

Patologías organizacionales y fallos de inteligencia

Organizational Pathologies and Intelligence Failures

JUAN ANTONIO MARTÍNEZ-SÁNCHEZ

Ministerio de Defensa (Armada Española)

JOSÉ MANUEL RODRÍGUEZ GONZÁLEZ

Universidad de Sevilla

RESUMEN: Generalmente, la ocurrencia de fallos y errores en el ámbito de la inteligencia se atribuye a factores unicastales, señalándose entre ellos las limitaciones en la obtención de la información, la complejidad de los fenómenos a los que se enfrentan los servicios y agencias de inteligencia, la acción del adversarios (decepción) y, sobre todo, los fallos y limitaciones humanas en todas las fases del ciclo de inteligencia, fundamentalmente en la dirección y en el procesamiento y análisis de la información. Sin embargo, a menudo se olvida la influencia de una serie de factores derivados directamente del carácter organizacional de los servicios de inteligencia y que afectan a su estructura y funcionamiento, impidiéndoles a menudo enfrentarse a la naturaleza cambiante, dinámica y flexible de los nuevos riesgos y amenazas del siglo XXI, fundamentalmente el terrorismo yihadista.

En la presente comunicación se exponen una serie de variables y factores organizacionales e institucionales que se encuentran en la base de determinados fallos de inteligencia. Igualmente se proponen una serie de medidas para prevenir, evitar o, cuando menos, minimizar los efectos de su ocurrencia.

PALABRAS CLAVE: Fallos de inteligencia, Patologías organizacionales, Ciclo de inteligencia, Cultura institucional.

ABSTRACT: Failures and errors happening in the field of Intelligence are generally attributed to the so called “sole cause” factors, noting among them: the constraints in information collection, the complexity of the phenomena faced by intelligence services and agencies, the action of the adversaries (deception) and, above all, the effect of human failures and limitations in all phases of the intelligence cycle, in particular during the direction and the processing-analysis phases. However, the impact of a series of factors directly resulting from the organizational nature of the intelligence services and that affect their structure and functioning is often forgotten. This fact often prevents the intelligence community from facing the changing, dynamic and flexible nature of the new risks and threats of the 21st century, in particular the one posed by the jihadist terrorism.

Throughout this document, a series of organizational and institutional variables and factors which are at the base of certain intelligence failures are depicted. Likewise, some measures to foresee, prevent or, at least, minimize the effects of this fails are proposed.

KEYWORDS: Intelligence failures, Organizational pathologies, Intelligence cycle, Institutional culture.

INTRODUCCIÓN

Ya en 1967, el sociólogo de las organizaciones Harold Wilensky (1967: 42-46, 126, 179) advirtió que la función de la inteligencia se encontraba impedida por ciertas características estructurales o burocráticas. Desde entonces han sido numerosos los autores que han señalado la influencia de ciertas patologías organizacionales propias de los servicios y agencias de inteligencia en numerosos fallos y errores de inteligencia (Berkowitz y Goodman, 2000; Brady, 1993; Laqueur, 1985; Lefebvre, 2004; Lowenthal, 2002; Marrin, 2003; O'Connor, 2012; Reynolds, 2004; Travers, 1997). Fueron los graves fracasos de la comunidad de inteligencia de los Estados Unidos en los albores del siglo XXI, fundamentalmente su incapacidad para anticipar y prevenir los atentados del 11 de septiembre de 2001 (11-S, en adelante) y el fiasco de las armas de destrucción masiva (*Weapons of Mass Destruction*, WMD) de Irak, los que impulsaron el interés por el estudio de este tipo de factores organizacionales o institucionales.

PATOLOGÍAS ORGANIZACIONALES EN INTELIGENCIA

Denominamos patologías organizacionales o burocráticas a ciertos factores relacionados con la propia organización y dinámica de los servicios y agencias de inteligencia y que provocan un mal funcionamiento de estos (tabla 1). Este tipo de patologías afectan a todo el ciclo de inteligencia, incluyendo la obtención de información, el procesamiento y análisis, la difusión de inteligencia y la toma de decisiones.

Tabla 1. Patologías organizacionales en los Servicios de Inteligencia

Modelo estructural característico y a menudo desfasado
Complejidad sistémica
Excesiva burocratización y jerarquización
Cultura organizacional o personalidad institucional
Políticas restrictivas de personal
Excesiva especialización
Carencias de cooperación y coordinación interna y externa
Politización de la inteligencia
Otros errores propios de los organismos dedicados a la seguridad

Modelo estructural

El modelo estructural sobre el que se asentaban muchos de los servicios de inteligencia occidentales -especialmente el estadounidense- fue responsable en buena parte de las numerosas patologías organizacionales que caracterizaron su funcionamiento en los inicios del siglo XXI. Este modelo, basado en una concepción de la inteligencia propia del período de la Guerra Fría, se caracterizaba por unas estructuras excesivamente grandes, compartimentadas y rígidas; y aunque se mostró adecuado en aquella época de confrontación entre bloques militares, resulta hoy día inadecuado para enfrentarse a las nuevas amenazas y riesgos del siglo XXI (Saiz Cortés, 2009: 12), como quedó patente en los atentados terroristas del 11-S y 11 de marzo de 2004 (11-M, en adelante). Los

Estados no supieron adaptar sus servicios y agencias de inteligencia al nuevo panorama geoestratégico surgido a finales del siglo XX e inicios del XXI. Un nuevo panorama en el que el adversario ya no era otro bloque militar o político, ni siquiera un Estado considerado tradicionalmente como adversario; sino más bien un conjunto de amenazas y riesgos asimétricos, que no siempre son de tipo militar ni provienen del exterior y que incluyen fenómenos como el terrorismo yihadista, el crimen organizado y transnacional, la ciberdelincuencia y el ciberterrorismo o los conflictos regionales. Todo ello llevó a un cambio en la noción de seguridad, que trasciende ahora los aspectos puramente militares y enfatiza los aspectos multidimensionales, globales y colectivos (Esteban, 2004: 77).

La excesiva burocracia y jerarquización de los servicios de inteligencia

La inteligencia es producto de un trabajo de equipo que se realiza en organizaciones complejas que generan por sí mismas una serie de estructuras y procedimientos burocráticos de actuación. A este respecto, son numerosos los autores que han criticado la excesiva burocratización como fuente de error en inteligencia (Betts, 2002: 174; Davis, 1999: xv; Russell, 2004). Dicho exceso de burocracia se relaciona con la existencia de numerosos niveles jerárquicos y directivos y afecta a todos los niveles del ciclo de inteligencia (Russell, 2004). Ello convierte a los servicios de inteligencia en estructuras rígidas, inflexibles, poco adaptadas a las necesidades de sus clientes y escasamente competitivas desde el punto de vista “empresarial” (Russell, 2004). A nivel operativo, la burocratización aumenta la vulnerabilidad de los servicios de inteligencia, al obstaculizar la obtención, el procesamiento y análisis de la información obtenida (Betts, 2002: 174).

La burocratización está estrechamente vinculada con la excesiva jerarquización y se encuentra en la raíz de los problemas de comunicación interna propios de los servicios y agencias de inteligencia. A diferencia de muchas empresas civiles, caracterizadas actualmente por organigramas flexibles y en los que predomina lo horizontal sobre lo vertical, los servicios de inteligencia siguen manteniendo estructuras puramente verticales y jerárquicas, reminiscencias de los rígidos modelos estructurales heredados de la época de la Guerra Fría, en los que cuestiones de seguridad obligaban a separar e incomunicar a los departamentos del mismo nivel y a éstos de los de otros niveles (Esteban, 2004: 93). Estos modelos se muestran inadecuados hoy día para enfrentarse a las nuevas amenazas de grupos terroristas, caracterizados por estructuras difusas, flexibles y con gran capacidad operativa.

