitabilidad

Por último, no debe olvidarse que los fallos, fracasos y errores de inteligencia están intrínsecamente relacionados con la intervención del ser humano, que siempre padece de múltiples limitaciones que pueden manifestarse en todas y cada una de las fases del ciclo de inteligencia (Martínez-Sánchez, 2016). De ahí su principal rasgo definitorio: su *inevitabilidad.*

1 En esta perspectiva, como posibles causas de una sorpresa estratégica se han señalado la falta o el exceso de información, los fallos en la obtención, integración y análisis de la información, el empleo por parte del adversario de tácticas de decepción y ocultación y los errores cometidos por políticos y decisores al ignorar las advertencias de inteligencia (Marrin, 2004).

2 El término *cisne negro (black swan)* fue acuñado por Nassim Nicholas Taleb (2007), para describir a aquel acontecimiento altamente improbable que posee tres características definitorias: es impredecible, tiene gran impacto y consecuencias trascendentales (económicas, políticas, estratégicas, etc.) y solo puede ser explicado en retrospectiva. Ejemplos de cisnes negros son la caída del Muro de Berlín, en 1989, los atentados del 11-S o los acontecimientos de la Primavera Árabe de 2010. Por su parte, en inteligencia se denomina *misterio* o *enigma* a aquellos interrogantes que no pueden ser explicados con certeza (Treverton, 2001, pp. 11-15). Así, las verdaderas intenciones detrás del programa nuclear de Corea del Norte constituirían un ejemplo de misterio.

Las principales causas de los fallos de inteligencia

Desde la perspectiva psicosocial, se puede afirmar que son tres las principales causas que explican su inevitabilidad: 1) los errores son inherentes a la actividad humana; 2) los fallos son consustanciales a la naturaleza de la inteligencia; y 3) los fallos son normales en los sistemas y organizaciones complejas (G. Díaz, 2017; Martínez-Sánchez & Rodríguez, 2019; Stempel, 1999). Como ya se ha apuntado, estas causas se relacionan directamente con la intervención del ser humano en las distintas fases del ciclo de inteligencia.

Los errores son inherentes a la actividad humana

Esta premisa parte de una afirmación irrefutable: "los errores pueden ocurrir en cualquier actividad" (Betts, 1978, p. 62). Y el ser humano está presente en todas las actividades que constituyen las fases del ciclo de inteligencia, por lo que también lo están sus limitaciones y, por tanto, la posibilidad de que cometa errores al intervenir en ellas. Son seres humanos, con sus múltiples sesgos psicológicos y cognitivos, los que deciden qué inteligencia obtener, cómo obtenerla y qué recursos dedicar a esa labor. Son personas las que se encargan de obtener la información, interpretarla, gestionarla, procesarla y analizarla. Son personas las que redactan y supervisan los informes de inteligencia. Y son humanos los que, finalmente, y sobre la base de los anteriores informes, toman decisiones de tipo político o estratégico.

Sin embargo, hay dos etapas del proceso de inteligencia en las que la intervención humana resulta fundamental: la fase de *análisis* y la de *planeamiento y toma de decisiones.*

La *fase de análisis* es una etapa crítica en la que el riesgo de cometer errores es elevado, debido a varios factores. En primer lugar, porque los analistas se mueven continuamente entre la ambigüedad y la incertidumbre, asumiendo constantemente riesgos, lo que los lleva a exponerse continuamente al fracaso (Hedley, 2005). En segundo lugar, porque el análisis constituye una tarea puramente intelectual, sometida a la influencia de múltiples limitaciones cognitivas (Handel, 1984; Heuer, 1999; Marrin, 2003). Y, en último lugar, porque, a pesar de que el análisis es una actividad individual, buena parte del trabajo del analista se realiza en grupo, de modo que se encuentra sujeto también a la influencia de numerosos sesgos grupales.

Entre las barreras psicológicas que afectan al analista se encuentran: las limitaciones perceptivas y de memoria; el uso de modelos mentales y los sesgos cognitivos (por ejemplo, sesgos ideológicos, políticos, de creencia personal); los sesgos relacionados con la obtención, procesamiento y evaluación de la información (la percepción de relaciones causa-efecto); los sesgos en la estimación de probabilidades y capacidades e intenciones del adversario; los sesgos en la generación y elección de hipótesis y el uso de reglas o estrategias heurísticas[3] (Heuer, 1999; Martínez-Sánchez, 2014). Entre los sesgos grupales que afectan

3 Una regla o estrategia heurística es un proceso de pensamiento automático y, a menudo, inconsciente que permite simplificar la resolución de problemas y la toma de decisiones, pero que no siempre garantiza un resultado correcto (A. Díaz, 2013).

al trabajo en equipo del analista sobresalen el consenso prematuro, la holgazanería social *(social loafing)*, la polarización y el pensamiento de grupo *(groupthink)* (Heuer, 2008).

