Gobernanza de la seguridad: seguridad inteligente frente a las nuevas amenazas

ANDRÉS MONTERO GÓMEZ

Adjunto al director del Gabinete de Análisis y Prospectiva
de la Secretaría de Estado de Seguridad

La gobernanza de la seguridad es la administración y gestión de la seguridad colectiva y, por tanto, el gobierno del riesgo, pero también del miedo y por tanto de la inseguridad. En las sociedades democráticas significa, además, que los procedimientos y marcos de gobierno de la seguridad colectiva y pública deben ser diseñados, articulados y evaluados ajustándose a estándares democráticos de legalidad y transparencia, eso que la cultura anglosajona ha recogido bajo el término *accountability*.

Como todos los abordajes democráticos de la *res publica*, la gobernanza de la seguridad demanda también una especie de separación de poderes. En democracia, la seguridad está indisolublemente impregnada del Estado de derecho y éste del imperio de la ley. Por tanto, existe un poder ejecutivo de la seguridad, un poder legislativo y otro judicial. Una tríada democrática de la seguridad que en nuestros Estados está, tal como le pasa al triángulo de la separación de poderes, desequilibrada hacia el ángulo del gobierno, del ejecutivo, en detrimento del legislativo y, aunque menos, del judicial. Podría decirse que el triángulo de la seguridad es más escaleno que equilátero. La traducción efectiva de esta descompensación se encuentra adherida al título de esta ponencia... el gobierno de la seguridad reside, y cada vez lo hará más, en su dimensión ejecutiva y, por tanto, en posiciones de seguridad dura.

Dentro del continuo que puedan representar les ciencias de la seguridad, las aproximaciones duras de la disciplina están bastante alejadas de la flexibilidad, ambigüedad, globalidad y versatilidad de las amenazas sociales actuales. Estas amenazas, que son transfronterizas, no responden ya ni siquiera a la configuración tradicional de un elemento que busca ocasionar un perjuicio con tal de obtener un beneficio. El terrorismo y la delincuencia organizada tienen en su *leit-motif* aprovechar las debilidades del sistema para obtener una ganancia ilícita. Asimismo, asumen que para alcanzar esa ganancia deben hacerlo a partir del ejercicio de la violencia, de la imposición por medio de la fuerza. La posibilidad de un

perjuicio es un elemento asumido y, sobre todo para el terrorismo, instrumentalizado. En cambio, otras amenazas que actualmente afectan a nuestras sociedades, como la inmigración (Montero, 2005) o aquellas derivadas de las descompensaciones medioambientales (Curbet, 2002) no tienen en su naturaleza el componente de causar daño sino que, muy al contrario, emanan directamente de disfuncionalidades inherentes al propio sistema social que hemos construido y amenazan su bienestar, su estabilidad y, por tanto, su seguridad. La seguridad moderna, entendida así, trasciende por tanto la conceptuación tradicional de una respuesta frente a una amenaza aversiva administrada de forma intencionada por agentes externos para pasar a convertirse en una configuración de esquemas, situaciones o disposiciones estructurales que no sólo responden sino que anticipan y prevén riesgos, riesgos que potencialmente erosionan o afectan a formas de convivencia elegidas o establecidas.

El gobierno de nuestra seguridad aún está demasiado orientado a medidas ejecutivas de respuesta reactiva, aún es poco proclive a planteamientos anticipatorios estructurales que tengan en cuenta la multidimensionalidad de los resortes democráticos frente a la complejidad de las nuevas amenazas y, por descontado, demasiado orientado a medidas de seguridad dura, ya sea policial o defensiva. Nuestros sistemas de seguridad no contemplan la disposición global de los riesgos. Tampoco la necesidad de contar con la implicación social, más allá de las organizaciones públicas especializadas en seguridad reactiva, para afrontarlos. Dicho esto, por lo que respecta a las amenazas que causan un daño social intencional en el horizonte de sus ganancias, como el terrorismo o la delincuencia organizada global, ni siquiera los sistemas de seguridad han conseguido adaptar sus enfoques a la personalidad de los retos. Desde hace décadas, el tratamiento de las amenazas de seguridad ha consistido en un abordaje sintomático, no basado en el conocimiento etiológico de los fenómenos sino en contrarrestar su presencia y efectos nocivos. El resultado es que las amenazas, como el tráfico de drogas o el terrorismo, llegan a contenerse a niveles estructurales, manteniéndose como males sociales crónicos, cuyo arraigo a veces se ve reforzado por las propias políticas públicas de respuesta.

En una sociedad del conocimiento, la intervención basada en el conocimiento y, por tanto, en la evidencia se plantea cada vez más como una medida efectiva en el momento de articular esquemas de respuesta, obligatoriamente, además, si pretende dotarse de alguna cualidad anticipatoria o preventiva. La seguridad basada en el conocimiento es seguridad inteligente, sustanciada en procedimientos de obtención, evaluación, análisis e interpretación de la información sobre las amenazas que consiguen desvelar las claves de un comportamiento que pueda ser pronosticado con unos márgenes de error asumibles.

