

COMITÉ CIENTÍFICO DE LA EDITORIAL TIRANT LO BLANCH

- | | |
|---|---|
| MARÍA JOSÉ AÑÓN ROIG
<i>Catedrática de Filosofía del Derecho de la
Universidad de Valencia</i> | VÍCTOR MORENO CATENA
<i>Catedrático de Derecho Procesal de la
Universidad Carlos III de Madrid</i> |
| ANA BELÉN CAMPUZANO LAGUILLO
<i>Catedrática de Derecho Mercantil de la
Universidad CEU San Pablo</i> | FRANCISCO MUÑOZ CONDE
<i>Catedrático de Derecho Penal de la
Universidad Pablo de Olavide de Sevilla</i> |
| JORGE A. CORDO HERRÁN
<i>Catedrático de Teoría y Filosofía de
Derecho. Instituto Tecnológico
Autónomo de México</i> | ANGELIKA NUSSBERGER
<i>Jueza del Tribunal Europeo de Derechos Humanos
Catedrática de Derecho Internacional de la Universidad de
Colonia (Alemania)</i> |
| JOSÉ RAMÓN COSSÍO DÍAZ
<i>Ministro de la Suprema Corte de Justicia de México</i> | HÉCTOR OLASOLO ALONSO
<i>Catedrático de Derecho Internacional de la Universidad
del Rosario (Colombia) y Presidente del Instituto Ibero-
Americano de La Haya (Holanda)</i> |
| OWEN M. FISS
<i>Catedrático emérito de Teoría del Derecho de la
Universidad de Yale (EEUU)</i> | LUCIANO PAREJO ALFONSO
<i>Catedrático de Derecho Administrativo de la
Universidad Carlos III de Madrid</i> |
| LUIS LÓPEZ GUERRA
<i>Juez del Tribunal Europeo de Derechos Humanos
Catedrático de Derecho Constitucional de la
Universidad Carlos III de Madrid</i> | TOMÁS SALA FRANCO
<i>Catedrático de Derecho del Trabajo y de la
Seguridad Social de la Universidad de Valencia</i> |
| ÁNGEL M. LÓPEZ Y LÓPEZ
<i>Catedrático de Derecho Civil de la
Universidad de Sevilla</i> | JOSÉ IGNACIO SANCHE GARGALLO
<i>Magistrado de la Sala Primera (Civil) del
Tribunal Supremo de España</i> |
| MARTA LORENTE SARIÑENA
<i>Catedrática de Historia del Derecho de la
Universidad Autónoma de Madrid</i> | TOMÁS S. VIVES ANTÓN
<i>Catedrático de Derecho Penal de la Universidad de Valencia</i> |
| JAVIER DE LUCAS MARTÍN
<i>Catedrático de Filosofía del Derecho y Filosofía Política de
la Universidad de Valencia</i> | RUTH ZIMMERLING
<i>Catedrática de Ciencia Política de la
Universidad de Mainz (Alemania)</i> |

CONCEPTOS FUNDAMENTALES DE INTELIGENCIA

Director
ANTONIO M. DÍAZ FERNÁNDEZ

Con la colaboración



tirant lo blanch

Valencia, 2016

Procedimiento de selección de originales, ver página web:

www.tirant.net/index.php/editorial/procedimiento-de-seleccion-de-originales

Copyright * 2016

Todos los derechos reservados. Ni la totalidad ni parte de este libro puede reproducirse o transmitirse por ningún procedimiento electrónico o mecánico, incluyendo fotocopia, grabación magnética, o cualquier almacenamiento de información y sistema de recuperación sin permiso escrito de los autores y del editor.

En caso de erratas y actualizaciones, la Editorial Tirant lo Blanch publicará la pertinente corrección en la página web www.tirant.com.

Director de la colección:
JOSÉ LUIS GONZÁLEZ CUSSAC
Universidad de Valencia

© Antonio M. Díaz Fernández

© TIRANT LO BLANCH
EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELF.S.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email: tlb@tirant.com
www.tirant.com
Librería virtual: www.tirant.es
DEPÓSITO LEGAL: V-287-2016
ISBN: 978-84-9119-314-2
IMPRIME: Guada Impresores, S.L.
MAQUETA: Tink Factoría de Color

Si tiene alguna queja o sugerencia, envíenos un mail a: atencioncliente@tirant.com. En caso de no ser atendida su sugerencia, por favor, lea en www.tirant.net/index.php/empresa/politicas-de-empresa nuestro Procedimiento de quejas.