En la *fase de planeamiento y toma de decisiones*, la opinión generalizada entre los estudiosos es que la clase política es responsable de buena parte de ellos (Betts, 1978; George, 2004; Johnson, 2006; Poteat, 1976)[4]. Esto se debe a factores como la falta de comunicación entre inteligencia y política, la inadecuada definición de las necesidades de inteligencia, el uso incorrecto de la inteligencia y la politización o subordinación de la inteligencia a la política.

Los fallos son consustanciales a la naturaleza de la inteligencia

Los fallos son naturales e inherentes a la inteligencia (Random, 1958). Berkowitz (2001) se muestra explícito en la defensa de esta premisa, al señalar que los fracasos son inevitables en los asuntos de inteligencia. Esto se debe en buena medida a que los servicios de inteligencia trabajan siempre en medio de la incertidumbre y con información siempre imperfecta (Betts, 2002; Heuer, 2005; Lefebvre, 2004).

Fenómenos como las relaciones internacionales, el terrorismo internacional o el crimen organizado constituyen problemas complejos, motivados y creados por la interacción de muchos y diversos factores (sociopolíticos, estratégicos, militares, económicos, etc.), lo que dificulta su comprensión y análisis. Dicha *complejidad* se ve agravada, además, por otros factores inherentes a la inteligencia ya señalados, como la ambigüedad y la incertidumbre, las características de la información y el uso de tácticas de decepción por parte del adversario.

Años antes de los ataques terroristas del 11-S, Mark Lowenthal (1993) y Holt B. Westerfield (1996) ya habían alertado sobre la incapacidad de la comunidad de inteligencia estadounidense para procesar adecuadamente escenarios de incertidumbre, una advertencia que es generalizable a la mayoría de los servicios de inteligencia del mundo (Montero, 2004). La incertidumbre se encuentra presente en toda la actividad de los servicios de inteligencia, y se manifiesta especialmente en el trabajo del analista a la hora de proyectar las tendencias actuales hacia el futuro: de realizar estimaciones o determinar la probabilidad de ocurrencia de eventos particulares (Lefebvre, 2004). Por otro lado, la incertidumbre se relaciona con lo que Lowenthal (1993) denomina "la lucha contra lo increíble", es decir, la dificultad para el analista de llegar a través del análisis a conclusiones que le resultan increíbles, dada su incapacidad de liberarse de sus creencias sobre el funcionamiento del mundo y de la conducta humana (Montero, 2004). De este modo, lo "increíble" estaría conformado por todos aquellos supuestos, circunstancias o acon-

4 Con frecuencia, los servicios de inteligencia son responsabilizados de determinados errores que, en realidad, han sido provocados por la acción o inacción de los decisores políticos. Esto ha llevado a determinados autores a distinguir entre errores o fallos de inteligencia *per se* y errores cometidos por los políticos (Marrin, 2004).

tecimientos que, aunque siendo factibles o plausibles, aparecen como inimaginables e inconcebibles para el analista.

Por otra parte, la información que se maneja en inteligencia presenta determinadas características que pueden afectar la calidad del análisis, convirtiéndose en potenciales fuentes de error. Hace más de cincuenta años, Sherman Kent (1964) ya advertía de la dificultad que suponía para el análisis de inteligencia tanto la *carencia de información* como su *exceso.*

Con frecuencia, se ha responsabilizado a la falta de información de la ocurrencia de determinados fallos en el análisis. Sin embargo, este argumento no es siempre acertado, pues, a menudo, es el propio analista el que, llegado un momento, decide, equivocadamente, que ya dispone de información suficiente para llegar a sus juicios y conclusiones (Heuer, 1999). Pero igual de preocupante resulta el *exceso de información,* un problema que hoy se ha acentuado debido a la proliferación de múltiples y variadas fuentes de información (fuentes abiertas, OSINT; fuentes humanas, HUMINT; inteligencia de señales, SIGINT; inteligencia de comunicaciones, COMINT, etc.).

Esto lleva a revisar otras características de la información, como su *diversidad* y su frecuente *falta de fiabilidad*, que se relacionan directamente con, por ejemplo, el empleo de fuentes no contrastadas, la carencia de herramientas analíticas para evaluar la fiabilidad de la información, ciertas tendencias psicológicas que llevan a otorgar validez a determinada información en detrimento de otra (sesgo de confirmación, asimilación de información a esquemas y modelos mentales) y el empleo, por parte del adversario, de tácticas de decepción (engaño, desinformación, negación).