1. Seguridad inteligente basada en el conocimiento

Los adecuados desarrollo e implementación de capacidades, procedimientos y medios de inteligencia son considerados actualmente claves para el provecho

exitoso de la delincuencia organizada y del terrorismo global a largo plazo (Montero, 2003; Lamo, 2004). En las modernamente llamadas ciencias de la seguridad, la inteligencia comprende las actividades, procesos e instituciones dedicadas a la obtención, tratamiento y difusión de información sobre áreas u objetivos de interés para la seguridad de las naciones.

A pesar de que no se ha llegado a un acuerdo en torno a la noción de inteligencia de seguridad, Esteban Navarro (2004) considera, con Troy (1991), la inteligencia para la seguridad como la poseedora de tres rasgos distintivos: la amenaza a la seguridad como objeto; la conversión, mediante análisis, de información recogida a través de una variada aplicación de instrumentos y fuentes; y su carácter reservado, a pesar de que muchas de las fuentes informativas sean de procedencia pública. En el ámbito de las ciencias de la seguridad, la inteligencia estaría conformada por una doble conceptuación: la inteligencia como proceso y la inteligencia como producto. En tanto que proceso, inteligencia de seguridad sería aquel conjunto de operaciones destinado a tratar y analizar la información relacionada con un entorno de seguridad. El tratamiento de esta información atraviesa todo un ciclo autoalimentado, el proceso de inteligencia que ustedes conocen muy bien y que, partiendo de los planes directivos que marcan los objetivos informativos, pasa por la puesta en marcha de recursos destinados a la obtención de información sobre todos los factores relacionados con los objetivos de información, para posteriormente dedicar capacidades analíticas a la elaboración de esta información en bruto hasta convertirla en inteligencia. La fase final de este proceso, la difusión de la inteligencia de seguridad, entronca con la naturaleza de producto de esta inteligencia. De este modo, el producto de inteligencia es consumido por personas u órganos a los que se difunde, habitualmente, para sustanciar mecánicas de toma de decisiones. A riesgo de simplificar, es válido concluir que el producto de la inteligencia de seguridad sirve a personas situadas en niveles de decisión para optar entre una o varias de las alternativas de respuesta frente a un determinado espacio problema.

Entonces, también sin profundizar demasiado, sigo ese razonamiento considerando que para las fuerzas y cuerpos de seguridad de España, igualmente y en sus áreas de competencia para instituciones como las aduanas o el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales, el espacio problema viene determinado por cómo garantizar el ejercicio de las libertades públicas y la seguridad ciudadana frente a unas amenazas que se resisten, diría que incluso ontológicamente, a los planteamientos analíticos lineales que hemos estado aplicando de manera tradicional para su desactivación. Y digo únicamente desactivación porque, hasta el momento, los organismos de seguridad no se han dado cuenta —en la mayoría de los casos porque difícilmente han interiorizado que ésta era su misión— de que la comprensión de la naturaleza y de las amenazas es la vía más lenta, pero también la más efectiva a largo plazo para que la desactivación no devuelva la amenaza a un estado latente del cual emerger después, sino para que lleve a su erradicación, a su fractura, en definitiva, a su desnaturalización.

Hasta hace muy poco, nuestra aproximación lineal y reactiva a las amenazas ha funcionado. De hecho, la mayoría de ustedes saben que continúa siendo efi-

ciente. Resolvemos muchos de los esquemas delictivos a través de brillantes investigaciones, nuestros indicadores no son ni mucho menos deficientes (en estadísticas sobre drogas y terrorismo somos potencias mundiales) y España es un país con una seguridad objetiva muy aceptable. Con todo, de repente se inmolan unos cuantos terroristas y asesinan a centenares de conciudadanos. O sin establecer el foco en un desgraciado atentado puntual, podemos mirar el plato de nuestra vajilla de porcelana por debajo y descubrir qué esconde en su contacto con el mantel; ¿por qué incautamos tanta cocaína en nuestro país?, ¿por qué los atentados islamistas de Casablanca y ambos «onces» tienen todos ellos múltiples interconexiones establecidas en España?, ¿qué grado de asentamiento tiene la criminalidad organizada transnacional en nuestro territorio? En resumen, estamos simplemente rascando el contorno superficial del fenómeno en tanto que el núcleo queda fuera de nuestro alcance y adaptado estructuralmente a nuestro contexto social.

