Real Instituto Elcano

Inteligencia Prospectiva de Seguridad

Andrés Montero Gómez

Documento de Trabajo (DT) 24/2006

5/10/2006

Inteligencia Prospectiva de Seguridad

Andrés Montero Gómez [*]

Resumen: El terrorismo yihadista y la delincuencia organizada global no sólo han retado las tradicionales concepciones de seguridad interior y exterior, sino que están poniendo de manifiesto que la seguridad reactiva o que la seguridad desgajada de la inteligencia son respuestas obsoletas de los Estados ante las amenazas.

Introducción[1]

El terrorismo yihadista y la delincuencia organizada global no sólo han retado las tradicionales concepciones de seguridad interior y exterior, sino que están poniendo de manifiesto que la seguridad reactiva o que la seguridad desgajada de la inteligencia son respuestas obsoletas de los Estados ante las amenazas. El desarrollo de doctrina, métodos y órganos para la inteligencia prospectiva de seguridad se presenta como una opción estructural para proporcionar a las instituciones de seguridad capacidades de respuesta inteligentes, preventivas y proactivas ante las nuevas amenazas.

La seguridad pública es un concepto no reducible a la respuesta policial, sino un pilar horizontal de la libertad ciudadana que debe atender a todos los elementos que contribuyen a generar vulnerabilidades ante las amenazas, a desencadenarlas y a mantenerlas en el tejido social. La propuesta para ofrecer una respuesta funcional, eficaz y eficiente, es que los poderes públicos adopten enfoques de seguridad inteligentes basados en el conocimiento comprensivo de las amenazas. Ese conocimiento parte de análisis descriptivos exhaustivos de los fenómenos, para después adentrarse en explicar sus causalidades. La inteligencia basada en el conocimiento es el sustrato a partir del cual las instituciones de seguridad estarán en condiciones de abordar estudios prospectivos que sirvan de apoyo para la toma de decisiones hacia una seguridad preventiva, que reduzca los riesgos manejando sus incertidumbres.

De la respuesta reactiva a la preventiva

Dentro del continuo que pudieran representar las 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 para obtener un beneficio. El terrorismo y la delincuencia organizada tienen en su *leit-motif* aprovechar las debilidades del sistema para obtener una ganancia ilícita. Del mismo modo, *asumen* que para lograr esta ganancia deben hacerlo a partir del ejercicio de la violencia, de la imposición por medio de la fuerza. La ocasión de un perjuicio es un elemento asumido y, en cierto modo sobre todo desde el terrorismo, instrumentado. En cambio, otras amenazas que

[*] *Coordinador del programa Prospint de la Secretaría de Estado de Seguridad.*

[1] Las opiniones expresadas en este Documento de Trabajo no representan a ninguna organización o institución.

actualmente afectan a nuestras sociedades, como la inmigración o aquéllas derivadas de las descompensaciones medioambientales no tienen en su naturaleza esa componente de infligir un daño sino que, por el contrario, emanan directamente de disfuncionalidades inherentes al propio sistema social que hemos construido y, desde dentro de él, amenazan su bienestar, su estabilidad y, por tanto, su seguridad. La seguridad moderna, así entendida, debería trascender por tanto la conceptuación tradicional de respuesta ante una amenaza aversiva administrada de modo intencional por agentes externos, para pasar a convertirse en una configuración de esquemas, situaciones o disposiciones estructurales que no sólo respondan sino que anticipen y prevean riesgos, riesgos que potencialmente erosionan o afectan a modos de convivencia elegidos o establecidos.

El gobierno de nuestra seguridad todavía está demasiado sesgado hacia medidas ejecutivas de respuesta reactiva, poco nutrido por planteamientos anticipatorios estructurales que tengan en cuenta la multidimensionalidad de los resortes democráticos frente a la complejidad de las nuevas amenazas y, desde luego, 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 y participación sociales, más allá de las organizaciones públicas especializadas en seguridad reactiva, para su afrontamiento. Dicho esto, por lo que respecta a las amenazas que introducen 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 logrado 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, permaneciendo como males sociales crónicos, cuyo arraigo a veces es fortalecido 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 consigan desentrañar las claves de un comportamiento que pueda ser pronosticado con márgenes de error asumibles.

Seguridad inteligente basada en el conocimiento

Los adecuados desarrollo e implementación de capacidades, procedimientos y medios de inteligencia son considerados hoy en día claves para el afrontamiento exitoso de la delincuencia organizada y del terrorismo global a largo plazo.[2] En las denominadas 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.