FALLO DE INTELIGENCIA

EN: intelligence failure

FR: erreur de renseignement

PT: falha de inteligência

Aunque el término error, fallo o fracaso de inteligencia es utilizado frecuentemente en el ámbito de la seguridad y defensa, no siempre aparece claramente definido. A ello ha contribuido, en buena medida, la falta de acuerdo entre autores e investigadores para consensuar cuándo se ha producido un error de inteligencia. Generalmente se considera que existe un error de inteligencia cuando de él derivan graves amenazas o consecuencias negativas para la seguridad de un país concreto o de toda la comunidad internacional. Sin embargo, a menudo se abusa del término error para describir situaciones con escasas repercusiones para la seguridad, de modo que cualquier acontecimiento inesperado e indeseado para la seguridad de un país puede ser calificado como fallo de sus servicios de inteligencia (Hollister, 2005). Otro factor que dificulta una adecuada definición del concepto es la tendencia generalizada a identificar los errores de inteligencia con las causas que los producen (por ejemplo, la politización de la inteligencia) o incluso con sus efectos (como es el caso de la sorpresa estratégica).

A pesar de lo anterior, se pueden citar algunas definiciones certeras de fallo o error de inteligencia. Según Lowenthal (1958), error de inteligencia es "la incapacidad de una o más partes del ciclo de inteligencia para producir inteligencia oportuna y fiable de un problema o evento 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 del error, al definirlo como "cualquier malentendido de una situación que lleva a un gobierno o a sus fuerzas militares a tomar acciones inadecuadas y contraproducentes para sus propios intereses". Finalmente, el *Diccionario de Inteligencia y Seguridad* integra las definiciones anteriores al considerar que fallo de inteligencia es aquella situación no deseada por el decisor político o militar que puede ocurrir en diferentes momentos del ciclo de inteligencia y que se produce por la incapacidad de la comunidad de

inteligencia para proporcionar inteligencia adecuada o por la inoperancia del propio decisor a la hora de aceptar las alertas de aquella (Díaz, 2013).

Una buena manera de aproximarnos al concepto de error de inteligencia es la consideración de los principales rasgos o características que definen su naturaleza, como son su diversidad, su etiología multicausal, sus consecuencias negativas para la seguridad nacional y la inevitabilidad de su ocurrencia.

La *diversidad* de este tipo de error lleva a la necesidad de elaborar una taxonomía apropiada de cara a su estudio, comprensión y, sobre todo, prevención. Una perspectiva tradicional consiste en clasificarlos en función de la fase del ciclo de inteligencia en que se producen, de modo que podría hablarse de errores en la fase de dirección, de obtención de información, en el proceso de integración y análisis y, finalmente, en la difusión de resultados (Martínez Sánchez, 2010). Por su parte y basándose en la taxonomía de errores realizada desde el ámbito empresarial, Hatch (2013) aporta un nuevo enfoque, al clasificar los errores de inteligencia en tres categorías: cognitivos, organizacionales y relacionados con el entorno político de seguridad. Entre los errores cognitivos se encontrarían los derivados de los sesgos cognitivos y del empleo de modelos mentales (*mind-sets*), la dificultad para enfrentarse a la naturaleza dinámica y cambiante de los fenómenos sociales, las limitaciones a la hora de plantear escenarios alternativos y la dificultad para distinguir entre lo relevante (señales) y lo accesorio (ruido).

Por su parte, los errores organizacionales se producen dentro de los servicios y agencias de inteligencia, tanto a nivel de sistemas como de procesos, e incluyen el *group-think* o pensamiento grupal, la excesiva burocracia y jerarquía, los causados por limitaciones de recursos materiales y humanos, los derivados de la falta de comunicación intra e inter agencias y las consecuentes restricciones a la hora de compartir información, y aquellos producidos por las limitaciones normativas y legales en la actuación de los servicios de inteligencia. Por último, los errores en el ámbito político se refieren a factores como la presencia de modelos mentales en los consumidores, la dependencia de los políticos de la opinión del electorado, que puede condicionar sus pensamientos y actuaciones en temas de seguridad e inteligencia, las dificultades de relación entre analistas y directivos de

inteligencia y los responsables políticos o ignorar las advertencias proporcionadas por los servicios de inteligencia.