Las nuevas amenazas no son nuevas. Es cierto que a veces las llamamos así para compensar psicológicamente nuestro retraso frente a ellas. Si son nuevas, nos decimos y les decimos, dejadnos por favor un tiempo para conocerlas y desmantelarlas. En realidad, son las amenazas de siempre, pero evolucionadas, en un sentido netamente darvinista si ustedes quieren, en los rasgos de personalidad de la sociedad global. Nosotros, el colectivo de la seguridad pública, también hemos evolucionado, nuestras estructuras internas se han modernizado, nuestros directivos han incorporado a sus estilos de gestión las más recientes técnicas de *management*, nuestros profesionales acceden a las instituciones con unos niveles aceptables de educación formal, nos hemos abierto a las nuevas tecnologías... A pesar de todo nuestras organizaciones son lentas, pesadas, muy burocratizadas, de personalidad conservadora, y están atrapadas en una orientación de profunda aversión al riesgo. Muy al contrario de las amenazas que constituyen el objeto de nuestro trabajo. Pero sobre la crítica constructiva volveremos después.

Las amenazas globales, que sintéticamente reuniremos bajo la etiqueta de delincuencia organizada global, tienen unos rasgos de personalidad distintivos: son transnacionales, son de estructura horizontal, difusa, interconectada y son inteligentes. Si me permiten el símil darvinista, entenderemos la inteligencia de la delincuencia organizada o del terrorismo como su capacidad de adaptarse a un ecosistema hostil, vigilado y rastreado por dispositivos de seguridad permanentes, para alcanzar propósitos que vulneren los límites establecidos por unas reglas de conducta, que en este caso están orientadas hacia el cumplimiento de la ley. La progresiva modificación de la fisonomía de los *cárteles* latinoamericanos dedicados al tráfico ilícito de cocaína o la creciente sofisticación de esquemas de blanqueo de capitales en grupos de delincuencia organizada son ejemplos de adaptabilidad y comportamiento inteligente; pilotar aviones comerciales en trayectos domésticos en EE.UU. para utilizarlos como gigantescos artefactos explosivos voladores dirigidos contra símbolos importantes de nuestra civilización, trasladando un mensaje multinivel destinado a varias audiencias a través de devastadores actos criminales, constituye otro trágico escenario de planificación lateral que se adapta a la previsibilidad de nuestras planificaciones. Por descontado que esta

inteligencia no está relacionada con ninguna acepción moral del concepto, pero incluso si llegásemos a debatir sobre esta dimensión observaríamos cómo grupos terroristas, sobre todo, han construido códigos morales propios que les permiten adaptar su propia conducta de manera egosintónica para autovalidarse el comportamiento violento en términos psicológicos. Sin tener que hacer elucubraciones demasiado complejas, la adaptabilidad criminal pide, al menos, la misma capacidad proactiva de los esquemas de seguridad dispuestos para proteger los límites (libertades públicas y seguridad ciudadana, transcribe nuestra Constitución) de este ecosistema donde las organizaciones criminales actúan como depredadores, aunque únicamente fuera para nivelar nuestra capacidad de respuesta frente a su adaptabilidad.

La inteligencia criminal es un espacio cualitativamente avanzado de la investigación criminal, una metodología propia de las policías judiciales y de los servicios de información policiales inscritos en causas judiciales contra la delincuencia. A pesar de todo, una aproximación integral a la seguridad requiere la extensión de la inteligencia —entendida como un proceso, como un producto y como especialidad policial institucionalizada— al propio engranaje de seguridad dispuesto para desactivar la delincuencia organizada y al terrorismo desde una perspectiva preventiva.

Considerada la inteligencia de seguridad como un marco superestructural en una renovada orientación de las agencias públicas de seguridad, quiero identificar la seguridad basada en el conocimiento como el primer componente de la seguridad inteligente. Numerosos esquemas de seguridad tradicionales se sostienen en una asunción horizontal, generalista, según la cual un determinado sistema en riesgo (entorno individual, entorno corporativo o entorno social) debe ser protegido mediante el blindaje reactivo contra un repertorio de amenazas eventuales. Es la aplicación de una doctrina lineal de distanciamiento, de encapsulamiento, de aislamiento del objeto de seguridad en lo que respecta a las amenazas que suponen un riesgo.

A menudo, estos sistemas tradicionales de seguridad, basados en la interposición de barreras físicas, en la contención o en la disuasión de las amenazas, ignoran completamente cualquier análisis sobre el comportamiento de los agentes amenazadores, sobre el triple anillo de contextos (el contexto del objeto en riesgo, el contexto de inserción de la amenaza y el contexto de interrelación que configura la amenaza con la sociedad o con sus agentes cuando se introduce en el espacio de seguridad) y sobre el comportamiento y capacidades de respuesta de los agentes a los que se somete a seguridad. La primera particularidad de la seguridad inteligente es su radicación en el conocimiento de toda la configuración de elementos que inciden en un espacio concreto de seguridad.