Las nuevas amenazas no son nuevas. Es cierto que a veces las denominamos así para compensar psicológicamente nuestro retraso ante ellas... si son nuevas, nos decimos y les decimos, déjennos por favor un tiempo para conocerlas y desmantelarlas. En realidad son las amenazas de siempre, pero evolucionadas, en un sentido netamente darwinista, para adaptarse a –o tal vez para contribuir a conformar–los rasgos de personalidad de la sociedad global. Por otra parte, el colectivo de la seguridad pública también ha evolucionado: las estructuras internas de las instituciones de seguridad se han

[2] A. Montero, 'Crítica de la razón bélica contraterrorista', *Revista Sistema*, nº 193, julio de 2006, pp. 121-129.

modernizado, los directivos de seguridad han incorporado a sus estilos de gestión las más extendidas técnicas de *management*, los profesionales de la seguridad acceden a las instituciones con aceptables niveles de educación formal, nos hemos abierto a las nuevas tecnologías... sin embargo, las organizaciones públicas de seguridad continúan comportándose de manera lenta y pesada, de forma muy burocratizada, adoleciendo de una personalidad conservadora y atrapadas en una orientación de profunda aversión al riesgo. Todo lo contrario de las amenazas que constituyen el objeto de su trabajo.

Las amenazas globales, que sintéticamente pueden reunirse 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 se permite el símil darwinista, la inteligencia de la delincuencia organizada o del terrorismo la entenderemos como su capacidad para adaptarse a un ecosistema hostil, aquél vigilado y escudriñado por dispositivos de seguridad permanente, a fin de lograr propósitos que vulneran los límites establecidos por unas reglas de conducta, que en este caso están orientadas hacia el cumplimiento de la ley. La progresiva modificación en 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 los EEUU para utilizarlos como gigantes artefactos explosivos volantes dirigidos contra símbolos importantes de nuestra civilización, trasladando un mensaje multinivel destinado a varias audiencias por medio de devastadores actos criminales es otro trágico escenario de planificación lateral que se adapta a la previsibilidad de nuestras planificaciones. Por supuesto que esta inteligencia no está relacionada con ninguna acepción moral del concepto, pero incluso si llegáramos a debatir sobre esa dimensión observaríamos como 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.[3] Así pues, y sin adentrarnos en elucubraciones demasiado complejas, es fácil pensar que la adaptabilidad criminal demanda al menos la misma capacidad proactiva de los esquemas de seguridad dispuestos para garantizar nuestros límites (libertades públicas y seguridad ciudadana, transcribiría la Constitución Española) de convivencia en ese ecosistema en donde las organizaciones criminales actúan como depredadores, aunque únicamente fuera para equilibrar nuestra capacidad de respuesta ante su adaptabilidad.

Considerada la inteligencia de seguridad como marco superestructural en una renovada orientación de las agencias públicas de seguridad, quiero identificar a la seguridad basada en el conocimiento como el primer componente de la seguridad inteligente. Numerosos esquemas de seguridad tradicionales están sustentados en una asunción horizontal, generalista, según la cual un determinado sistema en riesgo (entorno individual, entorno corporativo o entorno social) debe de 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 con respecto 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 amenazantes, 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 conforma la amenaza con la sociedad o con sus agentes cuando se introduce en el espacio de seguridad), y sobre la personalidad y capacidades de respuesta de los agentes a los que se somete a

[3] A. Montero, 'Ensayo sobre la mente de un terrorista', *Debats*, nº 91, 2005-2006, pp. 62-71.

seguridad. La primera particularidad de la seguridad inteligente es su raíz en el conocimiento acerca de toda la configuración de elementos que inciden en un espacio de seguridad concreto.

La inteligencia de seguridad basada en el conocimiento no es un componente fruto 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 arrope con una imagen de sofisticación a medidas de seguridad tradicionales. La inteligencia de seguridad simplemente ahorra costes procedimentales y estructurales (es eficiente), por una parte, y ajusta criterios entre medios y fines, disminuyendo los efectos colaterales al introducir precisión y selectividad en las herramientas aplicadas para el logro de objetivos (es efectiva), por otra. Y esto es así porque la seguridad es subsidiaria del conocimiento exhaustivo del medio en que opera.

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

Seguridad adaptativa y proactiva

Otra de las propiedades de la seguridad inteligente es su adaptabilidad. Al otro extremo de medidas de corte rígido, estáticas y con vocación de inmutabilidad, la nueva seguridad debe responder 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 lograr un sistema que aprenda de sí mismo, que es una de las propiedades intrínsecas a la inteligencia.