La excesiva burocratización y jerarquía afecta especialmente al trabajo de los analistas. Los servicios de inteligencia suelen mantener estructuras burocráticas en las que los analistas suelen ocupar puestos inferiores, lo que les impide acceder a toda la información necesaria para realizar de forma eficaz su trabajo (Martínez-Sánchez, 2010: 94). Como señala Russell (2004) la distancia jerárquica que separa hoy día a un analista de la dirección de un servicio de inteligencia puede llegar hasta a ocho niveles jerárquicos, afectando al producto final del proceso analítico (informe de inteligencia) en un doble sentido. En sentido descendente, una vez que los órganos directivos, políticos o decisores solicitan un informe de inteligencia, dicha solicitud debe descender a través de la cadena de mando, sufriendo continuas reformulaciones que modifican sustancialmente su contenido original y provocan una notable demora de tiempo hasta llegar finalmente a manos del analista. En sentido ascendente, cuando un analista eleva un informe, éste debe pasar por varios estratos jerárquicos superiores que someten el trabajo del analista a continuos procesos de revisión y que demoran la difusión de dicha

información a los decisores (Navarro, 2004: 33). El informe del Comité de Inteligencia del Senado estadounidense que analizó el fiasco de las WMD de Irak fue claro al respecto:

“En cada caso en que el Comité encontró un fallo analítico o de obtención de información, estos se debieron en parte a fallo de los directivos de la comunidad de inteligencia a través de sus cadenas de mando para supervisar adecuadamente el trabajo de sus analistas y personal encargado de la obtención de información” (U.S. Senate, 2004: 23).

Estos fallos de supervisión están relacionados con los continuos procesos de revisión y evaluación que sufren los analistas por parte de sus superiores y supervisores, y que pueden generarles frustración. Para ejemplificar la relación existente entre analistas y supervisores, Cremeans (1971: 111) recurre a la metáfora del “indio y el jefe en la cultura tribal de análisis de inteligencia”. El supervisor (“jefe”) es aquel del que se supone que lo sabe todo de un tema solo por su puesto o cargo y porque, en última instancia, es quien revisa, edita o simplemente aprueba el trabajo del analista no experto (“indio”). Sin embargo, en la vida real ocurre que el analista suele ser el experto en la materia y el supervisor, aunque probablemente lo fue alguna vez, ahora no es más que un “generalista” con demasiadas responsabilidades administrativas. Las tensiones entre analistas y sus supervisores se reflejan en lo que Cremeans (1971: 110) denomina la *ley de Platt* aplicada al análisis de inteligencia, y que se traduce en que el contenido final de un informe variará del original en función del número de supervisores que lo revise.

La complejidad de los sistemas de inteligencia

Como resultado de las anteriores características organizacionales (modelos estructurales rígidos y estáticos, exceso de burocracia y jerarquización), los servicios, agencias y comunidades de inteligencia se convierten en sistemas altamente complejos. Esta complejidad se ve exacerbada por otros factores como el secreto de las fuentes e información que manejan, la naturaleza de las amenazas a las que se enfrentan, la acción del enemigo (decepción) y, por supuesto, por la presencia del ser humano como factor generador de errores en el proceso de inteligencia. Resultado natural de esta complejidad es el aumento de la probabilidad de ocurrencia de fallos (Betts, 2002: 53; Díaz Matey, 2005: 7).

Este fenómeno ha sido explicado desde el punto de vista de la denominada “*Normal accident theory*” de Charles B. Perrow (1984). Este autor analizó detalladamente el accidente ocurrido el 28 de marzo de 1979 en la Central Nuclear de Three Miles Island (Pennsylvania) y concluyó que los accidentes son acontecimientos normales e imprevisibles en las organizaciones complejas, y que a menudo ocurren debido a la acumulación de pequeños fallos. Aplicado a los sistemas y organizaciones de inteligencia, los errores serían inevitables debido a la imposibilidad de controlar todos los posibles elementos que conforman la complejidad que los caracteriza.

Políticas de personal

Las políticas inadecuadas de personal son otro factor relacionado con el funcionamiento burocrático de los servicios de inteligencia que se encuentran detrás de la ocurrencia de numerosos fallos al afrontar las nuevas amenazas del siglo XXI, encabezadas por el terrorismo internacional.

Un primer aspecto a considerar es la *carencia de personal especializado*, fundamentalmente traductores y analistas, que han padecido los servicios de inteligencia en determinados momentos de la historia. Centrándose en los atentados del 11-S, George (2004: 391) denunció que en 1995 la plantilla de analistas de la CIA se había reducido en un 17% en comparación con la de 1990; y que en esa misma década la plantilla de personal de la Dirección de Inteligencia (*Directorate of Intelligence*, DI) fue disminuyendo paulatinamente hasta alcanzar el 22%. A esta carencia de analistas había que añadir la existencia, al final del siglo XX, de una desproporción negativa entre analistas y personal dedicado a otras tareas burocráticas, administrativas o directivas (Travers, 1997: 37).

Los trágicos acontecimientos del 11-S hicieron patente la carencia de analistas especializados en terrorismo y contraterrorismo. Resulta significativo que en septiembre de 2001 la CIA dispusiera en su Centro de Contraterrorismo de más personal directivo que analistas (Russell, 2004). En cuanto a la falta de personal traductor y experto en lenguas extranjeras, el Comité de Inteligencia del Senado estadounidense que investigó los ataques del 11-S fue muy claro al afirmar que:

“La comunidad de inteligencia no estaba preparada para manejar el desafío de traducir el volumen de inteligencia en lenguas extranjera que recogió. Las agencias de la comunidad de inteligencia experimentaron retrasos en la traducción de material, una escasez de especialistas y agentes de campo expertos en idiomas y un nivel de preparación solo del 30 por ciento en las lenguas más importantes relacionadas con el terrorismo” (U.S. Senate, 2002: xvi).

Esta carencia provocó la acumulación de información sin traducir y ocasionó retrasos y pérdidas de calidad en la información, mostrando la urgente necesidad de disponer del suficiente personal para traducir e interpretar información transcrita en lenguas árabes y dialectos como el pastún, el farsi, el urdu o el dari (Hulnick, 2002: 570).

A nuestro juicio, dos son los factores que se encuentran detrás de este déficit de personal especializado en los servicios y agencias de inteligencia. Por un lado, los recortes presupuestarios que sufren cíclicamente estos organismos; por otro la inadecuación de los procesos de reclutamiento, selección, formación y retención de su personal. Los continuos *recortes de presupuestos* suelen producirse en contextos de crisis económicas o como consecuencia de cambios en el panorama geoestratégico mundial que llevan a percepciones equivocadas sobre la reducción de riesgos y amenazas para la seguridad. Esto fue lo que ocurrió tras el final de la Guerra Fría y el desmembramiento de la Unión Soviética, cuando dichos recortes afectaron gravemente a los recursos de la comunidad de inteligencia estadounidense (Betts, 2002: 45; Travers, 1997: 39), disminuyendo las asignaciones económicas para recursos materiales y humanos.

En materia de reclutamiento y selección de personal, y como respuesta a los atentados terroristas islámicos en los inicios del siglo XXI, la mayoría de los servicios de inteligencia occidentales reaccionaron poniendo en marcha procesos de reclutamiento de nuevo personal, que en el caso del MI5 británico, la CIA o el mismo Centro Nacional de Inteligencia (CNI) español, sobrepasaron el millar de efectivos. De este modo, en noviembre de 2004 el gobierno estadounidense publicó un memorando en el que se instaba al entonces director de la CIA, Porter Goss, a instaurar un plan de acción que incluyera un incremento del 50% de su plantilla dedicada a operaciones y análisis de inteligencia, y del número de agentes expertos en lenguas y dialectos como el árabe, persa y pastún (Waterman, 2004). Sin embargo, estos procesos de reclutamiento

tampoco escaparon a la crítica (Bar-Joseph y McDermott, 2008: 128; Russell, 2004), cuestionándose los estrictos requisitos de seguridad exigidos en la selección de analistas, traductores y agentes operativos con conocimientos de lenguas y dialectos árabes. En la CIA dichos requisitos incluyen la superación de minuciosas investigaciones de seguridad cargadas de tendencias etnocéntricas en las que se sospecha de todo candidato no nacido en el país o de aquel que tenga parientes o conocidos en el extranjero, por considerarlos demasiado vulnerables a influencias extranjeras (Russell, 2004). Dichas barreras dificultan la contratación de traductores e intérpretes con auténtico conocimiento y comprensión del mundo y de la cultura musulmana y un adecuado dominio de sus dialectos (Betts, 2002: 47).