La inteligencia de seguridad basada en el conocimiento no es un componente surgido del capricho metafísico, la modernidad intelectual que de repente se introduce en el ámbito de la seguridad o un simple revestimiento conceptual o académico que dé cobijo con una imagen de sofisticación a medidas de seguridad tradicionales. La inteligencia de seguridad simplemente ahorra costes de procedimiento y estructura (es eficiente), por un lado, y ajusta criterios entre medios e incluso disminuye los efectos colaterales introduciendo precisión y selectividad en las herra-

mientas aplicadas para la consecución de objetivos (es efectiva), por el otro. Y eso es así porque la seguridad es subsidiaria del conocimiento exhaustivo del medio en el que opera.

Muy a menudo, la seguridad tradicional no tiene en cuenta un análisis de la personalidad de la amenaza y, por tanto, de sus potenciales de variación, de manera que deja expuesto el objeto de seguridad frente al más mínimo cambio de las condiciones iniciales. De este modo, lo único que se sabe de la amenaza es que produce un riesgo y puede suponer un peligro, y lo único que se sabe del objeto de seguridad es que es vulnerable y, por tanto, debe protegerse interponiendo espacio y obstáculos entre él y sus amenazas o, si no, erosionando la capacidad de producir riesgo de las amenazas.

2. Seguridad adaptativa y proactiva

Otra de las propiedades de la seguridad inteligente es su adaptabilidad. En el otro extremo de las medidas de tipo rígido, estáticas y con vocación de inmutabilidad, la nueva seguridad responde a esquemas flexibles, autoevaluables y cambiantes en función de la interacción entre las propiedades de los diversos agentes presentes en el escenario de seguridad. El objetivo es alcanzar un sistema que aprenda de sí mismo, que es una de las propiedades intrínsecas de la inteligencia.

La adaptabilidad no es una función reactiva frente a la amenaza, frente a la delincuencia organizada o al terrorismo. Muy al contrario, está determinada por la anticipación basada en el conocimiento de las características de las amenazas. Desde el conocimiento integral de la amenaza y de su contexto de inserción, pero también de la personalidad y habilidades de respuesta de las agencias de seguridad, se diseñan esquemas a medida que tengan en cuenta la evolución longitudinal del comportamiento de los actores. Para conseguir la adaptabilidad de un sistema de seguridad, es imprescindible dotarlo, primero, de recursos de inteligencia y, segundo, involucrar metodología prospectiva en estos recursos.

El objetivo de construir un sistema que aprenda de sí mismo pasa por incorporar protocolos de autoevaluación en cada esquema de seguridad. Estos protocolos, que pueden ser implantados desde órganos centrales de seguridad en toda una diversidad de proyectos a su cargo, deben formar una dimensión horizontal de cada sistema de seguridad. De este modo, se garantiza que cada uno de los recursos y procedimientos en marcha siempre responden a una necesidad evaluada, que no tienen efectos disfuncionales indeseados y que se ajustan a una racionalización permanente de los costes.

Un ejemplo bastante evidente de los problemas de adaptabilidad de los sistemas de seguridad, públicos y privados, se encuentra de nuevo en el modo de enfrentarse al terrorismo. La utilización de un esquema táctico concreto por parte de un grupo terrorista en los atentados que sacudieron Estados Unidos de América el 11 de septiembre de 2001 se ha traducido en un sobredimensionamento irracional de medidas de seguridad en los aeropuertos de todo el mundo. Este sesgo

está ignorando, sistemáticamente, la capacidad adaptativa que, en este caso, sí que rige el comportamiento de organizaciones criminales y bandas terroristas.

En la extensión de una introducción irreflexiva de recursos de seguridad en el transporte aéreo influyen, está claro, factores de contexto geoestratégico y elevadas dosis de politización. El hecho de que los atentados con gas sarín en el metro de Tokio en el año 1995, realizados por el grupo Aum Shinrikyo, no se tradujeran en una multiplicación de los sistemas de seguridad en las líneas metropolitanas de todo el mundo y, en cambio, los atentados aéreos del 11-S sí que han producido una práctica unanimidad en la extrapolación lineal de rígidas metodologías de seguridad a escala internacional, deja entrever la complejidad que envuelve a la seguridad objetiva y, sobre todo, a la subjetiva. Otro detalle anecdótico, además de tremendamente revelador, es que el descubrimiento de un artefacto explosivo chapucero en el zapato de un pasajero ha desencadenado una obsesiva búsqueda de amenazas en los zapatos de los viajeros de todo el mundo.