La adaptabilidad no es una función reactiva ante la amenaza, ante la delincuencia organizada o el terrorismo. Antes 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 lograr la adaptabilidad de un sistema de seguridad es imprescindible dotarlo, primero, de recursos de inteligencia y, segundo, involucrar metodología prospectiva en esos 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 llevados a la práctica 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 esta manera, el plan de seguridad 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 costos.

Un ejemplo bastante evidente de los problemas de adaptabilidad de los sistemas de seguridad, públicos y privados, lo tenemos de nuevo en el afrontamiento del terrorismo. La utilización de un esquema táctico concreto por parte de un grupo terrorista en los atentados que sacudieron los EEUU el 11 de septiembre de 2001, se ha traducido en un sobredimensionamiento 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 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, sin duda, factores de contexto geoestratégico y elevadas dosis de politización. El hecho de que los atentados con gas Sarín en el metro de Tokio en 1995, llevados a cabo 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 hayan significado práctica unanimidad en la extrapolación lineal de rígidas metodologías de seguridad a escala transfronteriza, deja entrever la complejidad que rodea a la seguridad objetiva y, sobre todo, a la subjetiva. Otro detalle anecdótico aunque tremendamente revelador es que el descubrimiento de un burdo artefacto explosivo en el calzado de un pasajero, relacionado con el terrorismo yihadista internacional, haya desencadenado una obsesiva búsqueda de amenazas en los zapatos de los viajeros de todo el mundo.

Semejantes viñetas de la vieja seguridad ante el nuevo terrorismo nos indican, de un modo bastante obstinado, de qué manera las planificaciones están obviando un análisis en profundidad de la personalidad (personalidades) de la amenaza terrorista, que al tiempo obstaculiza la instrumentación de medidas preventivas y anticipatorias. Es indudable que los planificadores y estrategas en el lado de las amenazas innovan, aplican el pensamiento divergente no a sus doctrinas pero sí a sus tácticas y buscan siempre abrir un túnel lateral en los esquemas de seguridad dispuestos para impedir o dificultar sus acciones. Todas nuestras respuestas suelen describir un alineamiento central, mientras el terrorismo y la delincuencia organizada circulan por los carriles laterales.

Por expresarlo de modo sintético, la proactividad es la concepción según la cual, una vez analizadas las amenazas potenciales en un entorno y sus cursos de comportamiento eventuales, se diseñan acciones que modifiquen esos 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 albergará la previsión de su comportamiento y, por ende, menos posibilidades se presentarán 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 están íntimamente relacionadas bien con fenómenos delictivos, bien con propuestas interestatales conflictivas, que encierran ambos la presencia de grupos de personas con intenciones hostiles, contornos grupales cerrados y excluyentes y búsquedas 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, serían subsidiarios a ese 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, por mejor decir, por una seguridad emanada de la inteligencia. El primer ministro británico Tony Blair simbolizó acertadamente este planteamiento al afirmar que “si alguna lección puede extraerse del 11-S es la importancia de no esperar a que se materialice la amenaza”. La clave está, pues, en la prevención basada en la inteligencia, esto es, en la comprensión adecuada de las dinámicas del fenómeno terrorista con el propósito de anticiparse proactivamente a ellas.

Inteligencia prospectiva para la seguridad y la defensa

En un intento de articular un marco conceptual, Bas[4] apunta que "el objeto de la prospectiva es anticipar futuribles (futuros posibles), asignándoles una probabilidad de ocurrencia estimada (subjetiva u objetivamente) y un grado de deseabilidad (acorde con los objetivos de partida). La Prospectiva trata, pues, de –a partir de información pasada y presente, así como de especulaciones acerca del futuro– 'dibujar' un mapa cognitivo que permita determinar distintas opciones y reducir el nivel de incertidumbre que acompaña a toda decisión".

La inteligencia prospectiva de seguridad es la utilización del conocimiento para la acción sobre futuros de riesgo, sobre la trayectoria o trayectorias presentes que conformarán esos futuros de riesgo. Por tanto, en seguridad y defensa no existe prospectiva sin conocimiento (inteligencia) y no existe valor si nuestra interpretación anticipada de los fenómenos no está ligada a la acción, a una acción preventiva. Esta acción prospectiva puede ser estratégica, como conciben la mayoría de los autores,[5] pero también táctica, es decir, también es útil avanzar en una prospectiva aplicada a las operaciones. Es comprometido, en este punto, mencionar las acciones preventivas, sobre todo en el ámbito de la defensa, cuando tras el 11-M una de las incorporaciones estratégicas más relevantes y polémicas a la doctrina de seguridad de algunos países ha sido la de los "ataques preventivos".[6] Sin embargo, la proactividad preventiva en seguridad no ha de ser estirada conceptualmente hasta tal punto que se actúe contra ciudadanos antes de que vulneren la ley, sino que se trata de accionar los recursos de seguridad para reducir las oportunidades –y esta reducción es la clave preventiva– de que la delincuencia pueda ejecutar sus propósitos de transgresión en contextos sociales concretos. De ese modo se conjugarán en una respuesta integrada a la amenaza global de la delincuencia organizada todas las potencialidades y recursos de los servicios de seguridad y policía.