A pesar de lo anterior, no se debe caer en la trampa de pensar que todos los problemas de los servicios de inteligencia se resolverían incorporando mayor número de analistas, ni que ello sea la clave para evitar la ocurrencia de nuevos fallos (Betts, 2002: 48). Evidentemente, un aumento en la contratación de nuevos analistas debe ir acompañada de *mejores oportunidades de promoción y carrera* para ellos. Una de las críticas que tradicionalmente ha recibido la CIA es que fracasa en formar y mantener buenos analistas pero crea buenos burócratas, de modo que existen escasos analistas verdaderamente expertos en sus respectivas áreas (Russell, 2004). Ello se relaciona con lo que Montero (2004b: 45) ha denominado “infravaloración de la cultura de análisis” en los servicios de inteligencia, que provoca que se valoren en mayor medida los aspectos directivos que los analíticos (Travers, 1997: 36, 37). En consecuencia, los sistemas de promoción profesional favorecen a aquellos analistas más experimentados (*senior*) dispuestos a ocupar puestos directivos, mejor valorados y remunerados. Transcurrido determinado tiempo, aquellos analistas más ambiciosos se convierten en gestores, perdiéndose entonces a profesionales con gran experiencia y conocimiento analítico (Marrin, 2003: 611; Travers, 1997: 36).

Otro aspecto relacionado con lo anterior son los *procesos de asignación de destinos* en los servicios de inteligencia, que a menudo se traduce en la mala distribución de analistas y la excesiva rotación a la que se ven sometidos. Dichos procesos son igualmente lentos y engorrosos, transcurriendo un excesivo tiempo desde que se anuncia una vacante hasta que es cubierta, a causa principalmente de las laboriosas y complicadas comprobaciones de seguridad de los candidatos. Con respecto a la *distribución de analistas*, es práctica frecuente de los servicios de inteligencia distribuir a su personal en función de sus necesidades puntuales (Lefebvre, 2004: 251). Tras los ataques del 11-S, la CIA trasladó de sus puestos a 160 analistas que trabajaban en asuntos políticos, económicos y militares, reconvirtiéndolos en “especialistas” en contraterrorismo (The Washington Post, 2002). Pero además, a lo largo de su vida profesional, los analistas suelen *rotar varias veces de un área de análisis a otra*, pasando a desempeñar su actividad en distintas áreas geográficas o funcionales. Aunque mantener a una misma persona demasiado tiempo en un puesto conlleva el riesgo de que acabe generando determinados esquemas mentales y actitudes y opiniones personales que afecten a la calidad y objetividad de su trabajo, una excesiva rotación crea un exceso de “generalistas” e impide que los analistas se conviertan en verdaderos expertos en temas o áreas específicas (Lefebvre, 2004: 251; Marrin, 2003: 628).

Cultura institucional y personalidad corporativa

Se denomina cultura institucional al conjunto de creencias, valores y normas de comportamiento que identifica a una organización y que es transmitida y compartida por

sus miembros. Entre las funciones de la cultura institucional señalamos las de moldear la actuación y comportamiento de sus empleados (Rodríguez Fernández, 1993: 239) y la de facilitar la participación e implicación de éstos en las misiones y actividades de la organización (Palací y Peiró, 1995), ejerciendo un efecto socializador y cohesionador (López Yáñez, 2004: 266-267). Existen varios aspectos relacionados con la cultura organizacional de los servicios y agencias de inteligencia que, a nuestro juicio, condicionan su actuación y afectan al trabajo de agentes y analistas. Entre ellos podemos mencionar la identidad policial o militar de sus miembros, la excesiva rigidez y conservadurismo de sus estructuras y procedimientos y el énfasis en el secretismo, que les lleva a no compartir la información y datos disponibles con otros servicios y agencias de inteligencia.

En numerosos casos, los servicios de información y/o inteligencia se encuentran muy influidos por la *identidad policial o militar* de sus miembros, lo que se refleja a menudo en sus procedimientos y modo de actuar (Montero, 2004b: 46). Ejemplo de esto es el caso del Servicio de Información de la Guardia Civil y el CNI españoles, o el *Federal Bureau of Investigation* (FBI) estadounidense. En el caso del CNI, pese a las reformas experimentadas en los últimos años, su cultura institucional posee un fuerte carácter castrense, justificado entre otros motivos, por la indudable tradición militar de sus antecesores inmediatos (CESED y CESID), su habitual dependencia orgánica del Ministerio de Defensa, su estructura jerárquica y organizacional típicamente castrense, el sometimiento de sus miembros a un régimen disciplinario similar al de las Fuerzas Armadas y la presencia de un importante número de militares y guardias civiles entre su personal, incluyendo buena parte de sus mandos intermedios y directivos (Martínez-Sánchez, 2012b).

Si bien la identidad policial o militar de los servicios de información e inteligencia no es necesariamente negativa, sí imprime irremediamente ciertos condicionantes en la actuación de su personal, relacionados a menudo con la presencia de valores y códigos éticos y morales, el carácter reactivo de su actuación, el énfasis en el análisis de los acontecimientos actuales en lugar de las predicciones y pronósticos futuros (prospectiva) y la excesiva dependencia de los hechos a la hora de interpretar la realidad (Montero, 2004b: 46).

La práctica totalidad de los servicios de inteligencia concede gran importancia a la interiorización y transmisión de sus *valores, códigos éticos y principios de actuación profesional*. Entre estos valores podemos mencionar la justicia, la integridad, la objetividad, la discreción, la dedicación al servicio, el trabajo en equipo, la adaptabilidad, la responsabilidad y el afán de mejora continua (Martínez-Sánchez, 2012a: 1133). Los miembros de los servicios de inteligencia se erigen a menudo en defensores del bien, la Ley y el Estado de Derecho frente a terroristas y criminales, que representan el mal y la amenaza para estos valores. Esta dicotomía entre el bien y el mal condiciona la forma en que agentes y analistas se enfrentan a fenómenos complejos como el terrorismo yihadista o el tráfico de armas. La identidad policial de determinados servicios de inteligencia se refleja igualmente en otro aspecto importante de cara a la prevención de riesgos y amenazas, como es un marcado *carácter reactivo más que proactivo* en su forma de actuar, de modo que se sienten más cómodos investigando hechos ya acontecidos que previniendo aquellos que aún no han sucedido. Sin embargo y como advertía el que fuera director del CNI español, Jorge Dezcallar (2003: 172, 173), el objetivo último de los servicios de inteligencia no es perseguir delitos ni obtener pruebas judiciales, sino realizar análisis estratégicos en busca de resultados a medio y largo plazo. En este sentido se ha criticado que los servicios de

inteligencia se han centrado frecuentemente en *análisis de la situación actual, minusvalorando la importancia de predicciones e investigaciones a largo plazo* (Betts, 2002: 50).

Finalmente, otro aspecto relacionado con la identidad policial de los servicios de inteligencia es la *excesiva dependencia de los hechos* a la hora de interpretar la realidad, lo que provoca que a los analistas les resulte extremadamente difícil hablar en términos de probabilidad de ocurrencia (Montero, 2006: 34; 2004b: 46). De este modo, en escenarios cargados de incertidumbre, propios de fenómenos como el terrorismo internacional o el crimen organizado, el analista no se atreverá a extraer conclusiones; y si, en una pulsión de osadía lo hace, probablemente, no encontrará la manera de transmitirla con eficacia a sus superiores.

Por otro lado y como mencionamos anteriormente, la excesiva jerarquía organizacional que caracteriza a la mayoría de los servicios de inteligencia limita el margen de acción de agentes y analistas, sometiéndolos continuamente al control y supervisión de sus superiores. Fruto de ello aparecen las *tendencias conservadoras* que caracterizan frecuentemente su cultura organizacional y que se reflejan en aspectos como la *falta de creatividad, capacidad de iniciativa e innovación* de los analistas, más preocupados a menudo por no salirse de las directrices y tendencias establecidas por la organización que por mejorar los productos de su trabajo. Esta “cultura de la cautela”, como la ha denominado Walter Laqueur (2004), o “de aversión hacia el riesgo” en palabras de Betts (2002: 46), puede obedecer a imposiciones legales y directrices marcadas por políticos y gobiernos y provoca que quienes trabajan en inteligencia se atengan de forma estricta a las instrucciones, normas y procedimientos internos de actuación, sin arriesgarse a asumir riesgos que pongan en peligro su carrera o puesto de trabajo. Ello restringe la eficacia y efectividad de los servicios de inteligencia ya que, como afirma Laqueur (2004) muy acertadamente, una cautela tan exagerada puede ser adecuada para un ministerio de salud o de agricultura, pero resulta fatal en el ámbito de la inteligencia.