Estas viñetas de la vieja seguridad frente al nuevo terrorismo nos indican, obstinadamente, de qué manera las planificaciones están obviando un análisis en profundidad de la personalidad de la amenaza terrorista, que obstaculiza la instrumentación de medidas preventivas y anticipatorias. Es indudable que los planificadores y estrategas en el bando de las amenazas innovan, aplican el pensamiento divergente no en sus doctrinas pero sí en sus tácticas y buscan siempre abrir un túnel lateral en los esquemas de seguridad dispuestos para impedir o dificultar sus acciones. Todas nuestras respuestas describen una alineación central en tanto que el terrorismo o la delincuencia organizada circulan por los carriles laterales.

Por decirlo de un modo más sintético, la proactividad (de la que se lleva más de una década hablando en la seguridad pública y más aun en la seguridad privada) es la concepción según la cual, una vez analizadas las amenazas potenciales en un entorno y sus eventuales cursos de comportamiento, se diseñan acciones que modifiquen estos cursos de comportamiento, anticipándose a la dinámica de la amenaza para reducir el riesgo sobre un determinado entorno. Evidentemente, a mayor complejidad en la definición de la amenaza, más dificultad presentará la previsión de su comportamiento y, por tanto, menos posibilidades se ofrecerán de acción proactiva para minimizar o impedir el peligro latente. Actualmente, en la ya de por sí intrincada realidad internacional multipolar, las amenazas complejas para nuestras sociedades se encuentran íntimamente relacionadas ya sea con fenómenos delictivos o bien con propuestas interestatales conflictivas, que contienen en ambos casos la presencia de grupos de personas con intenciones hostiles, contornos grupales cerrados y excluyentes y búsqueda de beneficios personales, en términos económicos o de poder, que se sitúan por encima de la ley y de los derechos humanos.

La naturaleza fundacional de las comunidades de inteligencia es la prevención de las amenazas. No específicamente investigarlas o reprimirlas, sino esencialmente prevenirlas. La articulación de medios de observación e investigación, de análisis e interpretación de la realidad, sería subsidiaria a este horizonte de prevención y evitación de peligros, amenazas y agresiones. Una inteligencia con identidad preventiva.

La prevención de la delincuencia organizada transnacional o del terrorismo en el futuro no pasa por la seguridad sino por la inteligencia o, mejor dicho, por una seguridad emanada de la inteligencia. El primer ministro británico Tony Blair simbolizó acertadamente este planteamiento al afirmar que «si puede extraerse alguna lección del 11-S, ésta es la importancia de no esperar a que se materialice la amenaza». La clave está, pues, en la prevención basada en la inteligencia, es decir, en la comprensión adecuada de las dinámicas del fenómeno terrorista con el propósito de anticiparse proactivamente.

3. Patologías de la inteligencia

A pesar de todo, mucho antes del terrorismo en masa del 11-S, ya se advertían instaladas en las comunidades de inteligencia, ya fuesen las consideradas tradicionales o las denominadas criminales, determinadas tendencias viciadas que comprometían las capacidades de los actuales modelos de análisis de la información en los servicios de inteligencia y seguridad, que llevan años sufriendo de una rigidez que impide su evolución a un ritmo adecuado para prevenir el comportamiento de amenazas complejas. En concreto, dos patologías modernas del análisis de inteligencia eran (y continúan siendo, a mi entender) su politización, por un lado, y su incapacidad para procesar adecuadamente escenarios de incertidumbre, por el otro.

En lo que respecta a la politización de la inteligencia, su efecto más perverso, en el lado del analista, se observa en informes que confieren más probabilidad de ocurrencia a sucesos que se consideran más probables a priori en el pensamiento dominante de la corriente política en el poder en un instante determinado (por ejemplo, los informes que ponen de manifiesto que España es la puerta de entrada de la cocaína a la Unión Europea son consumidos y asimilados por las autoridades europeas sin resistencia alguna, en tanto que aquellos que cuestionan esta visión encuentran muchas dificultades de aceptación). En el lado del consumidor del informe, entonces, la politización de la inteligencia se traduce en conceder una mayor virtualidad y, por extensión, en otorgar medios para desarrollar acciones basadas en eso, a análisis que coinciden con su planteamiento en lo que respecta al asunto de se trate. En la investigación en el área de la psicología cognitiva se han dedicado numerosos experimentos a demostrar, con un éxito abrumador, que cuando un esquema mental para explicar cierto escenario social se encuentra sólidamente alojado en nuestro cerebro, si la información que procesamos de nuestro entorno no es coincidente con la perspectiva que ya hemos asumido, no modificamos nuestros esquemas para adaptarlos a la realidad, sino que, por el contrario, intentamos deformar la realidad hasta ajustarla a nuestros esquemas. Los analistas favorecen de manera natural la información que mejor se ajusta a sus modelos mentales previos, a menudo menospreciando cualquier información que pueda abonar una hipótesis alternativa (Montero, 1998, 2004; George, 2004). Los analistas deberían estar entrenados para evitar este efecto, aunque sus intereses personales o corporativos aconsejen a veces politizar sus conclusiones. El programa

Prospint, hasta ahora a través de su módulo de razonamiento, introduciendo un módulo específico de análisis alternativo, incidirá en la reversión de esta patología. A través del análisis alternativo, formaremos a la comunidad de profesionales que pretendemos establecer técnicas para revelar asunciones analíticas inconscientes o para cuestionar evidencias o lógicas débiles, considerando hipótesis o resultados alternativos, incluso en ausencia de evidencia aparente.