Finalmente, cabe resaltar el *carácter sensible* (clasificado, confidencial o secreto) de buena parte de la información obtenida y utilizada por los servicios de inteligencia, lo que restringe su circulación y difusión interna (G. Díaz, 2005). Este carácter sensible proviene tanto de la necesidad de proteger a las fuentes y métodos de obtención de información como de garantizar su seguridad interna y evitar su posible fuga hacia el exterior. Al respecto, los fallos al proteger la información clasificada a menudo se encuentran en el origen de numerosos fallos de inteligencia (G. Díaz, 2005). Desgraciadamente, ni la máxima seguridad ni las comprobaciones más rigurosas pueden evitar que se produzcan fugas y filtraciones (como ocurrió en el conocido caso de WikiLeaks).

La dificultad para proteger la información clasificada se relaciona, entre otros factores, con ciertos defectos de los procesos de reclutamiento del personal de los servicios de inteligencia: en concreto, con la ausencia de instrumentos de selección completamente fiables e infalibles (test psicológicos, técnicas de perfilado psicológico o polígrafos) que permitan seleccionar al personal con total certeza de que no supondrá un riesgo para el servicio de inteligencia y la seguridad nacional. A ello se añade una multitud de factores —incluidos los personales, económicos e ideológicos, así como la coacción y la venganza— que dificultan las comprobaciones y evaluaciones de seguridad y que pueden llevar a una persona a traicionar a la institución y a su país.

Por otra parte, hay que tener en cuenta que no todas las fugas de información se deben a la acción de traidores o infiltrados. Los Gobiernos y los propios servicios de inteligencia pueden filtrar información de forma intencional, con el objetivo, por ejemplo, de calibrar a la opinión pública o de confundir y engañar al adversario (Hulnick, 2002).

Por último, es necesario recordar que toda actividad de inteligencia se desarrolla en un contexto de tensión o confrontación entre partes, generalmente organizaciones o Gobiernos, en el que cada una de ellas pone en marcha una serie de estrategias y medidas para contrarrestar la acción de la otra (Berkowitz, 2003; Shulsky & Schmitt, 2002).

Además, uno de los objetivos de todo organismo de inteligencia es el estudio de sus potenciales adversarios, para obtener una ventaja sobre ellos y poder anticiparse a los acontecimientos. Esta dinámica lo obliga, a su vez, a protegerse de la acción de los servicios de inteligencia adversarios, para impedir que estos conozcan sus propios planes e intenciones y puedan, también, anticiparse a ellos. Esto se consigue básicamente de dos modos: aumentando la seguridad interna y poniendo en marcha medidas de decepción o engaño intencional, mediante la manipulación de la información, a fin de inducir conclusiones erróneas en el adversario. La decepción incluye básicamente dos tipos de acciones: la negación y la desinformación.

La negación tiene como objetivo proteger secretos mediante la ocultación, camuflaje y otras actividades que entorpecen los sistemas de obtención de información del adversario. La desinformación consiste en proporcionar al adversario información parcial o totalmente falsa, recurriendo para ello a actividades como la elaboración y difusión de información falsa, la manipulación de los medios de comunicación y de los canales diplomáticos o el uso de dobles agentes. El uso de tácticas de decepción por parte del adversario se convierte, de esta manera, en la causa de determinados fallos de inteligencia (G. Díaz, 2005; Marrin, 2004; Whaley, 1973)[5].

Los fallos son normales en los sistemas complejos

Esta premisa se basa en la teoría de los accidentes normales *(normal accident theory)*, desarrollada a partir de los estudios de Charles Perrow (1984). Según este autor, los accidentes son inevitables en los sistemas complejos debido a que son sistemas altamente interconectados, interactivos y acoplados, lo que hace altamente probable la ocurrencia y suma de pequeños errores imposibles de prever. Por lo tanto, cuanto más complejo es un sistema,

5 Un ejemplo emblemático del empleo de tácticas de decepción para manipular las percepciones del adversario sobre las propias capacidades e intenciones lo constituye la operación Barbarroja (1940). Los días previos al ataque alemán, los rusos disponían de suficiente información que alertaba sobre la concentración de tropas de la Wehrmacht cerca de sus fronteras y sobre el aumento de vuelos de reconocimiento de la Luftwaffe sobre su territorio. Del mismo modo, la inteligencia estadounidense le había advertido insistentemente a los rusos sobre las intenciones de Hitler. En respuesta, los alemanes pusieron en marcha varias tácticas de decepción: justificaron dichos preparativos militares, primero, afirmando que tenían como objetivo preparar la invasión de Inglaterra y, luego, que se trataba de una medida disuasoria ante un posible ataque soviético (O'Connor, 2012).

mayor es la probabilidad de que se produzcan fallos y accidentes. Y, por supuesto, los servicios de inteligencia son sistemas complejos.