La *falta de capacidad para predecir la innovación* es otro de los factores que se encuentran detrás del fallo de la comunidad de inteligencia de los EE.UU. para predecir los atentados del 11-S. A pesar de que los servicios de inteligencia estadounidenses disponían de evidencias que ahora se valoran como claras, ningún analista fue capaz de prever que un grupo de terroristas yihadistas armados con cuchillos secuestrarían varios aviones comerciales para estrellarlos contra algunos de los edificios más emblemáticos y representativos del poder del país, situados en zonas urbanas y en los que trabajaban miles de personas. Esta incapacidad para predecir la innovación se relaciona con la *falta de creatividad e imaginación* en los análisis sobre el adversario (Russell, 2004; Laqueur, 1998: 301) y con las limitaciones para valorar y contextualizar información e indicios excesivamente novedosos cuya combinación conduce a conclusiones difíciles de asimilar por los modelos mentales sesgados del propio analista, incapaz de liberarse de sus creencias sobre el funcionamiento del mundo y de la conducta humana (Montero, 2004b: 45; Montero, 2006: 33). Todo lo anterior impide al analista enfrentarse con éxito a amenazas flexibles y cambiantes como el terrorismo, que requieren anticipación, capacidad de proyectar escenarios alternativos y utilizar el pensamiento divergente (Montero, 2004b: 45)

La excesiva especialización de los servicios de inteligencia

Refiriéndose a la comunidad de inteligencia de los EE.UU., Russ Travers (1997: 36) ha criticado la excesiva especialización de las distintas agencias de inteligencia, que lleva a que cada una de ellas se ocupe de un aspecto o componente específico del análisis de inteligencia (aspectos económicos, militares, políticos, etc.)¹. Esta extrema especialización obedece a la división de trabajo impuesta en la comunidad de inteligencia estadounidense, en buena parte por presiones del Congreso, con el objetivo de acabar con las duplicidades que se producían cuando distintas agencias realizaban análisis sobre las mismas cuestiones.

Esta división de trabajo ha sido criticada por algunos autores. Crear una comunidad de inteligencia y luego realizar una división de trabajo entre sus miembros va contra el sentido común y acarrea diversas consecuencias negativas. En primer lugar, lo que Russ Travers (1997: 35) ha denominado la “balcanización de la comunidad de inteligencia” que demanda necesariamente buenas dosis de coordinación y cooperación que, como veremos posteriormente, no siempre se consiguen. Dividir el análisis de inteligencia en subcomponentes militares, económicos y políticos y luego repartir la responsabilidades entre varias agencias supone “sembrar las semillas para errores inevitables” (Travers, 1997: 35-36). En segundo lugar, cuando el consumidor de la inteligencia solicita a dichas agencias una serie de análisis sobre un tema, cada una de ellas lo hará desde el punto de vista de su propia área de especialización, sin tener en cuenta la interrelación con otros aspectos y componentes. Consecuentemente, la inteligencia que llega finalmente al decisor se caracteriza por una *falta de fusión o integración* que le impide disponer de una perspectiva global y actuar en consecuencia. Como resultado final, la carencia de fusión e integración provoca que la comunidad de inteligencia como un todo sea menos efectiva que la suma de sus partes.

Por último, no hay que olvidar que la duplicidad y competencia entre agencias favorece la expresión abierta de desacuerdos y discrepancias, permitiendo a los decisores disponer de diversos puntos de vistas y reduciéndose así la probabilidad de cometer errores (Betts, 1978: 77-78). La excesiva división y especialización del trabajo conduce irremediabilmente a una disminución del análisis competitivo.

Falta de cooperación y coordinación

Muy relacionado con la excesiva especialización de los servicios de inteligencia se encuentra la falta de cooperación y coordinación que se produce entre ellos. Lógicamente, cuanto mayor es una comunidad de inteligencia y más elementos o agencias la componen, mayores son las necesidades de cooperación y coordinación que exige.

La falta de coordinación se encuentra entre las causas de los numerosos errores al no prevenir los atentados terroristas del 11-S y 11-M; atentados que cuestionaron seriamente los procedimientos y mecanismos de coordinación y cooperación de los distintos servicios de inteligencia occidentales (Merlos, 2007: 30). Pulido (2007: 59) ha señalado como causa del fallo de previsión de los atentados del 11-S la falta de comunicación y coordinación entre el FBI y la CIA, agravada por la división de competencias existente entre ambas agencias. El informe del Comité de Inteligencia del Senado de los EE.UU. fue claro, al identificar graves fallos a la hora de compartir información:

¹ Actualmente la comunidad de inteligencia norteamericana está formada por 17 agencias. Véase: <https://www.intelligence.gov/how-the-ic-works>

“Antes del 11 de septiembre, la información se compartía de manera inadecuada no solo dentro de la Comunidad de Inteligencia, sino también entre la Comunidad, otras agencias federales y las autoridades estatales y locales. En resumen, la investigación conjunta descubrió problemas significativos en la forma en que las agencias de inteligencia compartían información entre ellas y con organismos que necesitan información para proteger a la nación contra ataques terroristas” (U.S. Senate, 2002: 355).

En el caso de los atentados del 11-M en Madrid se ha citado la tradicional descoordinación y falta de comunicación entre los servicios de información e inteligencia españoles en materia de lucha antiterrorista. También en este caso las agencias gubernamentales fallaron a la hora de compartir información sobre la amenaza terrorista que suponía Al-Qaeda para España (Falkenrath, 2004). Prueba de ello son las sugerencias recogidas en la declaración de la Unión Europea sobre la lucha contra el terrorismo a raíz de estos atentados y que reservó íntegramente su capítulo 9 al intercambio de información como medida preventiva de primer orden en los siguientes términos: “El Consejo Europeo invita a los Estados miembros a mejorar los mecanismos de cooperación y fomentar la colaboración sistemática y efectiva entre los servicios de policía, de seguridad y de información” (citado por Navarro, 2005: 21).

Los errores al compartir información también estuvieron presentes en el controvertido asunto de las armas de destrucción masiva de Irak. El Comité de Inteligencia del Senado estadounidense concluyó que la CIA había abusado de su posición privilegiada en la comunidad de inteligencia a la hora de compartir información con otras agencias, lo que había ido en detrimento de la calidad de las evaluaciones de inteligencia (U.S: Senate, 2004: 27).

Esta falta de cooperación y coordinación entre servicios de inteligencia puede deberse a varios motivos, incluyendo la existencia de barreras organizacionales para la libre circulación e intercambio de información que impide que los analistas puedan disponer de toda la información relevante e integrarla correctamente (Marrin, 2004: 662), los celos profesionales (Sansó-Rubert, 2007: 83-84) y la competencia por apuntarse el éxito de determinadas operaciones, que puede incluso conducir a lo que se conoce como *stovepiping* u ocultación voluntaria de información. También se ha señalado la carencia de un organismo que centralice y coordine la información y las labores de inteligencia, así como el hecho de que estas labores se realicen frecuentemente por funcionarios de diferentes agencias, con métodos y procedimientos distintos, diferentes normas de seguridad y de difusión de la información (O'Connor, 2012).

Los problemas de coordinación y cooperación afectan frecuentemente a la relación que se establece entre varios servicios de inteligencia en el seno de una comunidad de inteligencia, pero también pueden aparecer problemas de relación en el interior de los propios servicios de inteligencia, es decir, entre sus miembros. Entonces hablamos principalmente de *problemas de comunicación* -entendiendo comunicación en sentido amplio- entre departamentos (entre analistas y personal dedicado a la obtención de información, por ejemplo) o dentro de un mismo departamento (entre analistas, o entre éstos y sus supervisores). Dentro de los departamentos dedicados al análisis de inteligencia, los problemas de comunicación entre analistas y sus supervisores tienen que ver con las relaciones jerárquicas establecidas entre ellos por la organización, de las que ya hemos hablado anteriormente, pero también se pueden mencionar los problemas de relación entre los propios analistas.