En cuanto a la etiología de los errores de inteligencia, hoy en día se asume que son *múltiples las causas* que influyen en su ocurrencia y que, por tanto, deben analizarse desde la consideración del ciclo de inteligencia como un proceso global en la que cualquier disfunción de alguna de sus fases provoca que el proceso entero deje de funcionar correctamente (Díaz Matey, 2005).

Los fallos y errores de inteligencia suelen conllevar *consecuencias negativas para la seguridad nacional*, caso del fallo de la inteligencia estadounidense para predecir el ataque japonés a Pearl Harbor en 1941, el bombardeo por aviones de la OTAN de la embajada china en Belgrado en mayo de 1999 a causa de la inteligencia errónea suministrada por la CIA, o el desencadenamiento de la invasión de Irak en 2004 a raíz del fiasco de las armas de destrucción masiva. Otras consecuencias importantes de los errores de inteligencia son las críticas y continuas reformas que sufren los servicios y agencias de inteligencia, al ser acusados frecuentemente de ser responsables de su ocurrencia. Baste mencionar a este respecto las importantes reestructuraciones sufridas por buena parte de los servicios, agencias y comunidades de inteligencia occidentales tras los atentados yihadistas del 11 de septiembre de 2001 (Estados Unidos), 11 de marzo de 2004 (Madrid) y 7 de julio de 2005 (Londres).

Pero sin duda es la *inevitabilidad* el principal rasgo definitorio de los errores de inteligencia (Brady, 1993; Marrin, 2004), hasta el punto de que algunos autores afirman que no solo son inevitables sino inherentes a la naturaleza de la inteligencia (Betts, 1978; Hollister, 2005). Esta afirmación se sustenta en varios argumentos. El primero de ellos surge de la aplicación al ámbito de la inteligencia de la *Normal accident theory* (teoría de los accidentes normales) de Charles Perrow (1984). Según Perrow, los accidentes son normales en sistemas y organizaciones complejas, ya que en ellas ocurren pequeños fallos y errores imposibles de prever. Ello se debe fundamentalmente a dos fenómenos que aparecen en este tipo de sistemas y que se denominan *fuerte acoplamiento* y *complejidad interactiva*. El fuerte acoplamiento describe aquella situación en la que un incidente (error) en un elemento o parte de un sistema tiene efectos rápidos e impor-

tantes en otras partes del sistema. La complejidad interactiva implica que varios errores o fallos aislados en un sistema interactúan y producen efectos inesperados en el sistema en su conjunto. Desde esta perspectiva, y como organizaciones complejas que son, las agencias, servicios y comunidades de inteligencia están sometidas a la acción de múltiples factores que impiden prever y evitar la ocurrencia de errores.

A la complejidad sistémica que caracteriza a las organizaciones de inteligencia hay que añadir la confusión que deriva de la naturaleza de los fenómenos a los que se enfrentan (terrorismo internacional, ciberdelincuencia, crimen organizado, etc.); la dificultad de predecir, prever y anticipar acontecimientos políticos y sociales (relaciones internacionales, sorpresas estratégicas, eventos inesperados); las barreras que implica el carácter secreto de la inteligencia, de sus fuentes y actividades; y el peligro que entraña la acción, oposición y actividades de los servicios de inteligencia de otros países adversarios (contrainteligencia y tácticas de decepción).

Un último argumento a favor de la inevitabilidad de los fallos de inteligencia se basa en el hecho de que el error es consustancial a toda actividad humana. El ser humano está presente en todas las fases del ciclo de inteligencia, lo que aumenta la posibilidad de que en ellas se produzcan fallos y errores. De hecho, muchos de los fallos identificados en las fases de dirección, de obtención de información y difusión de inteligencia se relacionan directamente con errores y limitaciones humanas. Sin embargo, es durante el análisis cuando aumenta el riesgo, debido a las limitaciones humanas y psicológicas del analista, como las carencias de formación, conocimientos y experiencia, la influencia de sesgos cognitivos y modelos mentales, limitaciones y fallos en los procesos psicológicos básicos (atención, memoria, pensamiento o emoción) y la influencia de sus factores de personalidad y cualidades personales.