Desde esta perspectiva, los servicios y comunidades de inteligencia, en cuanto sistemas complejos que son, están sometidos a la acción de múltiples factores que impiden prever y evitar la ocurrencia de errores. En ese sentido, los fallos de inteligencia serían, en buena parte, resultado de ciertas disfunciones organizacionales, entre ellas las patologías burocráticas propias de los sistemas de inteligencia (Berkowitz & Goodman, 2000; Betts, 2002; Brady, 1993; Cremades-Guisado & Cancelado-Franco, 2021; Laqueur, 1985; Lefebvre, 2004; Lowenthal, 2000; Marrin, 2003; Reynolds, 2004; Travers, 1997). Entre estas patologías se encuentran la anacronía y caducidad del modelo estructural de los servicios de inteligencia, basado en una concepción de la inteligencia propia de la Guerra Fría. Este modelo se caracteriza por presentar unas estructuras excesivamente grandes, compartimentadas y rígidas, completamente inadecuadas para enfrentarse a la naturaleza flexible, difusa y asimétrica de las nuevas amenazas del siglo XXI, encabezadas por el terrorismo internacional (Martínez-Sánchez & Rodríguez, 2019). Otra patología organizacional es su excesiva burocratización, derivada de la existencia de numerosos niveles jerárquicos y directivos y que dificulta su funcionamiento en todos los niveles del ciclo de inteligencia (Russell, 2004).

La implantación de determinadas políticas de personal es otra causa de numerosos fallos. Los recortes presupuestarios y la consiguiente reducción de recursos económicos, derivados del cambio de panorama estratégico tras la Guerra Fría, llevaron a una notable reducción del personal de la mayoría de servicios de inteligencia occidentales y a una consecuente carencia de profesionales especializados, sobre todo traductores y analistas[6]. Poco ayudaron a suplir esta carencia las políticas de reclutamiento, caracterizadas por estrictos requisitos de seguridad que ralentizan la contratación de nuevo personal (Betts, 2002; Russell, 2004). Otros problemas de estas políticas de personal son los criterios de asignación de destinos y distribución de analistas, así como su excesiva rotación en distintas áreas geográficas y funcionales (Lefebvre, 2004; Marrin, 2003).

La cultura organizacional o personalidad corporativa es otro ingrediente que contribuye a los fallos, al condicionar la actuación de sus miembros. Esta personalidad corporativa se caracteriza por una fuerte identidad policial o militar, una excesiva dependencia de los hechos a la hora de interpretar la realidad y cierta actitud conservadora y excesivamente cautelosa en su actuación, todo lo cual penaliza la iniciativa y capacidad de innovación (Montero, 2004).

6 Al respecto, resulta llamativa la situación reportada por Russell (2004): en septiembre de 2001, el Centro de Contraterrorismo (Counterterrorism Center) de la CIA disponía de mayor cantidad de directivos que de analistas.

Finalmente, podemos señalar la excesiva especialización y compartimentación de las comunidades y agencias de inteligencia[7]. En primer lugar, porque esta necesariamente requiere una elevada dosis de coordinación y cooperación entre agencias que, como ha demostrado la experiencia reciente, no siempre se consigue. En segundo lugar, porque la fragmentación conduce irremediablemente a una disminución de las capacidades de análisis de las diferentes agencias (Betts, 1978). Estas circunstancias dan lugar a una grave carencia de integración o congruencia de la información que recibe el decisor político desde distintas agencias de inteligencia, lo que le impide armonizar diversos puntos de vista y disponer así de una perspectiva global con base en la cual actuar en consecuencia (Travers, 1997).

Evitar los fallos de inteligencia, ¿una batalla perdida?

Como se ha insistido, los fallos de inteligencia son inevitables. Sin embargo, es posible minimizar su ocurrencia mediante la adopción de diversas estrategias y medidas. Un primer paso es aceptarlos y asumirlos como algo inherente a la naturaleza de la inteligencia. Creer que los fallos son predecibles y evitables denota un desconocimiento total de la naturaleza y las funciones de los servicios de inteligencia. En consecuencia, productores y consumidores de inteligencia deben aprender a conocerlos, identificarlos y, en última instancia, a convivir con ellos para que afecten lo mínimamente posible la calidad de su trabajo. Esto les exige tanto a la comunidad de inteligencia como a su personal desarrollar altas dosis de autorreflexión, autocrítica y capacidad de aprender de sus errores y fracasos a través del análisis detallado de su naturaleza, causas y consecuencias.