Incapacidad para relacionar datos

Este fenómeno puede producirse tanto cuando un analista sufre dificultades para relacionar datos que están a su disposición -en cuyo caso estaríamos hablando de un error en la fase de análisis- como cuando varias agencias o servicios de inteligencia se muestran incapaces de relacionar e integrar en un producto único todos los datos que poseen sobre un determinado asunto. En ambos casos, estas dificultades provienen frecuentemente de la excesiva división o compartimentación de las comunidades y servicios de inteligencia a la que antes aludíamos y que ocasionan barreras de coordinación, cooperación y comunicación, tanto a nivel interno como externo.

Ya en 1978, Richard Betts advertía del desafío que suponía para los analistas de inteligencia integrar datos e indicadores fragmentarios, dudosos e incluso contradictorios, muchos de los cuales por sí solos constituyen claras señales de alarma o advertencia (Betts, 1978: 75). Quince años más tarde, este autor se reafirmaba al señalar que los errores en unir datos fragmentarios son muy comunes en el ámbito de la inteligencia (Betts, 2002: 56).

Al analizar retrospectivamente la ocurrencia de graves fracasos de inteligencia a menudo se concluye que no se tuvieron en cuenta determinados indicios que señalaban claramente la existencia de una amenaza o ataque. En septiembre de 1941 la inteligencia estadounidense disponía de suficientes datos que apuntaban a un posible ataque japonés a Pearl Harbour, pero fue incapaz de integrar estos trozos dispersos de información que hubieran permitido componer una imagen coherente de la situación (Wohlstetter, 1962). Idéntico caso ocurrió con los atentados del 11-S, en los que el Comité de Inteligencia del Senado detectó “una incapacidad persistente para comprender el significado colectivo de piezas de inteligencia individuales” (U.S. Senate, 2002: xvi, 59); de modo que a pesar de la acumulación de indicios y pruebas que así lo indicaba, la comunidad de inteligencia estadounidense no fue capaz de prever los ataques terroristas de Nueva York y Washington. Como relata O’Connor (2012), desde 1998 a 2001, varios terroristas de Al-Qaeda habían entrado en los EE.UU. procedentes de Hamburgo y Bangkok, mientras la CIA controlaba otras células durmientes. Por otra parte, los servicios de inteligencia norteamericanos conocían que Osama bin Laden era un enemigo poderoso, desde los ataques a las embajadas africanas de 1998 y al destructor USS “Cole” en 2000. A principios de 2001 el FBI investigó la denuncia presentada por una escuela de vuelo que alertaba del interés de varios individuos musulmanes, encabezados por Zacarias Moussaoui, por aprender a pilotar aviones en vuelo, despreocupándose de maniobras de despegue y aterrizaje; y en verano de 2001 fueron detectados varios terroristas sospechosos en Las Vegas, bebiendo y celebrando una fiesta; y un agente del FBI de Fénix (Arizona) alertó a sus superiores de la posibilidad de un atentado, al igual que lo hicieron otros servicios de inteligencia extranjeros. En conclusión, la capacidad de Washington para percibir la trama y “conectar los datos”, se vio gravemente afectada por la falta de coordinación y cooperación entre la fuerzas policiales y las agencias de inteligencia de EE.UU. (Falkenrath, 2004).

Politización o subordinación de la inteligencia a la política

La politización constituye una de las principales causas de los fracasos de inteligencia (Betts, 1978: 61; Cremeans, 1971: 113; Lefebvre, 2004: 241; O’Connor, 2012). Politización es un concepto amplio e impreciso en el ámbito de la inteligencia y que hace referencia a múltiples realidades y situaciones. De modo general, podemos decir que este fenómeno se produce siempre que la política interfiere en la producción de la inteligencia (Esteban y Carvalho, 2012: 59). Ello puede deberse a la presión de los

decisores políticos para que los servicios y agencias de inteligencia les suministren la inteligencia que desean. Esta forma de politización se encuentra detrás del fiasco de las armas de destrucción masiva de Irak, causado por la errónea creencia del Gobierno estadounidense de que Saddam Hussein mantenía conexiones con Al-Qaeda y disponía de capacidades WMD². También pudiera ocurrir que, de manera voluntaria, la comunidad de inteligencia ajuste sus productos e informes a los puntos de vista y directrices de los políticos al objeto de favorecer una línea preferente de pensamiento, con independencia de la realidad (Gates, 1992: 5). En otras ocasiones los miembros de los servicios de inteligencia -fundamentalmente analistas, supervisores y directivos de inteligencia- son los responsables de la politización, al actuar movidos por motivaciones o intereses políticos propios y conceder mayor importancia a aquella información que coincida con sus propios planteamientos políticos (Montero, 2004b: 45). En ambos casos podemos considerar que la politización constituye una patología provocada por tendencias organizacionales o institucionales.

Otras patologías organizacionales

Otras patologías organizacionales tienen que ver con las tendencias institucionales a prejuzgar las intenciones y capacidades del adversario y actuar en consecuencia.

Sobrestimar y *subestimar* las capacidades del adversario son causas frecuentes de fallos de inteligencia. Ejemplo claro de sobrestimación es la creencia generalizada de la comunidad de inteligencia estadounidense sobre las capacidades balísticas nucleares de la Unión Soviética durante la Guerra Fría, o el error en la estimación de las capacidades WMD de Irak en 2004. Por el contrario, la subestimación de las intenciones y capacidades militares alemanes que cometió el dirigente soviético Josef Stalin subyace en el éxito de los alemanes al invadir Rusia en 1941. También erró la comunidad de inteligencia estadounidense al subestimar las capacidades destructivas que poseía Al-Qaeda en los inicios del siglo XXI, lo que impidió la adopción de medidas adecuadas para prevenir los atentados masivos del 11-S de 2001 (Alonso, 2011: 9).

La subestimación se relaciona íntimamente con el *exceso de confianza* (Martínez-Sánchez, 2010: 97), que se produce cuando gobiernos y servicios y agencias de inteligencia confían excesivamente en sus propias capacidades y desechan la posibilidad de ser atacados por el adversario. Este fue uno de los múltiples errores que cometieron los israelíes en 1973 al minusvalorar la amenaza árabe y descartar la posibilidad de ser atacados, firmemente convencidos como estaban de que aquellos no podrían ganar la guerra. Este error se encuentra también detrás de los múltiples fallos cometidos por la comunidad de inteligencia estadounidense al predecir los ataques terroristas de 2001; y de los errores de la inteligencia española para prevenir los atentados del 11-M. En junio de 2002, el entonces Director del CNI español, Jorge Dezcallar (2003:186), declaraba:

“No creo que España se vaya a convertir en un país atractivo [para las células yihadistas], ni siquiera como base logística. Para toda esta gente España sigue siendo el recuerdo de la época Al-Ándalus [...] Porque es Al-Ándalus, [...] el recuerdo de un pasado mítico y feliz. Creo que elegirían otros muchos sitios donde hacer atentados antes que hacerlos aquí [...] Habrá que estar vigilantes, pero no veo que vaya a ocurrir a corto plazo. Y tampoco veo que

² Consecuentemente con este planteamiento, la Administración Bush presionó a la comunidad de inteligencia para que le proporcionara datos e informes que sustentaran y confirmaran su punto de vista, otorgando mayor validez a aquellos análisis que respaldaban estas conclusiones y desechando los que no las sustentaban (Montero, 2004b: 45).

España, inicialmente al menos, vaya a ser un objetivo prioritario de atentados terroristas. Me puedo equivocar, pero no lo creo”.

Para explicar este fenómeno, autores como el ex-senador demócrata norteamericano Gary Hart (2003: 46), han hecho referencia a la existencia de una especie de “fatiga post-guerra fría”, caracterizada por un exceso de confianza ante el cambio en el escenario estratégico mundial y por la falta de adversarios con las suficientes capacidades para amenazar seriamente la seguridad nacional.

Este exceso de confianza lleva a menudo a la pasividad e inactividad. Pocos meses después de los atentados del 11-M en Madrid, Richard Falkenrath (2004), ex Comisionado de Contraterrorismo del Departamento de Policía de Nueva York, criticó la pasividad de buena parte de los gobiernos a la hora de prevenir ataques terroristas en suelo europeo. Según este autor, los ataques de 11-M fueron resultado de la inactividad del entonces presidente Aznar para remediar una serie de debilidades estructurales específicas en las leyes y prácticas de la lucha antiterrorista. Entre éstas se ha señalado la *falta de un régimen jurídico adecuado* que favorezca la actuación preventiva de los servicios de inteligencia (Falkenrath, 2004).