LA SORPRESA ESTRATÉGICA

En el ámbito académico se ha señalado la estrecha relación existente entre error de inteligencia y sorpresa estratégica. El análisis y estudio de acontecimientos calificados históricamente como sorpresas estratégicas

muestra que detrás de ellos suele estar presente algún error de inteligencia (Marrin, 2004). En este sentido se ha citado el empleo de tácticas de *deception* (negación y desinformación) por parte del adversario, como ocurrió en la invasión de Rusia por las tropas alemanas en junio de 1940 (Operación Barbarroja); la incapacidad de la inteligencia estadounidense para distinguir entre la información relevante (señal) y la accesorio (ruido), que favoreció el ataque japonés a Pearl Harbor en 1941; la subestimación de las capacidades militares e intenciones de Egipto y Siria y la elaboración y empleo por las autoridades y analistas de inteligencia israelíes de modelos mentales que impidieron prevenir el ataque árabe a Israel en 1973; el *surprise-imaging*, ejemplificado en el estupor que supuso para los Estados Unidos la invasión de Afganistán por la URSS en 1978; o el fracaso de la comunidad de inteligencia estadounidense para anticiparse y prevenir los ataques terroristas del 11 de septiembre de 2001. Como causa específica de la sorpresa estratégica se ha citado el síndrome *cry wolf*, que se produce cuando las continuas alertas de amenazas provenientes de los servicios de inteligencia generan una especie de fatiga en los decisores políticos y militares, que acaban finalmente ignorando alertas posteriores, absteniéndose de intervenir, incluso cuando esas amenazas están fundadas (Díaz, 2013).

Otros autores van más allá, al considerar que error de inteligencia y sorpresa estratégica son términos equivalentes, llegando incluso a afirmar que los fallos en el ámbito de la inteligencia se llaman *intelligence failures* o *strategic surprises* (Betts, 1982). Dicha equiparación está justificada por diversos factores históricos y políticos, entre los que se encuentra el hecho de que los primeros avances teóricos en el estudio de los errores de inteligencia se realizaron en base al análisis de acontecimientos militares calificados como importantes sorpresas estratégicas, por lo que la confusión era frecuente. Además, la sorpresa es una constante en las relaciones internacionales y ocasionalmente acontecen *eventos espontáneos imprevisibles* que sorprenden a toda la comunidad internacional, como ocurrió con la caída del muro de Berlín en 1989 o las revueltas de la Primavera Árabe de 2010. Uno de los principales objetivos de los servicios y agencias de inteligencia, como órganos asesores de los gobiernos en política exterior, es la anticipación y previsión de acontecimientos importantes para la seguridad nacional, de modo que cuando se produce la sorpresa estratégica se suele hablar de fracaso de los servicios de inteligencia. De la misma manera, al

igual que el error de inteligencia, la sorpresa estratégica es también inevitable ya que la inteligencia proporcionada sobre determinado asunto nunca puede ser completamente perfecta ni estar libre de error o posibles malinterpretaciones. Por último, hay que considerar que, aun conociendo las intenciones ofensivas del enemigo, resulta difícil prever cuándo y cómo se producirá dicho ataque. Acontecimientos como el bombardeo japonés a Pearl Harbor o los más recientes atentados del 11 de septiembre de 2001 así lo demuestran.

¿SE PUEDEN PREVENIR LOS ERRORES DE INTELIGENCIA?

La certeza de que los errores de inteligencia y las sorpresas estratégicas son inevitables podría conducirnos a una visión extremadamente negativa y pesimista en la prevención de futuros fracasos y amenazas para la seguridad. Sin embargo, asumiendo dicha inevitabilidad, desde la comunidad de inteligencia y el ámbito académico se han ofrecido numerosas medidas para minimizar la ocurrencia de este tipo de errores, incluyendo la mejora de la formación, experiencia, capacidades y habilidades profesionales de los analistas, las mejoras tecnológicas en la recogida, procesamiento e integración de la información, el impulso y potenciación de las fuentes humanas (HUMINT) como método de mayor eficacia en la obtención de información, la mejora de las relaciones entre la inteligencia y la política y los numerosos intentos de reestructuración organizacional de los sistemas de inteligencia en busca de una mayor eficacia.

Sin embargo, para Hatch (2013) las medidas anteriores suponen a menudo un aumento de la complejidad de los servicios y agencias de inteligencia, sobrecargando de trabajo tanto a analistas como a directivos de inteligencia, y aumentando la vulnerabilidad de la comunidad de inteligencia al fracaso. Para este autor, la clave de la prevención de los fallos de inteligencia se encuentra en el funcionamiento de las Organizaciones de Alta Fiabilidad (*High Reliability Organizations, HRO's*), propias de ámbitos como la Medicina, la seguridad aérea o las operaciones en centrales nucleares. Este tipo de organizaciones se caracterizan por alcanzar una gran fiabilidad en condiciones dinámicas de incertidumbre, complejidad, alto riesgo y costes potencialmente fatales en caso de fallos y errores.