El análisis, por definición, trata con incertidumbres, ya que de no ser así no necesitaríamos un procesamiento sistemático de información cuando esta misma nos revelase conclusiones ciertas. Pues bien, esta incertidumbre nos lleva a la segunda patología de la inteligencia, la lucha contra aquello que resulta increíble. Aquí las cosas son más complejas si es posible, ya que se relacionan íntimamente con la previsión cualitativa y con los escenarios culturalmente aceptables. Esta clase de previsiones, que a diferencia de las predicciones meteorológicas no están centradas en cálculos matemáticos, se dedican a conocer futuros probables y posibles a partir de análisis conceptuales y de significados, es decir, a describir el comportamiento de un fenómeno complejo y a trazar su evolución y tendencia. El objetivo sería, de esta manera, anticiparse a un punto determinado de la tendencia evolutiva de un problema, como es el terrorismo, cortocircuitando su desarrollo. A pesar de todo, la utilización de herramientas para el análisis cualitativo era tan precaria el 11 de septiembre de 2001 como lo es ahora. Aunque desde mucho antes se dispone de técnicas como la de escenarios, que permite construir futuribles a partir de una combinación precisa de indicadores, los analistas realmente capacitados para implementarla y los políticos preparados para consumir los informes que de ella se derivan son del todo escasos. A eso debemos añadirle la dificultad de los propios analistas para valorizar piezas de información muy novedosas (por ejemplo, contextualizar adecuadamente indicios que le decían al FBI que un cierto número de personas seguían clases de vuelo en los EE.UU.) cuya ecuación analítica nos conduce a combinaciones concluyentes que resultan increíbles (estrellar aviones contra las Torres Gemelas) para los modelos mentales sesgados del propio analista, incapaz de librarse de sus creencias sobre cómo ha de funcionar el mundo y hasta dónde es capaz de llegar la conducta humana.

Otros impedimentos para que nuestra seguridad sea proactiva y preventiva entroncan directamente con la personalidad de nuestras propias instituciones. Lo ha escrito Walter Laqueur, director del prestigioso Instituto de Estudios Estratégicos de Washington.[1] En la cultura de los servicios de inteligencia y seguridad debe operarse un cambio psicológico que introduzca la innovación y el atrevimiento, desbancando a la burocracia y a la rutina. En la misma línea, el analista de la Rand Corporation Brian Jenkins (2004) se pregunta si no será que los servicios de inteligencia no están psicológicamente preparados para gestionar la naturaleza dinámica y cambiante del terrorismo global y, nosotros añadiremos, de la delincuencia organizada global. Instituciones públicas de seguridad ancladas en

1. Laqueur, W. «Las desgracias de la CIA». *La Vanguardia*, 15 de junio de 2004.

estructuras muy burocratizadas, procedimientos operativos rígidos, infravaloración de la cultura de análisis, anémica y poco imaginativa gestión de las fuentes humanas de información.

España dispone de unos excelentes servicios contraterroristas y de inteligencia criminal. Tenemos problemas de integración de los diferentes elementos de inteligencia de seguridad en un verdadero esquema nacional, igual que en otros países. A pesar de todo, el principal obstáculo de la inteligencia de este período de globalización no es estructural sino, como apunta lúcidamente Laqueur, cultural. La nueva delincuencia global reclama una nueva cultura de la inteligencia, una nueva seguridad inteligente.

La cultura institucional o personalidad corporativa determina el comportamiento de las organizaciones. Igual que la personalidad individual marca la conducta del ser humano. La orientación de los servicios de información de las fuerzas de seguridad está muy influida por la identidad policial de sus miembros. En lo que respecta al CNI, es predominante una cultura militar heredada de sus organizaciones matrices, desde el SECED de Carrero Blanco hasta el reciente CESID, a pesar de la entrada entre sus directivos de personal civil universitario. Pues bien, la identidad policial o militar de los agentes de inteligencia contraterrorista no es necesariamente negativa, pero imprime unos ciertos condicionantes, generalmente relacionados con la rigidez de pensamiento.

La rigidez en el razonamiento analítico se nutre, esencialmente, de tres obstáculos: uno estructural, otro metodológico y un último de procedimiento. El estructural procede de una jerarquía vertical muy burocratizada, incompatible con el comportamiento de amenazas flexibles, dinámicas y horizontales (Esteban Navarro, 2004). La iniciativa y la innovación están penalizadas por el sistema, el cual tiende al conservadurismo extremo. En cambio, anticiparse a la delincuencia global requiere capacidad de proyectar escenarios, de ruptura, de manejar con soltura el pensamiento divergente. La cultura institucional de los servicios de inteligencia sanciona la creatividad en beneficio de la burocracia.