La *falta de autocrítica* es otra de las patologías organizacionales que puede afectar a los servicios de inteligencia occidentales. Como defiende Marrin (2004), estudiar y aprender de los errores del pasado es fundamental para no repetirlos. Sin embargo, pese a los numerosos errores cometidos a lo largo de la historia y a los múltiples estudios realizados a raíz de ellos, algunos servicios de inteligencia no parecen haber aprendido mucho de ello. El caso de los atentados del 11-M es un claro ejemplo de ello. En palabras de Falkenrath (2004), España no realizó un examen autocrítico del porqué no se impidió dicho suceso, como lo demuestra la creación de la fallida Comisión de Investigación, formada por políticos con escaso conocimiento de la materia y más interesados en defender los intereses de sus partidos políticos que en esclarecer la verdad de los hechos. Ello impidió investigar realmente los atentados, averiguar sus causas y asesorar sobre posibles medidas para evitar su repetición.

PATOLOGÍAS ORGANIZACIONALES. ALGUNAS MEDIDAS CORRECTORAS.

Los graves fracasos de inteligencia y la necesidad de impedir que ocurran de nuevo conllevan generalmente importantes reformas estructurales en los servicios, agencias y comunidades de inteligencia (Betts, 1978: 71; Betts, 2002: 52; Schulsky y Schmitt, 2002: 63). Fue lo sucedido tras los ataques del 11-S y el denominado fiasco de las WMD de Irak. A raíz de estos fallos, los miembros de la comunidad de inteligencia estadounidense iniciaron un debate decisivo sobre la idoneidad del modelo de inteligencia imperante hasta ese momento y la necesidad de introducir reformas estructurales para adaptarse a las exigencias del nuevo panorama mundial (Navarro, 2004: 34). Se trataba con ello de establecer una estructura organizacional que facilitara el análisis de inteligencia, en lugar de entorpecerlo (Travers, 1997: 38). Ello exigía, en primer lugar, adaptar la estructura, organización y funcionamiento de los servicios de inteligencia a la naturaleza asimétrica, flexible y desconcertante de los nuevos riesgos y amenazas, como el terrorismo yihadista, los conflictos regionales, la creación de estados fallidos o la delincuencia organizada. Desde este punto de vista, algunos autores han propuesto medidas orientadas hacia la adopción de modelos empresariales (Díaz Fernández, 2006: 11), mucho más dinámicos, adaptables y flexibles que las organizaciones de inteligencia (Bar-Joseph y McDermott, 2008: 131). Desde esta perspectiva, Pincus (2001) menciona la importancia de considerar a la comunidad de

inteligencia estadounidense como una empresa que debe disponer de un método adecuado para evaluar el éxito o fracaso de su actuación de cara a la consecución de sus objetivos. Refiriéndose específicamente al CNI español y poco antes de los atentados del 11-M, Dezcallar (2003: 173) señaló la necesidad de adoptar un modelo más flexible y adaptable a los cambios constantes de la situación y cuya actuación responda en mayor medida a las demandas del Gobierno.

La búsqueda de modelos estructurales más flexibles y versátiles pasa irremediablemente por disminuir la influencia de las tendencias burocráticas que afectan a los servicios y agencias de inteligencia, algo difícil en tanto que estas instituciones son organismos estatales caracterizados por la excesiva jerarquización y burocracia propias de toda Administración. Otro aspecto importante de las reformas estructurales acaecidas tras los atentados terroristas de 2001 y 2004 ha sido el énfasis en la mejora de la cooperación y coordinación, no solo dentro y entre las agencias que pertenecen a una misma comunidad de inteligencia, sino también entre países que comparten los mismos riesgos y amenazas.

En cuanto a los problemas de comunicación interna, dentro de las organizaciones de inteligencia es imprescindible disponer de un sistema adecuado de distribución y difusión de información que haga llegar a los analistas los datos importantes para el desarrollo de su trabajo. A este respecto, la comunicación y coordinación entre analistas de distintas áreas de una misma organización de inteligencia permite proveer a los consumidores de inteligencia de una perspectiva más exacta y equilibrada que la que posee un único analista (Marrin, 2003: 613). Los órganos encargados de obtener información deben tener clara y continuamente definidas cuáles son las necesidades de los analistas (Rosales, 2007: 139) y éstos deben solicitar de forma activa y “agresiva” la información que necesiten y proporcionar continuamente retroalimentación sobre la que reciben y el grado de adecuación a sus necesidades y objetivos (Watanabe, 1997: 47). Impulsar la coordinación y comunicación interna implica además la eliminación de las excesivas barreras burocráticas, jerárquicas y de seguridad que impiden el flujo de inteligencia y la interacción entre analistas (Berkowitz, 2001: 615). También reclama un esfuerzo del analista para relacionarse con sus compañeros y colegas de otras agencias, interesarse por lo que hacen y cómo lo hacen, compartiendo métodos, técnicas, experiencias e información. Ello se traducirá en una mejora en la obtención de datos, la disminución de duplicidades y conflictos de competencias y, en definitiva, en un aumento de la calidad de los productos de inteligencia (Watanabe, 1997: 47). Sin embargo y aunque necesarias, estas medidas no siempre son suficientes para obtener un buen producto de inteligencia. El consenso entre analistas de inteligencia es un valor importante y deseable, pero no garantiza que las conclusiones y juicios obtenidos de ese consenso sean correctos (Watanabe, 1997: 46).

Con relación a la cooperación entre servicios y agencias pertenecientes a la misma comunidad de inteligencia, la experiencia de los atentados del 11-S y 11-M mostraron la necesidad de mejorar la coordinación entre agencias nacionales al objeto de compartir información imprescindible en la lucha contra el terrorismo global (Falkenrath, 2004; Isaacson y O'Connell, 2002). En este contexto adquiere máxima importancia el concepto de “comunidad de inteligencia” en un sentido amplio, entendida como un “sistema integrado por las agencias y organismos relevantes en materia de inteligencia, que sirven a los objetivos estratégicos del Gobierno de la nación de forma coordinada, gracias a la labor de una estructura de superior nivel que promueve y garantiza las relaciones y la conexión necesarias, a los niveles y por los procedimientos adecuados, para optimizar los resultados” (Sansó-Rubert, 2007: 81). Desde este punto de vista

integral, además de a los servicios y agencias de información e inteligencia, podríamos incluir dentro de la comunidad de inteligencia a otras muchas organizaciones e instituciones capaces de proporcionar información de interés para las necesidades del Gobierno, como embajadas y delegaciones consulares en el exterior, representaciones ante organismos internacionales; así como otros departamentos y organismos ministeriales como la Agencia Tributaria o el Servicio de Vigilancia Aduanera. Es más, en un sentido “extraordinariamente amplio”, para Sansó-Rubert (2007: 81) cabría incluir dentro de la comunidad de inteligencia a otros organismos públicos y privados como empresas multinacionales, entidades bancarias, centros universitarios y *think-tanks*. De hecho, son muchos los autores que reivindican desde hace tiempo una mayor cooperación de los servicios de inteligencia con el sector privado (Berkowitz y Goodman, 2000; Jordán, 2002: 304). En todo caso, el complejo entramado de elementos que conforma una comunidad de inteligencia demanda necesariamente fórmulas adecuadas y eficaces de coordinación y cooperación entre sus miembros. Ello pasa por la creación de centros de coordinación nacionales en materia de inteligencia, como ocurrió con el *Terrorist Treat Integration Center* estadounidense en 2003, tras los graves fallos de inteligencia del 11-S y de las WMD de Irak; o del Centro Nacional de Coordinación Antiterrorista español, apenas unos meses después de los atentados del 11-M.