El desarrollo de capacidades de inteligencia prospectiva es un territorio con amplio potencial en las fuerzas de seguridad y un interesante campo de investigación y perfeccionamiento para sus analistas. Bien es cierto que el análisis de riesgos que, por ejemplo, se está aplicando en control de personas y mercancías en recintos aeroportuarios, o la introducción de componentes de perfilado en el análisis de información financiera relacionada con el blanqueo, son prometedores comienzos en esta línea de trabajo. Sin embargo, la prospectiva estaría muy lejos y sería muy ineficiente si no se trabajara continuamente en la calidad del proceso de análisis de información, sobre todo en lo que se refiere al desarrollo de sistemas de tratamiento de información rigurosos y homogéneos en las fuerzas de seguridad del Estado y, muy particularmente, a la arquitectura de una metodología específica para el análisis estratégico de información y la producción de inteligencia para las decisiones estratégicas en seguridad pública.

Detección y medición descriptivas: primer axioma de la prospectiva
Con respecto a lo que podríamos definir como primer axioma de una prospectiva eficiente, el tratamiento de la información, en los estudios de futuro es imprescindible tomar conciencia de que el cimiento ineludible de una predicción es una descripción exhaustiva del fenómeno, del espacio de conocimiento, desde el cual se pretende construir trayectorias de futuro. Cuando nos adentramos en la prospectiva de seguridad,

[4] Enric Bas, "Prospectiva y prevención de la delincuencia organizada", Conferencia Prospint para Directivos de Seguridad Pública, 4/V/2005, Ministerio del Interior, Madrid. Véase también Enric Bas, *Prospectiva*, Ariel, Barcelona, 1999.
[5] Como referente principal, véase M. Godet, "Prospective et stratégie: approche intégrée", *Futuribles*, nº 137, noviembre de 1989.
[6] F. Arteaga, "La Estrategia de Seguridad Nacional de Estados Unidos de 2006", ARI nº 71/2006, Real Instituto Elcano.

nos percatamos de que el conocimiento más difícil de aprehender no tiene que ver con el futuro, sino con el presente. Hasta tal punto es así que si fuéramos capaces de disponer de una descripción precisa de las variables, factores o componentes de un fenómeno de seguridad concretizado (que puede ser estratégico como la evolución del yihadismo en España o más operacional como las actividades de un grupo criminal estable de tráfico de seres humanos), de las relaciones de influencia entre esos elementos y de la dinámica de comportamiento de cada elemento individualmente y en relación con otros; y si además ese esquema de conocimiento incluyera todas y cada uno de los componentes suficientes y necesarios para materializar el comportamiento del fenómeno, sin que faltara o sobrara ninguno, entonces la previsión sería automática, sería una predicción, un futuro predecible. El inconveniente con la prospectiva de seguridad, con cualquier otra prospectiva sectorial o general, es que nada sucede de esta manera tan determinista.

Las herramientas de pronóstico que operan sobre datos cuantitativos funcionan bien, lo que ocurre es que no somos capaces de operacionalizar adecuadamente la mayoría de las variables y, cuando logramos una aproximación satisfactoria, con toda probabilidad nos hemos dejado fuera de la ecuación prospectiva un factor de influencia causal que ni siquiera hemos detectado. Lo más importante, y lo más complejo, de proyectar futuros es detectar y medir variables en el presente: por ese orden, detectar primero y medir después. En seguridad, buena parte de los componentes de determinación del comportamiento de un fenómeno son de naturaleza social y, más claramente, humanos. La metodología de las ciencias sociales o de las psicológicas ha avanzado considerablemente en las últimas décadas hasta incorporar diseños multivariantes que aprehenden toda una serie de factores, los categorizan y jerarquizan, para ofrecernos un perfil cuantitativo de un objeto de estudio. Sin embargo, como bien conocen los especialistas en ciencias del comportamiento, aún a pesar de los intentos de operacionalización y cuantificación de la personalidad humana, todavía somos incapaces de describir con precisión, empleando nada más instrumental psicométrico, la conducta de un individuo. La opción del análisis eficaz es integrar ese resultado cuantitativo en un método cualitativo de interpretación. Sin embargo, incluso cuando hubiéramos desarrollado sistemas cualitativos fidedignos –que no los tenemos–, la detección exhaustiva y la medición precisa de factores continúa siendo ineluctable.