Dado que los servicios y agencias de inteligencia se enfrentan al reto de obtener y garantizar la máxima fiabilidad posible en su actuación en condiciones similares, Hatch ha propuesto la aplicación de los conocimientos y lecciones aprendidas en el campo de las HRO's al estudio, reflexión y prevención de los errores de inteligencia. En este sentido, la primera cuestión que se plantea es la necesidad de poseer un indicador adecuado para medir la fiabilidad del análisis de inteligencia, proponiendo para ello el concepto de *impacto positivo* sobre la toma de decisiones de los consumidores, mediante la entrega de análisis correctos, útiles, oportunos y en el momento adecuado. Imprescindible resulta también la adopción, a nivel organizacional, de una actitud apropiada ante el error y fracaso, basada no en su negación u ocultación sino en saber reconocerlos, aceptar su ocurrencia e interiorizarlos como medio de anticiparse a ellos y poder prevenirlos o evitarlos.

Como método fundamental para prevenir errores, Hatch propone la aplicación del llamado ciclo de fiabilidad al análisis de inteligencia, compuesto por varias fases, cada una de las cuales asigna una serie de funciones y responsabilidades a analistas y directivos de inteligencia. La primera fase, de *anticipación*, se basa en un diagnóstico adecuado de la situación del sistema, la identificación de vulnerabilidades y la monitorización de posibles señales o indicadores de debilidad. La etapa de *prevención o mitigación* consiste en adoptar acciones para evitar, mitigar o prepararse ante la posibilidad de ocurrencia del error. Una vez sucedido éste, en la fase de *recuperación* se afrontan sus consecuencias, equilibrando la necesidad de reevaluación del proceso de inteligencia con las demandas de la organización a corto plazo. Finalmente, la fase de *construcción de la fiabilidad* persigue la adopción de una cultura organizativa y un clima laboral que promuevan la fiabilidad, así como la mejor preparación y formación del personal mediante medidas como el aprendizaje y desarrollo de técnicas, habilidades y valores relacionados con la fiabilidad, la transferencia adecuada de información y conocimientos, el fomento del juicio crítico de los analistas y la mejora de las relaciones con los consumidores de inteligencia.

BIBLIOGRAFÍA

- Betts, Richard K. (1978) "Analysis, War and Decision: Why Intelligence Failures Are Inevitable", en *World Politics*, vol. 31, nº 1, pp. 61-89 · Brady, Christopher (1993) "Intelligence Failures: 'Plus ça Change'", en *Intelligence and National Security*, vol. 4, nº 8, pp. 86-96 · Díaz Fernández, Antonio M. (dir.) (2013) *Diccionario Inteligencia y Seguridad*. Madrid, Ed. LID y Presidencia del Gobierno · Díaz Matey, Gustavo (2005) "Methodological approaches to the concept of intelligence failure", en *UNISCI Discussion Papers*, nº 7, enero, pp. 3-15 · Hatch, Scott J. (2013) "Rethinking Failure Managing the 'Reliability Cycle': An Alternative Approach to Thinking About Intelligence Failure", en *Studies in Intelligence*, vol. 57, nº 2, pp. 29-37 · Hollister, John H. (2005) "Learning from Intelligence Failures", en *International Journal of Intelligence and Counterintelligence*, vol. 18, nº 3, pp. 435-450 · Lowenthal, Mark M. (1985) "The Burdensome Concept of Failure", en Maurer, Alfred C., Tunstall, Marion D. y Keagle, James M. (eds.) *Intelligence: Policy and Process*. Boulder, Westview Press, pp. 43-56 · Marrin, Stephen (2004) "Preventing Intelligence Failures by Learning from the Past", en *International Journal of Intelligence and Counterintelligence*, vol. 17, nº 4, pp. 655-672 · Martínez Sánchez, Juan A. (2010) "Errores de Inteligencia", en Velasco, Fernando; Navarro, Diego y Arcos, Rubén (eds.) *La inteligencia como disciplina científica*. Madrid, Plaza y Valdés, pp. 91-108 · Perrow, Charles (1984) *Normal Accidents: Living with High-Risk Technologies*. New York, Basic Books · Shulsky, Abraham y Schmitt, Gary J. (2002) *Silent Warfare: Understanding the World of Intelligence* (3rd Ed.) Dulles, VA: Potomac Books Inc.

Juan Antonio Martínez Sánchez
Ministerio de Defensa, España