En materia de cooperación internacional, en un contexto geoestratégico actual conformado por amenazas y riesgos globales que no solo afectan a la seguridad nacional sino también a la colectiva, se requiere una respuesta integral caracterizada por la multidisciplinariedad y multilateralidad, así como por el fortalecimiento de la cooperación en materia de inteligencia a nivel internacional (Sansó-Rubert, 2007: 80). Ello permitirá potenciar la cooperación con otros Estados y la coordinación entre servicios y agencias de inteligencia de diversos países (Isaacson y O'Connell, 2002; Rosales, 2005: 43; Rosales, 2007: 128), contemplándose incluso la creación o impulso de agencias supranacionales de inteligencia (Esteban, 2004: 98-99), a semejanza de lo que ya ocurre con las agencias policiales (INTERPOL, por ejemplo).

Otro aspecto a analizar es la *política de personal* de los servicios de inteligencia, sobre todo en lo concerniente al reclutamiento, selección, formación y retención de sus miembros. Se hace necesario invertir y aumentar los presupuestos destinados a ello, para dotar a la comunidad de inteligencia de más y mejores capacidades humanas y materiales. Imprescindible resulta un aumento de las plantillas, fundamentalmente en lo que respecta a traductores/intérpretes, analistas y agentes y operadores HUMINT. Especial atención merece también la mejora de las condiciones y perspectivas profesionales de los analistas, mediante incentivos económicos y mejores posibilidades de formación y promoción (Marrin, 2003: 611; Russell, 2004). Un adecuado equilibrio en la distribución y rotación de analista en áreas geográficas y funcionales es una medida complementaria para aumentar su capacitación y experiencia, mejorando de esta manera la calidad de los análisis.

La *personalidad institucional* constituye otro impedimento para la eficacia de los servicios de inteligencia al imponer ciertos condicionantes éticos y morales a sus miembros, penalizando además la creatividad, imaginación, capacidad de innovación e iniciativa de su personal, al tiempo que impide contemplar la realidad desde otras perspectivas distintas a las suyas propias. Sin ignorar los condicionantes morales, políticos y religiosos propios de la sociedad en que vive y trabaja, el analista debe dejar a un lado su identidad policial o militar y abordar su trabajo desde un punto de vista lo más aséptico y objetivo posible (Montero, 2004b: 46). Por otra parte, los servicios de

inteligencia deben introducir mecanismos que fomenten la capacidad de imaginación, innovación y atrevimiento de su personal, fundamentalmente los analistas (Laqueur, 2004).

Un cambio en la personalidad institucional u organizativa de los servicios de inteligencia debe ir acompañado de un fuerte impulso de la cultura de inteligencia que proporcione a la sociedad y a la opinión pública un adecuado conocimiento y comprensión, tanto de sus estructuras, funciones y marco jurídico (Navarro, 2005: 11-12) como de los nuevos riesgos y amenazas a los que nos enfrentamos en la actualidad, “para que comprenda la magnitud del reto al que se enfrenta” (Dezcallar, 2004: 39). Ello requiere de los servicios y agencias de inteligencia alejarse del tradicional secretismo y oscurantismo del que tradicionalmente han hecho gala, mediante el fomento de medidas como informar a la sociedad de la razón de ser de los servicios de inteligencia, favorecer políticas de desclasificación documental y fomentar la investigación sobre la materia (Navarro, 2005: 12).

Finalmente y a nuestro juicio, todas las anteriores reformas organizacionales deben ir acompañadas de un *régimen jurídico eficaz* en la lucha contra los nuevos riesgos y amenazas a la seguridad internacional. Este régimen jurídico debe cumplir tres requisitos básicos (Falkenrath, 2004). En primer lugar, disponer de procedimientos legales activos y dinámicos que permitan a los agentes de los cuerpos y fuerzas de seguridad del estado (FCSE) el acceso a la información procedente de los servicios de inteligencia. Como contraprestación, los servicios de inteligencia debieran poder acceder a la información obtenida por las FCSE sobre temas de su interés. Finalmente, las fiscalías han de tener la capacidad para incluir información proporcionada por los servicios de inteligencia en los procedimientos judiciales, sin perjuicio de la acción penal y sin correr el riesgo de que se divulgue dicha información. Como es lógico, el cumplimiento de estos requisitos pasa por una mayor coordinación y cooperación entre los servicios de inteligencia, los cuerpos policiales y la Administración de Justicia, fundamentalmente jueces y fiscales (Falkenrath, 2004).

A pesar de todas las medidas anteriormente enumeradas, es necesario puntualizar que no siempre estas reformas estructurales y organizacionales resultan eficaces (Bar-Joseph y McDermott, 2008: 132). Además, como advierte Hollister (2005: 446), muchas reformas estructurales dirigidas a solucionar patologías específicas introducen o acentúan otras patologías, generando en ocasiones más costos que beneficios, sin conseguir evitar la ocurrencia de errores (Betts, 1978: 84-86). No hay que olvidar a este respecto que tras toda reestructuración de la comunidad de inteligencia se produce un periodo de transición durante el cual se pierde eficacia (Travers, 1997: 41), convirtiendo al país en más vulnerable aún a las amenazas y riesgos. A ello hay que añadir el coste económico que toda reestructuración de una comunidad de inteligencia implica y que, a menudo, es difícilmente asumible por los Estados.

BIBLIOGRAFÍA

Alonso, Rogelio (2011), “*La innovación terrorista: desafíos para la prevención y contención del terrorismo yihadista*”, Documento de opinión del Instituto Español de Estudios Estratégicos, 08/2011.

Bar-Joseph, Uri y McDermott, Rose (2008), “Change the Analyst and Not the System: A Different Approach to Intelligence Reform”, *Foreign Policy Analysis*, Vol. 4, No. 2, pp. 127-145.

- Berkowitz, Bruce D. (2001), "Better Ways to Fix U.S. Intelligence", *Orbis*, Vol. 45, No. 4, pp. 609-619.
- Berkowitz, Bruce D. y Goodman, Allan E. (2000), *Best Truth: Intelligence in the Information Age*, Yale: Yale University Press.
- Betts, Richard K. (1978), "Analysis, War and Decision: Why Intelligence Failures Are Inevitable", *World Politics*, Vol. 31, No. 1, pp. 61-89.
- (2002), "Fixing Intelligence", *Foreign Affairs*, Vol. 81, No. 1, pp. 43-59.
- Brady, Christopher. (1993), "Intelligence Failures: Plus ça Change", *Intelligence and National Security*, Vol. 4, No. 8, pp. 86-96.
- Cremeans, Charles D. (1971), "Basic Psychology for Intelligence Analysts", *Studies in Intelligence*, Vol. 15, No. 1, pp. 109-114.
- Davis, Jack (1999), "Introduction. Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis", en Heuer, Richards J., *Psychology of Intelligence Analysis*, Langley (VA): Central Intelligence Agency, pp. x-xxiv.
- Dezcallar, Jorge (2003), "Los servicios de inteligencia: una herramienta indispensable", en Aguilar, Miguel A. y Ridaó, José M. (Eds.), *El terrorismo: una amenaza del siglo XXI*, Actas del XIV Seminario Internacional de Defensa, Madrid: Asociación de Periodistas Europeos, pp. 155-194.
- (2004), "Libertad y seguridad", *Política Exterior*, Vol. 18, No. 102, pp. 31-40.
- Díaz Fernández, Antonio 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 del Observatorio de Política Exterior Española (Fundación Alternativas), 3/2006.
- Díaz Matey, Gustavo (2005), "Methodological approaches to the concept of intelligence failure", *UNISCI Discusión Papers*, No. 7, pp. 3-15.
- (2008), "Hacia una definición inclusiva de inteligencia", *Inteligencia y Seguridad*, No. 4, pp. 59-84.
- Esteban, Miguel A. (2004), "Necesidad, funcionamiento y misión de un servicio de inteligencia para la seguridad y la defensa", en *Estudios sobre Inteligencia: fundamentos para la seguridad internacional* (Cuadernos de Estrategia, 127), Madrid: Instituto Español de Estudios Estratégicos, pp. 73-99.
- Esteban, Miguel A. y Carvalho, Andréa V. (2012), "Inteligencia: concepto y práctica", en González Cussac, José L. (Coord.), *Inteligencia*, Valencia: Tirant lo Blanch, pp. 17-71
- Esteban, Miguel A. y Navarro, Diego (2003), "Gestión del Conocimiento y Servicios de Inteligencia: la dimensión estratégica de la información", *El Profesional de la Información*, Vol. 12, No. 4, pp. 269-281.
- Falkenrath, Richard A. (2004), "Europe's Dangerous Complacency", *Financial Times*, 7 Julio, p. 17.
- Gates, Robert M. (1992), "Guarding Against Politicization", *Studies in Intelligence*, Vol. 36, No. 5, pp. 5-13.
- George, Roger Z. (2004), "Fixing the problem of analytical mind-sets: alternative analysis", *International Journal of Intelligence and Counterintelligence*, Vol. 17, No. 3, pp. 385-405.
- Hart, Gary. (2003), "Post-Cold War Lassitude Contributed to the Attack on America", en Williams, Mary E. (Ed.), *The Terrorist Attack on America*, San Diego: Greenhaven, pp. 42-46.
- Hollister, John H. (2005), "Learning from Intelligence Failures", *International Journal of Intelligence and CounterIntelligence*, Vol. 18, No. 3, pp. 435-450.