De este modo, las condiciones de partida en una inteligencia prospectiva de seguridad que pretenda trascender las especulaciones más o menos literarias es que el foco de atención del análisis sea inclusivo de variables sociales, por contraposición a exclusivo de factores tradicionales de seguridad dura (incautaciones, atentados, cuántas armas, cuántos delitos), por un lado, y que el prospectivista de seguridad tenga acceso a la información sobre las variables, factores y elementos de una estructura, situación o grupo que pretende estudiar. Es decir, adoptar aproximaciones macro, meso y micro y disponer de elementos de observación y detección lo suficientemente afinados.

Este planteamiento se traduce en que cuando intentemos abordar análisis prospectivos sobre la delincuencia organizada o el terrorismo tendremos que pensar más allá del fenómeno criminal concreto, todavía más si el objeto de nuestro análisis es estratégico. La prospectiva de seguridad puede aplicarse a la evolución de un grupo terrorista, a anticipar su comportamiento. Los investigadores de las unidades contraterroristas conocen bien lo difícil que es, teniendo presentes además las constricciones de tiempo y seguridad que rigen la labor de desarticulación de grupos terroristas. Sin embargo, si alguien con acceso a toda la información de campo durante los dos años previos al 11-S o al 11-M (y acceso a toda la información operativa quiere decir sin compartimentación por agencias, que fragmenta y sesga la interpretación que pudiera hacer un analista) hubiera sido capaz de asociar piezas de información y además las hubiera contextualizado en función de elementos de naturaleza social, las instituciones públicas de seguridad quizá hubieran tenido una oportunidad predictiva. Con todo, es dudoso que,

aún cuando el acceso a la información hubiera sido total, la detección y observación de las variables apropiadas para un pronóstico hubiera sido la mejor. El prospectivista de seguridad siempre debería preguntarse si tiene encima de su mesa todas las variables, si ha hecho un buen ejercicio de catalogación y repertorio, o si tiene que continuar indagando antes de proyectar futuros. Y aquí llegamos al segundo axioma de la inteligencia prospectiva de seguridad: el método.

Arquitectura metodológica específica para el análisis estratégico en seguridad
La piedra que cimienta la prospectiva es la observación. Observamos, detectamos, medimos y catalogamos. Luego, otorgamos pesos de influencia, asociamos y proyectamos. La garantía inaugural de cualquier unidad de inteligencia prospectiva en seguridad es disponer de órganos de obtención de información que aporten líneas de conocimiento directo del fenómeno objeto de estudio. Estos canales de información viva, que en la gran mayoría de supuestos tienen clasificación de seguridad (son confidenciales, reservados o secretos), en el análisis prospectivo se contextualizan con el aporte de fuentes abiertas de información. No es sensato pensar en crear unidades de prospección en inteligencia sin disponer de, aunque sea, un microdepartamento destinado a tratar y procesar información de fuentes abiertas, que en el caso del análisis estratégico debería de ser una observación guiada, pautada, aunque sin renunciar a la flexibilidad.

Pues bien, situándonos en el ideal de departamentos prospectivos con acceso a información tanto clasificada como abierta, el siguiente escalón metodológico radica en garantizar que nuestros focos de observación estén sintonizados sobre un repertorio lo suficientemente nutrido de variables detectadas, esto es, que nos planteemos las preguntas adecuadas y que nos concentremos sobre las variables clave. Desde una óptica instrumental, para conseguir estos repertorios de variables, la prospectiva suele recurrir al análisis estructural.

Por describirlo sin demasiadas complicaciones, el análisis estructural consiste en comenzar catalogando la columna vertebral de un fenómeno, y los factores y elementos que lo componen, sin adentrarse de momento en sus interrelaciones causales o correlacionales, aunque sí estableciendo interconexiones entre componentes del sistema (de momento nos basta con saber que un elemento está ligado a otro, y dejaremos para posteriores averiguaciones cuál es su relación de influencia). Al respecto de las interconexiones, que después condicionarán nuestro “mapeado” de las relaciones de influencia entre variables, algo que suele obviarse cuando arranca un análisis estructural es que el prospectivista debería tener una teoría sobre cómo funciona el fenómeno. Es exactamente lo mismo que ocurre en la investigación científica: es la teoría la que guía la recogida de los datos. No es necesario subrayar, por tanto, la relevancia de que los equipos de futuristas no sean nada más que metodológicos, sin contacto alguno con el área disciplinar de conocimiento aplicado (imposible hacer proyecciones sobre yihadismo internacional sin recurrir a un especialista en la materia o sin que el equipo prospectivo sea un binomio especialista conceptual-especialista metodológico).