Pero no solo se requiere comprender los fallos cometidos. También resulta indispensable avanzar en el estudio académico de los éxitos y aciertos, a fin de determinar qué elementos o factores están presentes en ellos y marcan la diferencia entre el éxito y el fracaso. Sin embargo, esta práctica se ve obstaculizada por el hecho inconveniente de que, al contrario de lo que sucede con la información sobre fallos y fracasos (que termina siendo pública), los servicios de inteligencia se muestran muy reticentes a compartir públicamente las claves de sus éxitos para no comprometer sus fuentes y métodos (Marrin, 2004).

En todo caso, la principal estrategia para minimizar la ocurrencia de fallos y errores pasa por la implantación de una serie de medidas y acciones a lo largo de todas las fases del ciclo de inteligencia.

En la *fase de dirección o planeamiento*, es imprescindible aumentar el conocimiento que poseen los decisores (políticos y militares) sobre las posibilidades y limitaciones del trabajo de los servicios y agencias de inteligencia (George, 2004; Heuer, 1999). Fundamental resulta también estrechar las relaciones existentes entre los servicios de inteligencia y los

7 Por poner un ejemplo ilustrativo, la comunidad de inteligencia estadounidense está formada actualmente por 17 agencias o elementos. Al respecto, véase https://www.intelligencecareers.gov/icmembers.html

consumidores de sus productos, especialmente la clase política (Berkowitz, 2001; A. Díaz, 2006; Marrin, 2004; Navarro, 2004). Esto les permitiría a los consumidores transmitirles de manera clara y directa cuáles son sus necesidades específicas, en lo que Marrin (2004, p. 668) ha denominado "un mayor énfasis en la atención al cliente" como medio de reducir la frecuencia de fallos y errores. Esta mayor relación e interacción entre productores y consumidores de inteligencia les facilita a los primeros poseer retroalimentación sobre el valor y la eficacia de su trabajo, para poder reorientarlo si es necesario. Todo ello sin descuidar los posibles inconvenientes de estrechar las relaciones entre ambos sectores: fundamentalmente el riesgo de injerencia de la inteligencia en política y de los políticos en inteligencia, es decir, el riesgo de politización.

En la *fase de obtención de información*, es fundamental gestionar adecuadamente el elevado volumen de datos con los que trabajan los servicios y agencias de inteligencia, a fin de perfeccionar los procesos de selección, clasificación, almacenamiento y recuperación de la información obtenida. Ello pasa por la mejora de los métodos de obtención y gestión de información procedente de fuentes abiertas (OSINT), así como por el impulso y potenciación de las fuentes humanas (HUMINT), imprescindibles e insustituibles en la lucha contra las nuevas amenazas, como el terrorismo internacional.

Finalmente, quizás sea la *fase de análisis* en la que más se ha incidido con el objetivo de mejorar la calidad de los productos de inteligencia. En esta fase se han hecho grandes avances, tanto en la mejora de la formación y capacitación de los analistas como en el desarrollo e implantación de técnicas estructuradas para el análisis de inteligencia y el control de sesgos psicológicos (Heuer & Pherson, 2011).

Sin embargo, las principales reformas se han producido a nivel institucional, mediante la reestructuración y reorganización de las agencias de inteligencia para adaptarlas a los nuevos riesgos y amenazas del siglo XXI (Shulsky & Schmitt, 2002). En esta línea, se ha propuesto la adopción de estructuras basadas en modelos empresariales, mucho más dinámicos, adaptables y flexibles (A. Díaz, 2006).

Además, un mejor funcionamiento de los servicios de inteligencia pasa necesariamente por el control y gestión de ciertas tendencias organizacionales: el fomento de la cooperación y coordinación (no solo dentro y entre las agencias de una misma comunidad de inteligencia, sino también a nivel internacional), y la eliminación de las excesivas barreras burocráticas, jerárquicas y de seguridad que condicionan su actividad (Berkowitz, 2001).

En aspectos de cooperación, se ha destacado la importancia de impulsar el concepto de *comunidad de inteligencia* en sentido amplio, para que incluya la participación y colaboración de organismos e instituciones públicas y privadas, tales como universidades, institutos académicos y centros de pensamiento *(think tanks)* (Berkowitz & Goodman, 2000).

No obstante, y como señala Hedley (2005), la introducción de reformas y supuestas mejoras no garantiza siempre la adecuada calidad del producto final. Las reformas tardan años en aplicarse y, cuando finalmente se implantan, siempre surgen críticos que deman-

dan nuevas reformas y cambios (Laqueur, 2004). Además, su introducción a menudo ocasiona nuevas patologías y disfunciones que aumentan el riesgo de nuevos futuros fallos y errores (Marrin, 2004).

Conclusión

Los errores y fallos de inteligencia son inevitables. Esta irrefutable afirmación, utilizada a menudo por productores y consumidores de inteligencia como excusa para justificar sus errores y fracasos, esconde una compleja realidad: estos fallos han ocurrido y seguirán ocurriendo en el futuro, a pesar de los múltiples esfuerzos de la comunidad de inteligencia para prevenirlos. Aceptar que son inevitables constituye el primer paso para disminuir su incidencia y combatir y minimizar sus efectos y consecuencias.