El obstáculo metodológico procede de una deficiente especialización en herramientas de procesamiento analítico de la información. Aunque parezca sorprendente, los centros de conocimiento por excelencia, institutos de investigación o universidad, no transfieren con el dinamismo deseable todo el saber instrumental sobre herramientas para pensar, para extraer conclusiones. Son pocos los analistas de seguridad capaces de extraer hipótesis y conclusiones como si fuesen científicos, por mucho que llevemos años repitiéndonoslo a nosotros mismos, a la manera de un mantra, más que poniendo realmente los medios para materializar este horizonte. Es más, se trata de una orientación cultural no muy bien vista por la personalidad institucional. Progresivamente, se están abriendo puentes de comunicación entre ambos mundos, pero continúan siendo lentos y desconfiados.

En lo que respecta al obstáculo de procedimiento, que intima con la identidad policial de la mayoría de los analistas, está imbricada en la excesiva dependencia de los hechos a la hora de interpretar la realidad. La dependencia de los hechos es el eje medular, sin duda, de las investigaciones policiales. Lo que ocurre es que esta dependencia se ha alojado en la personalidad grupal de los servicios de inteli-

gencia criminal, de manera que a sus analistas les provoca verdadero pánico razonar, y mucho más hablar, en términos de probabilidad de ocurrencia. El grueso de los análisis se detiene en cuanto el especialista que los redacta se encuentra frente a escenarios cargados de incertidumbre. El analista no se atreverá a extraer conclusiones y si, en una pulsión de audacia, lo hace, probablemente no encontrará los medios para transmitir con eficacia el escenario a sus superiores jerárquicos.

Estos obstáculos se están confirmando *in vivo* en los ejercicios de evaluación dentro de los programas de capacitación de analistas de las agencias públicas de seguridad. Entre las observaciones se destaca cómo, por ejemplo, nuestros analistas se detienen y autocontienen en las etapas de procesamiento relacionadas con la extracción de conclusiones. El razonamiento, la extracción de conclusiones, es el momento crítico del proceso, donde el analista debe visualizar información que está contenida de manera latente en las premisas informativas pero que no sería observable sin poner en relación asociativa estos mismos elementos de información. Nuestra valoración en el momento de estudiar el comportamiento de los analistas nos ha llevado a dos planteamientos: por un lado, los profesionales se sienten inseguros por no haber sido dotados de metodología para el pensamiento sistematizado; por el otro, están inquietos porque parte de su identidad corporativa está construida sobre la sanción de la especulación argumental. En nuestras culturas corporativas de seguridad pública, la extracción de conclusiones está muy identificada, erróneamente, con la especulación, y por cuestiones también relacionadas con una subordinación jerárquica deficientemente interiorizada, la mayoría de nuestros analistas no están en condiciones de defender asertivamente un argumento, sobre todo si es *ex novo*, frente a sus directivos.

La solución no pasa, por descontado, por fracturar completamente las actuales personalidades corporativas. La alternativa sería introducir, en el seno de los propios servicios de inteligencia, mecanismos de corrección para compensar las derivas contraproducentes que puedan tener estas personalidades organizacionales.

En la misma línea de disfuncionalidades, habitualmente en los órganos de inteligencia de seguridad se produce una confusión entre la dirección y el análisis. Los servicios de inteligencia criminal se encuentran demasiado abajo en los organigramas policiales o están demasiado compartimentados como para producir análisis que tengan en cuenta todos los elementos. Cuando encontramos ni que sea un analista orgánicamente ubicado más arriba, resulta que no tiene acceso a información operativa y, por tanto, sus interpretaciones muestran deficiencias. Ahora mismo en muchas naciones (valoren ustedes mismos si el caso es aplicable a España) no hay un solo analista profesional de la seguridad pública que pueda interpretar un mapa completo y total de las investigaciones sobre terrorismo en su país por su incapacidad para manejar, al mismo tiempo, todas las piezas del puzzle informativo de interés. En algunos modelos, a menudo es un directivo en algún vértice institucional el que puede llegar a acumular todas las claves, pero no está necesariamente preparado en metodología de análisis, ya que no es un técnico, para procesar de forma concluyente todas las piezas de la información.

En ciertos países, las libertades públicas se garantizan basándose en un modelo que ha alimentado una cultura de seguridad pública sustanciada en la

competencia entre dos o más cuerpos nacionales de seguridad o policía. Un esquema de estas características tiene ventajas e inconvenientes. Entre los problemas, forjados durante décadas, se encuentra el hecho de que los servicios de inteligencia de seguridad han desarrollado personalidades institucionales allí donde la propiedad de la información y de sus fuentes es un valor.