- Hulnick, Arthur S. (2002), “The Downside of Open Source Intelligence”, *International Journal of Intelligence and Counterintelligence*, Vol. 15, pp. 565-579.
- Isaacson, Jeffrey A. & O’Connell, Kevin M. (2002), “Beyond Sharing Intelligence, We Must Generate Knowledge”, *RAND Review*, Vol. 26, No. 2.
- Jordán, Javier (2002), “El terrorismo en la sociedad de la información: el caso de Al Qaida”, *El profesional de la información*, Vol. 11, No. 4, pp. 297-305.
- Laqueur, Walther (1985), *A World of Secrets: Uses & Limits of Intelligence*, New York: Basic Books.
- (1998), “The Future of Intelligence”, *Society*, Vol. 35, No. 2, pp. 301-311.
- (2004), “Las desgracias de la CIA”, *La Vanguardia*, 15 junio.
- Lefebvre, Stéphane (2004), “A Look at Intelligence Analysis”, *International Journal of Intelligence and Counterintelligence*, Vol. 17, No. 2, pp. 231-264.
- López Yáñez, Julián (2004), “Cultura organizativa”, en Salvador, Francisco; Rodríguez, Jose L. y Bolívar, Antonio (Eds.), *Diccionario enciclopédico de Didáctica*, Málaga: Aljibe, pp. 263-270.
- Lowenthal, Mark M. (2002), *Intelligence: From Secrets to Policy* (2nd. ed.), Washington, DC: Congressional Quarterly Press.
- Marrin, Stephen (2003), “CIA’s Kent School: Improving Training for New Analysts”, *International Journal of Intelligence and CounterIntelligence*, Vol. 16, No. 4, pp. 609-637.
- (2004), “Preventing Intelligence Failures by Learning from the Past”, *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.
- (2012a), “Aplicaciones de internet al reclutamiento de personal de los servicios de inteligencia”, en *Actas de las IV Jornadas de Estudios de Seguridad*, Madrid: Instituto Universitario “General Gutiérrez Mellado” de Investigación sobre la Paz, la Seguridad y la Defensa, pp. 1123-1144.
- (2012b), “El reclutamiento de personal en el Centro Nacional de Inteligencia”, *Papeles del Psicólogo*, Vol. 33, No. 3, pp. 202-210.
- Merlos, Juan A. (2007), “La Inteligencia humana en el Combate del Terrorismo Yihadista”, *Revista Ejército*, No. 797, pp. 30-36.
- Montero, Andrés (2004a), “Psicología del contraterrorismo”, *La Razón*, 2, de julio.
- (2004b), “Psicología del terrorismo e inteligencia contraterrorista”, *Papeles del Psicólogo*, Vol. 25, No. 88, pp. 39-47.
- (2006), “Gobernanza de la Seguridad: seguridad inteligente frente a nuevas amenazas”, *Revista Catalana de Seguretat Pública*, Vol. 16, pp. 25-37.
- Navarro, Diego (2004), “Introducción”, en Navarro, Diego (Coord.), *Estudios sobre inteligencia: fundamentos para la seguridad internacional* (Cuadernos de Estrategia, 127), Madrid: Instituto Español de Estudios Estratégicos, pp. 15-40.
- (2005), “Introducción”, en Navarro, Diego (Coord.), *El papel de la inteligencia ante los retos de la seguridad y defensa internacional* (Cuadernos de Estrategia, 130), Madrid: Instituto Español de Estudios Estratégicos/Centro Nacional de Inteligencia, pp. 11-34.
- O’Connor, Thomas R. (2012). *The history and lessons of intelligence failure*. Disponible en: <https://www.ics.uci.edu/~ucrec/intranet/miscdocs/HSclassnotes/class5.html>

- Palací, Francisco J. y Peiró, José M. (1995), *La incorporación a la empresa*, Valencia: Promolibro.
- Perrow, Charles B. (1984), *Normal Accident: Living with High-Risk Technology*, New York: Basic Books.
- Pincus, Walther (2001), “Intelligence Shakeup Would Boost CIA”, *The Washington Post*, 8 de noviembre, p. A1.
- Platt, Washington (1957), *Strategic Intelligence Production: Basis Principles*, New York: Frederick A. Praeger.
- Pulido, Julia (2007), “Las respuestas de la Inteligencia norteamericana ante la amenaza terrorista”, en Navarro, Diego y Esteban, Miguel A. (Coord.), *Terrorismo global: gestión de información y servicios de inteligencia*, Madrid: Plaza y Valdés, pp. 49-64.
- Reynolds, Paul (2004) “Long history of intelligence failures”, *BBC News*. Disponible en: http://news.bbc.co.uk/2/hi/middle_east/3883605.stm
- Rodríguez Fernández, Andrés (1993), “La cultura en las organizaciones públicas y privadas”, *Psicothema*, Vol. 5 (suplemento), pp. 237-260.
- Rosales, Ignacio A. (2005), “La Inteligencia en los procesos de toma de decisiones en la seguridad y defensa”, en *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional* (Cuadernos de Estrategia, nº 130), Madrid: Instituto Español de Estudios Estratégicos/Centro Nacional de Inteligencia, pp. 39-64
- (2007), “Conceptos clave: Integración, Inteligencia compartida y análisis”, en Navarro, Diego y Esteban, Miguel A. (Coords.), *Terrorismo global. Gestión de información y servicios de inteligencia*, Madrid: Plaza y Valdés, pp. 127-143.
- Russell, Richard L. (2004), “Intelligence Failures: The wrong model for the war on terror”, *Policy Review*, No. 123, pp. 61-72.
- Saiz Cortés, Alberto (2009), “Intervención del Secretario de Estado Director del CNI en la presentación del Máster Interuniversitario en Analista de Inteligencia”, Universidad Rey Juan Carlos, 26 marzo.
- Sansó-Rubert, Daniel (2007), “¿Es la Inteligencia la respuesta a los nuevos riesgos y amenazas?”, *Revista Ejército*, No. 794, pp. 78-84.
- Shulsky, Abram N. & Schmitt, Gary J. (2002), *Silent Warfare: Understanding the World of Intelligence* (3rd. Ed.), Dulles, VA: Potomac Books Inc.
- The Washington Post (2002), “CIA feels strain of Iraq and Al Qaeda”, 17 noviembre.
- Travers, Russ (1997), “A Blueprint For Survival: The coming Intelligence Failure”, *Studies in Intelligence*, No. 1, pp. 35-43.
- U.S. Senate (2002), “Report of the joint inquiry into the terrorist attacks of September 11, 2001”, S. Report No. 107-351, 107th. Congress, 2d. Session, December 10.
- (2004), “Report of the Select Committee on Intelligence on the Intelligence Community’s prewar Intelligence assessments on Iraq”, S. Report No. 108-301, 108th. Congress, 2d. Session, July 9.
- Watanabe, Frank (1997), “Fifteen Axioms for Intelligence Analysts”, *Studies in Intelligence*, Vol. 1, pp. 45-47.
- Waterman, Shaun (2004), “Bush orders massive CIA recruitment drive”, *United Press International*, 24 noviembre. Disponible en: http://www.upi.com/Business_News/Security-Industry/2004/11/24/Bush-orders-massive-CIA-recruitment-drive/UPI-39571101341622/
- Wilensky, Harold L. (1967), *Organizational Intelligence*, New York: Basic Books.

Wohlstetter, Roberta (1962), *Pearl Harbor: Warning and Decision*, Palo Alto (Ca): Stanford University Press.