Desde un punto de vista psicosocial, dicha inevitabilidad deriva de distintos factores y circunstancias. Por un lado, la intervención del ser humano, complejo y falible, en todas las fases del ciclo de inteligencia. Por otro, la complejidad de los servicios y agencias de inteligencia, así como de los fenómenos a los que se enfrentan, en un contexto dominado por la incertidumbre, la ambigüedad y la necesidad de operar con información imperfecta: a veces escasa, a veces excesiva, pero casi siempre de escasa fiabilidad.

Estos factores, al no ser enfrentados, pueden originar defectos en los procesos de obtención, procesamiento y análisis de la información que se traducen, a menudo, en informes de inteligencia incorrectos que, a su vez, provocan que los decisores políticos y militares tomen decisiones inapropiadas. A ello hay que añadir la responsabilidad de los decisores cuando utilizan de manera inadecuada (rechazando, ignorando o malinterpretando) la inteligencia correcta que se les proporciona.

La certeza de que los fallos son inevitables no debe servir de excusa para que productores y consumidores de inteligencia justifiquen sus errores y, sobre todo, las consecuencias que estos acarrean. Asumir que los fallos son inherentes a los procesos y ciclos de inteligencia no debe llevar a una visión extremadamente negativa y pesimista de la prevención de futuros fracasos y amenazas para la seguridad.

Sería utópico esperar que los servicios de inteligencia sean capaces de predecir o impedir todas y cada una de las acciones del adversario (lo que habría impedido atentados terroristas como los del 11 de septiembre de 2001 en Estados Unidos, los del 11 de marzo de 2004 en Madrid o los del 14 de julio de 2016 en Niza, Francia)[8]. Pero ello no es impedimento para hacer todo lo posible para evitarlos o, cuando menos, para minimizar la probabilidad de su ocurrencia y la magnitud de sus efectos. Este es uno de los grandes

8 Cuatro años antes de los atentados del 11-S, Russ Travers (1997) anunciaba premonitoriamente, en un artículo de sugerente título ("A blueprint for survival: The coming intelligence failure"), que, pese a los esfuerzos de la comunidad de inteligencia por explicar sus fallos, esta iba a seguir cometiendo cada vez más y mayores errores de inteligencia: algunos de ellos tan graves que su eficacia se iba ver seriamente cuestionada, mucho más de lo que lo había sido hasta el momento. El tiempo acabaría por darle la razón.

retos de la comunidad de inteligencia: minimizar la ocurrencia y el impacto negativo de sus fallos y aumentar al máximo el impacto positivo de sus productos en la formulación de políticas y toma de decisiones (Marrin, 2004).

A este fin, son muchos los autores que han señalado la necesidad de introducir mejoras en los servicios y agencias de inteligencia y en la calidad de sus análisis (Betts, 1978; Hedley, 2005; Marrin, 2004). Al respecto, los numerosos cambios introducidos en la mayoría de las comunidades de inteligencia occidentales en lo que llevamos de siglo han incluido profundas reformas estructurales, un aumento significativo de nuevo personal, un mayor énfasis en la calidad de los procesos de obtención, procesamiento y análisis de información y un esfuerzo considerable para fomentar la cooperación y la coordinación (tanto a nivel interno como externo; tanto a nivel nacional como internacional).

En todo caso, como han señalado Betts (2002) y Hedley (2005), hay que tener presente siempre que ni el estudio en profundidad de los grandes errores de inteligencia cometidos a lo largo de la historia ni las múltiples reformas introducidas a raíz de estos podrán impedir la ocurrencia de futuros fallos. Efectivamente, un mejor funcionamiento de los servicios y agencias de inteligencia puede conducir a un aumento de los éxitos y por consiguiente, a una disminución de los fallos; pero la perfección es inalcanzable en inteligencia, y al final estos ocurrirán. Ahí radica la inevitabilidad de los fallos de inteligencia.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

El autor no declara fuente de financiamiento para la realización de este artículo.

Sobre el autor

Juan Antonio Martínez-Sánchez es militar activo, doctorando en Ciencias Jurídicas y Sociales de la Universidad de Cádiz, y licenciado en psicología por la Universidad de Sevilla. Sus principales líneas de investigación son la psicología militar operativa y los aspectos psicológicos del análisis de inteligencia.

https://orcid.org/0000-0002-7696-5023 - Contacto: jamartsan@ea.mde.es

Referencias

Berkowitz, B. (2001). Better ways to fix U.S. intelligence. *Orbis, 45*(4), 609-619. http://dx.doi.org/10.1016/S0030-4387(01)00099-0

Berkowitz, B. (2003, 2 de febrero). The big difference between intelligence and evidence. *The Washington Post*. https://bit.ly/3xKMzL7

Berkowitz, B., & Goodman, A. (2000). *Best truth: Intelligence in the information age*. Yale University Press.