El suelo sobre el que crece el análisis estructural es el ejercicio de afloramiento de variables, a lo que un equipo de futuros debería dedicar el tiempo y los ejercicios (*brain storming*, etc) necesarios. Después vendrá si esas variables identificadas sobre las que se centrará la proyección de futuros están o no, o son o no, cuantificadas o cuantificables y si disponemos de adecuadas descripciones de cada una de ellas (estadística descriptiva, en supuestos cuantitativos). Así pues, el afloramiento de variables es el nudo gordiano de esta etapa de elaboración de una matriz del espacio de análisis, tan relevante que condicionará inexorablemente los futuros a construir.

Algunos prospectivistas realizan análisis estructurales a través de procedimientos exclusivamente cuantitativos. Lo más habitual es realizar algún tipo de análisis factorial exploratorio. Es un error. El reduccionismo en estudios de futuro es el camino más seguro para equivocarse en una proyección. En ciencias de seguridad, como un espacio disciplinar de las ciencias sociales, los fenómenos son multivariantes y gran parte de sus elementos constituyentes son cualitativos o, al menos por el momento, son factores de difícil operacionalización. Los análisis factoriales exploratorios representan una base excelente sobre la que comenzar a construir un análisis estructural, pero un campo abonado al sesgo interpretativo si pretenden ser el único canal de desarrollo de una proyección de futuros.

Contrariando al paradigma positivista que predomina en nuestra ciencia, la cuantificación de variables es, tras la detección de esas mismas variables, el talón de Aquiles de la prospectiva. Tanto lo será que, con la potente evolución que han registrado las ciencias matemáticas y estadísticas en convergencia con la informática en las últimas décadas, todavía los económetras son incapaces de hacer predicciones con mínima incertidumbre sobre la evolución de los valores en bolsa. Sí, en efecto disponemos de innumerables previsiones sobre el comportamiento de valores económicos y bursátiles pero ¿a que no existe ninguna consultora que nos asegure la inversión en un paquete de valores compuesto por todos los cotizantes en bolsa que vayan a ganar siempre?; no existe porque, incluso siendo valores cuantificados, existen terceras variables de índole social (no cuantificadas y, lo que es peor, ni siquiera detectadas y contempladas por los modelos econométricos) que explican porqué, en un momento determinado, se produce una oscilación repentina de algunos valores.

El análisis estructural antecede al –y se complementa con el– análisis morfológico. En realidad, muy bien podríamos acordar que se trata de dos fases dentro del mismo tipo de análisis, aquél dedicado a establecer primero la configuración molar de un espacio problema para después descomponerla en sus componentes moleculares (en su morfología). La construcción de un espacio morfológico consiste en la esquematización de las combinaciones posibles de los elementos que forman parte de cada factor identificado en el análisis estructural. Es un ejercicio de detalle, en donde se derivan esos constituyentes de los factores estructurales, combinándolos en varias posibilidades con sentido para cada factor. Si hiciéramos un símil con un intento de hacer prospectiva sobre el comportamiento de un individuo, el análisis estructural consistiría en elaborar el repertorio de los factores que determinan ese comportamiento (desde los sociales, personales, laborales, familiares, hasta la personalidad y, dentro de ella, el carácter, su constitución, su inteligencia), mientras que el análisis morfológico sería el intento de descomposición de esos factores estructurales (por ejemplo, los factores laborales se descompondrían en el puesto que ocupa, sus funciones, la historia laboral y las diversas posibilidades e influencias de cada uno de ellos; la personalidad se descompondría en sus rasgos, el carácter en las actitudes o la inteligencia en estilos cognitivos de respuesta), buscando las distintas combinaciones probables para cada uno de esos elementos resultado de la descomposición. Cuanto más exhaustivo sea el análisis morfológico, menos incertidumbre en el momento de proyectar los futuros. De nuevo, si trabajamos con variables operacionalizadas y cuantificadas, un análisis factorial exploratorio nos producirá una reducción de componentes principales de cada factor. Sin embargo, en fenómenos de seguridad este supuesto es anecdótico si pretendemos abarcar para todo el espacio estructural, aunque sí es factible utilizar este procedimiento estadístico para alguna de las variables del problema sometido a estudio que tengamos apropiadamente medidas y convertidas en números. El análisis morfológico aporta soluciones teóricas que después pueden depurarse por una combinación de instrumental cuantitativo (análisis factorial confirmatorio, redes neurales) y cualitativo para encarrilar los escenarios de futuro.