En fin… hasta aquí hemos llegado con una serie de pinceladas más destinadas a la provocación de reflexiones que a establecer un juicio preciso e inequívoco de la realidad. Nos encontramos ante un reto formidable para las instituciones de inteligencia y seguridad de los Estados, que deben emplear medios de obtención de información más potentes e incisivos, como las operaciones de infiltración a largo plazo, pero también multiplicar el esfuerzo de sus órganos de análisis para liberarlos de viejas patologías que asienten rigideces estructurales. La garantía de una seguridad efectiva contra el terrorismo y el crimen organizado transnacional, ambos fenómenos complejos, depende hoy, más que nunca, de sistemas de inteligencia legítimos, flexibles y libres de anclajes racionales disfuncionales.

Bibliografía

Alonso-Fernández, F. (1994) *Psicología del Terrorismo.* Barcelona: Masson-Salvat.

Andrés Pueyo, A. (1997) *Manual de psicología diferencial*. Barcelona: McGraw-Hill.

Arent, H. (1972) *Le système totalitaire.* París. Seuil.

Atran, S. (2003) «Genesis of suicide terrorism». *Science,* 299:1534-1539.

Bilbeny, N. (1993) *El idiota moral.* Barcelona: Anagrama.

Blanco, A. (2004) «El avasallamiento del sujeto». *Claves de Razón Práctica*, 144 (12-21).

Crenshaw, M. (1995) *Terrorism in context.* University Park: Pennsylvania State University Press.

Curbet, J. (2002) «El suicidio de la especie». *Seguridad Sostenible*, 7.

Domínguez Iribarren, F. (1998) *ETA: estrategia organizativa y actuaciones: 1978-1992.* Bilbao: UPV.

Esteban Navarro, M.A. (2004) «Necesidad, funcionamiento y misión de un servicio de inteligencia para la seguridad y la defensa». En *Estudios sobre Inteligencia, Cuaderno de Estrategia nº 127*, Instituto Español de Estudios Estratégicos.

George, R.Z. (2004) «Fixing the problem of analytical mind-sets: alternative analysis». *International Journal of Inlelligence and Counterintelligence*, 17(3): 385-405.

Jenkins, B. (2004) «Redefining the enemy». *Rand Review*, 28(1): 16-23.

Kepel, G. (2000) *Jihad: expansion et déclin de l'islamisme.* París: Éditions Gallimad.

Lamo de Espinosa, E. (2004) *Bajo puertas de fuego.* Madrid: Taurus.

Laval, G. (1995) *Malaise dans la pensée. Essai sur la pensée totalitaire.* París: Publisud.

Lowenthal, M. (1993) «Intelligence Epistemology: dealing with the unbelievable». *International Journal of Intelligence and Counterintelligence*, 6(3): 319-325.

Moghadam, A. (2003) «Suicide bombings in the Israeli-Palestinian conflict: a conceptual framework». *Studies in conflict and terrorism*, 26(2): 65-92.

MONTERO, A. (1998) «Servicios de Inteligencia». *Ejército. Revista de las Armas y Servicios*, 686: 28-47.

MONTERO, A. (2003a) «Una hipótesis psicológica sobre los correlatos neurocognitivos de la violencia sistemática del terrorismo». *Psicopatología Clínica Legal y Forense*, 3(1): 87-99.

MONTERO, A. (2003b) «Inteligencia para la seguridad contra el terrorismo». *Gobernanza y Seguridad Sostenible*, 10.

MONTERO, A. (2004) «Psicología del terrorismo e inteligencia contraterrorista». *Papeles del Psicólogo*, 88: 67-71.

MONTERO, A. (2005) «Vulnerabilidad de la inmigración ante la criminalidad». *Gobernanza y Seguridad Sostenible*, 26.

RAINE, A.; SANMARTÍN, J. (2000) *Violencia y Psicopatía.* Barcelona: Ariel.

REICH, W. (1990) *Origins of terrorism: psychologies, ideologies and states of mind.* Cambridge: Cambridge University Press.

REINARES, F. (1998) *Terrorismo y Antiterrorismo.* Barcelona: Paidós.

REINARES, F. (2001) *Patriotas de la muerte.* Madrid: Taurus.

SÁNCHEZ-CUENCA, I. (2001) *ETA contra el Estado*. Barcelona: Tusquets.

TROY, T.F. (1991) «The correct definition of intelligence». *International Journal of Intelligence and Counterintelligence*, 5 (4): 433-454.

WESTERFIELD, H.B. (1996) «Inside ivory bunkers: CIA analysts resist managers pandering». *International Journal of Intelligence and Counterintelligence*, 9 (4): 407-424.