Betts, R. (1978). Analysis, war and decision: Why intelligence failures are inevitable. *World Politics, 31*(1), 61-89. http://dx.doi.org/10.2307/2009967

Betts, R. (2002). Fixing intelligence. *Foreign Affairs, 81*(1), 43-59. http://dx.doi.org/10.2307/20033002

Betts, R. (2007). *Enemies of intelligence. Knowledge and power in American national security*. Columbia University Press.

Brady, C. (1993). Intelligence failures: Plus ça change. *Intelligence and National Security, 4*(8), 86-96. https://doi.org/10.1080/02684529308432227

Corera, G. (2004, 9 de julio). CIA shoulders the blame. *BBC News*. https://bbc.in/3S5u1xm

Cremades-Guisado, A., & Cancelado-Franco, H. (2021). La inteligencia como organización burocrática: disfunciones del modelo weberiano. *Revista Científica General José María Córdova, 19*(34), 479-496. https://doi.org/10.21830/19006586.701

Díaz Fernández, A. M. (2006). *El papel de la comunidad de inteligencia en la toma de decisiones de la política exterior y de seguridad de España* (Documento de Trabajo n.º 3). Observatorio de Política Exterior Española, Fundación Alternativas. https://bit.ly/3S8tN8q

Díaz Fernández, A. M. (Coord.) (2013). *Diccionario LID Inteligencia y Seguridad.* LID Editorial Empresarial; Presidencia del Gobierno de España.

Díaz Matey, G. (2005) Methodological approaches to the concept of intelligence failure. *UNISCI Discussion Papers, 7*. https://bit.ly/3SpvD4O

Díaz Matey, G. (2017), *La esencia de la inteligencia: hacia una correcta relación entre producción y consumo de inteligencia* (Documento de Opinión n.º 52). Instituto Español de Estudios Estratégicos. https://bit.ly/3r0nOqt

Duffy, M. (2003, 27 de julio). Could it happen again? *Time*. https://bit.ly/3BET2bJ

Esteban N., M., & Navarro B., D. (2003). Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información. *El Profesional de la Información, 12*(4), 269-281. https://bit.ly/3qYZTrx

George, R. (2004). Fixing the problem of analytical mind-sets: alternative analysis. *International Journal of Intelligence and Counterintelligence, 17*(3),385-404.http://dx.doi.org/10.1080/08850600490446727

Handel, M. I. (1977). The Yom Kippur War and the inevitability of surprise. *International Studies Quarterly, 21*(3), 461-502. https://doi.org/10.2307/2600234

Handel, M. I. (1984). Intelligence and the problem of strategic surprise. *Journal of Strategic Studies, 7*(3), 229-281. https://doi.org/10.1080/01402398408437190

Hedley, J. (2005). Learning from intelligence failures. *International Journal of Intelligence and CounterIntelligence, 18*(3), 435-450. https://doi.org/10.1080/08850600590945416

Herman, M. (1996). *Intelligence power in peace and war.* Cambridge University Press.

Heuer, R. (1999). *Psychology of intelligence analysis*. Central Intelligence Agency.

Heuer, R. (2005). Limits of intelligence analysis. *Orbis, 49*(1), 75-94. https://doi.org/10.1016/j.orbis.2004.10.007

Heuer, R. (2008). *Small group processes for intelligence analysis*. Central Intelligence Agency; Sherman Kent School.

Heuer, R., & Pherson, R. (2011). *Structured analytic techniques for intelligence analysis*. CQ Press.

Hulnick, A. (2002). The downside of open source intelligence. *International Journal of Intelligence and Counterintelligence, 15*(4), 565-579. https://doi.org/10.1080/08850600290101767

Johnson, L. (2006). A framework for strengthening U.S. intelligence. *Yale Journal of International Affairs, 1*(2), 116-131. https://bit.ly/3Siqv2i

Kent, S. (1964). A crucial estimate relived. *Studies in Intelligence, 8*(4), 1-18. https://bit.ly/3SiqBqG

Kuhns, W. J. (2003). Intelligence failures: Forecasting and the lessons of epistemology. En R. Betts & T. Mahnken (Eds.), *Paradoxes of strategic intelligence: Essays in honor of Michael I. Handel* (pp. 77-96). Routledge. https://doi.org/10.4324/9780203508640

Laqueur, W. (1985). *A world of secrets: Uses & limits of intelligence*. Basic Books.