En combinación con el análisis morfológico, y ya encaminándonos a la modelización de escenarios o futuribles, los prospectivistas están recurriendo cada vez más a tres tipos de minerías: la de datos, la de textos y la minería *web*. Las minerías buscan asociaciones latentes entre piezas de información. Es preciso no confundir la minería con la recuperación de información. Recurriendo al significado que pretende evocar el nombre de "minería", aplicado al procesamiento de información, entenderemos que el propósito de estas técnicas es encontrar "mineral" útil entre las "rocas". Cuando nos referimos a información, la minería asiste en la tarea de hallar, precisamente, esa información que, aún estando presente en el volumen de datos, no es directamente visible al analista. Estos "minerales" de información, cuando estamos tratando números, textos o *webs*, están casi siempre referidos a piezas informativas que emergen durante el trabajo de minería al establecer, a través de ese procesado, asociaciones entre elementos informativos que sí son visibles al analista *a priori* (las "rocas"). Evidentemente, las minerías son útiles en cualquier segmento del proceso de información, ya operativo o estratégico. Puede ser aplicado, incluso, en los compases previos a la construcción de una teoría o modelo de la realidad por parte del analista (es decir, antes o durante el análisis estructural) a fin de encontrar indicadores sustantivos que iluminen la senda interpretativa.

Tras estas fases de análisis, el interpretador de información dedicado a elaborar prospectiva de seguridad estará en condiciones de modelizar escenarios, de construir modelos de realidad. A los escenarios se puede llegar a partir de un estudio Delphi o combinándolo con los análisis que ya hemos descrito. Lo que es inexorable en la edificación de futuribles es considerar las variables centrales, proximales y distales influyentes en el comportamiento de un problema y encontrar el modo en que se relacionan entre ellas para determinar ese comportamiento tal como se manifiesta. Son las distintas evoluciones previsibles de esas variables y de sus relaciones las que compondrán las posibilidades, esto es, el abanico de escenarios que el analista propondrá al decisor como rutas eventuales de desarrollo del futuro.

En un informe prospectivo que guarde consistencia metodológica deberían exponerse varios futuribles para trazar la evolución de un objeto de estudio. Habitualmente suelen plantearse un mínimo de tres escenarios:

(1) El tendencial, que recoge la hipótesis más plausible sobre la conducta de las variables y que coincide, básicamente, con la teoría que ya hemos mencionado el prospectivista elabora como modelo de la realidad que está estudiando.
(2) El escenario de contraste, que es una variación probabilística del escenario tendencial, y que dibujaría la posibilidad de comportamiento que resultaría caso de que las variables centrales del fenómeno se vieran sometidas a distinto tipo de influencias. El contraste es un ejercicio de pensamiento alternativo, en donde el analista debería considerar el rango de "holgura" de algunas de las variables involucradas para trazar lo que ocurriría si (el *what if* típico de la prospectiva) ciertos ingredientes del fenómeno trazaran otro curso de comportamiento. Ciertos autores consideran que el escenario de contraste sería aquel futurible que nos mostraría lo que ocurriría al suceder justo lo contrario de lo que se ha propuesto en el escenario tendencial, de manera que el contraste serviría como una especie de "seguro" en el proceso de toma de decisiones (similar a "voy a considerar que ocurre lo contrario por si acaso).
(3) El escenario prescriptivo, que equivaldría a situar, dentro del espacio problema que hemos definido, el foco del análisis en las variables ligadas a la institución de seguridad que lleva a cabo el estudio o a los organismos de seguridad de un país o al gobierno o, por resumir, a los actores que emprenderían la acción ligada al estudio prospectivo que se está elaborando (si se trata de un estudio prospectivo sobre política exterior española en Marruecos que está elaborando el RIE, el escenario

prescriptivo exploraría como una determinada acción de instituciones y empresas españolas podría modelar un futuro concreto y, por tanto, cómo sería ese futuro). A la inteligencia prospectiva de seguridad es el escenario que más interesa y sobre el que las instituciones públicas deberían comenzar a trabajar. A este futurible concierne aquello que, como sociedad y a través de nuestras instituciones especializadas, podemos hacer para evitar que un determinado escenario de riesgo se desarrolle o materialice. Es, por ende, el escenario que evita llegar hasta el punto de tener que tomar medidas drásticas, como ataques preventivos o acciones por el estilo, puesto que compone el futuro desde el presente a partir de nuestro diagnóstico y de nuestra intervención sobre lo diagnosticado. Por supuesto, el escenario prescriptivo es tan difícil o más (puesto que implica conocer muy bien nuestras organizaciones e incluirlas en el análisis evitando prejuicios y señalando cada uno de nuestros defectos y limitaciones) de modelizar que los anteriores.