Laqueur, W. (2003). *La guerra sin fin: el terrorismo en el siglo XXI*. Destino.

Laqueur, W. (2004, 15 de junio). Las desgracias de la CIA. *La Vanguardia*. https://bit.ly/3BBiuih

Lefebvre, S. (2004). A look at intelligence analysis. *International Journal of Intelligence and Counterintelligence, 17*(2), 231-264. https://doi.org/10.1080/08850600490274908

Lowenthal, M. (1985). The burdensome concept of failure. En A. C. Maurer, M. Tunstall, & J. Keagle (Eds.), *Intelligence: Policy and process* (pp. 43-56). Westview Press.

Lowenthal, M. (1993). Intelligence epistemology: Dealing with the unbelievable. *International Journal of Intelligence and Counterintelligence, 6*(3), 319-325. https://doi.org/10.1080/08850609308435222

Lowenthal, M. (2000). *Intelligence: From secrets to policy*. Congressional Quarterly Press.

Marrin, S. (2003). CIA's Kent School: Improving training for new analysts. *International Journal of Intelligence and CounterIntelligence, 16*(4), 609-637. https://doi.org/10.1080/716100469

Marrin, S. (2004). Preventing intelligence failures by learning from the past. *International Journal of Intelligence and CounterIntelligence, 17*(4), 655-672. https://doi.org/10.1080/08850600490496452

Martínez-Sánchez, J. A. (2014). Psicología e Inteligencia: factores psicológicos que condicionan el análisis de inteligencia. En F. Velasco, y R. Arcos (Eds.), *Estudios en inteligencia: respuestas para la Gobernanza democrática* (pp. 181-202). Plaza y Valdés.

Martínez-Sánchez, J. A. (2016). Fallo de Inteligencia. En A. M. Díaz Fernández (Dir.), *Conceptos fundamentales de inteligencia* (pp. 183-190). Tirant lo Blanch.

Martínez-Sánchez, J. A., & Rodríguez G., J. M. (2019). *Patologías organizacionales y fallos de inteligencia* (Análisis GESI, 10). https://bit.ly/3DOVuPt

Montero, A. (2004). Psicología del terrorismo e inteligencia contraterrorista. *Papeles del Psicólogo, 25*(88), 39-47. http://www.papelesdelpsicologo.es/resumen?pii=1158

Navarro B., D. (2004). Introducción. *Cuadernos de Estrategia, 127*, 7-31. Instituto Español de Estudios Estratégicos.

O'Connor, T. (2012). *The history and lessons of intelligence failure*. Austin Peay State University. https://bit.ly/3LAdqze

Perrow, C. (1984). *Normal accident: Living with high-risk technology.* Basic Books.

Poteat, G. H. (1976).The intelligence gap: Hypotheses on the process of surprise. *International Studies Notes, 3*(3), 14-18. https://www.jstor.org/stable/44235762

Random, R. A. (1958). Intelligence as a science. *Studies in Intelligence, 2*(2), 75-79. https://bit.ly/3BI1cQi

Reynolds, P. (2004, 11 de julio). Long history of intelligence failures. *BBC News*. https://bbc.in/3LFUmje

Russell, R. L. (2004). Intelligence failures: The wrong model for the war on terror. *Policy Review, 123*, 61-72.

Shulsky, A, & Schmitt, G. (2002). *Silent warfare: Understanding the world of intelligence* (3rd ed.). Potomac Books Inc.

Steele, R. (2002, 11 de marzo). The new craft of intelligence: Making the most of open private sector knowledge. *Time Magazine*. https://bit.ly/3C3ER13

Stempel, J. (1999). Error, folly, and policy intelligence. *International Journal of Intelligence and CounterIntelligence, 12*(3), 267-281. https://doi.org/10.1080/088506099305034

Taleb, N. (2007). *The black swan: The impact of the highly improbable*. Random House.

Travers, R. (1997). A blueprint for survival: The coming intelligence failure. *Studies in Intelligence, 40*(5), 35-43. https://bit.ly/3BHvq64

Treverton, G. (2001). *Reshaping national intelligence for an age of information*. Cambridge University Press.

United States Senate Select Committee on Intelligence (2004, 9 de julio). *Report of the Select Committee on Intelligence on the intelligence community's prewar intelligence assessments on Iraq* (S. Report n.º 108-301). U.S. Government Printing Office.

Westerfield, H. B. (1996). Inside ivory bunkers: CIA analysts resist manager's "pandering". Part I. *International Journal of Intelligence and Counterintelligence, 9*(4), 407-424. https://doi.org/10.1080/08850609608435325

Whaley, B. (1973). *Code Word Barbarrosa.* The MIT Press.

Wohlstetter, R. (1962). *Pearl Harbor: Warning and decision*. Stanford University Press.