A partir de ese mínimo, pueden construirse tantos escenarios como la elasticidad y rigor del análisis permitan. Incluso, los escenarios suelen ser bautizados nominalmente para etiquetar en cierto modo el futurible al que se refieren (por ejemplo, "escenario negro"[7]). Como quiera que sea, debiera de ser preceptivo en prospectiva considerar alternativas y, de manera sistemática, varios futuribles. Las predicciones absolutamente deterministas, por el momento, no existen. Esto es cierto, sobre todo, en prospectiva de seguridad, tan dependiente de variables sociales, por un lado, y tan constreñida a procesos de toma de decisiones que no permiten demasiada especulación por su impacto en las vidas de los ciudadanos, por otra. Los informes de inteligencia prospectiva de seguridad, además de la clara visibilización del abanico de posibilidades, deberían tener gradación de incertidumbre, ser escalables en su tratamiento del conocimiento.

La gradación de incertidumbre es introducir una secuencia en la redacción y exposición del informe prospectivo que debería dejar muy claro, ante el consumidor del producto, qué información conoce el analista como cierta; qué porción de su producto corresponde a una descripción del fenómeno; qué otra se adentra en explicarlo; cuál supone la proposición de una hipótesis; y dónde comienza el trazado de los futuribles, en donde sea posible de los cuales deberían plantearse las probabilidades asociadas. Esto permitirá a las personas dedicadas a decidir saber que grado de certidumbre asumen al adoptar una posibilidad decisoria y sobre qué elementos del análisis, desde los más seguros a los más eventuales, toman una resolución de acción.

La construcción de escenarios tiene, desde luego, el objetivo de proponer futuribles para la toma de decisiones, pero no sólo. La realización de análisis prospectivos sustanciará gran parte de la actividad de un departamento de futuros, pero será una actividad sin futuro, si se permite el juego de palabras, si no está acompañada de otro propósito que habrá de convertirse en la tarea de mantenimiento de un *staff* prospectivo: la construcción de perfiles con indicadores de alerta temprana. La elaboración de indicadores de alerta temprana es una actividad destinada directamente a la prevención accionable. Consiste en encontrar marcadores que anticipan la presencia de un fenómeno, factores que, no constituyendo una amenaza en sí mismos, nos dicen que su manifestación habitualmente antecede a una amenaza o elementos que, una vez han emergido, nos conducirán eventualmente a un riesgo.

[7] Puede encontrarse un ejercicio de este tipo, aunque sin pretensiones probabilísticas, en C. Alonso Zaldívar, *Invasión de Irak: escenarios negros*, Documento de Trabajo, 14/I/2003, Real Instituto Elcano.

Unidades de futuros en instituciones de seguridad

Del informe de la comisión de investigación establecida en los EEUU para aclarar, hasta donde fuera posible, la naturaleza de la respuesta de los poderes públicos ante los atentados terroristas del 11 de septiembre de 2001,[8] pueden extraerse muchas conclusiones. Dos son, en lo que respecta a nuestras reflexiones en este ARI, especialmente salientes: (1) la necesidad de encontrar vértices instituciones de convergencia en el tratamiento de la información, de manera que exista al menos un grupo de interpretación que pueda estar en condiciones de valorar amenazas con información útil y accionable, procedente de una coordinación adecuada entre agencias de seguridad; y (2) la conveniencia de mejorar nuestra interpretación de la amenaza a partir del análisis de esa información.

Respecto de la primera conclusión que destacamos, la creación del Homeland Security Department y el nombramiento de un director nacional de Inteligencia en EEUU, o la institución del Centro Nacional de Coordinación Antiterrorista en España, son pasos que se han dado, aunque lentos y tímidos, hacia la congruencia. Respecto de la segunda, la preparación de profesionales de la seguridad pública para interpretar de manera más eficaz y preventiva las amenazas complejas a la ciudadanía, quedan en los EEUU la creación del Centro Sherman Kent para el Análisis de Inteligencia y, en España, la creación del programa Prospint de Inteligencia, Estrategia y Prospectiva en Seguridad Pública.[9] Ambas iniciativas buscan desarrollar doctrina y capacitar analistas de seguridad pública en metodologías de interpretación de realidades complejas que trasciendan esquemas rígidos y autocomplacientes de aproximación a las amenazas de seguridad. Es decir, y en suma, aprender a manejar la incertidumbre.

El programa Prospint, además, está planificado para el desarrollo de metodologías de análisis y de interpretación que doten a una eventual comunidad española de analistas de inteligencia de las herramientas para abordar diagnósticos estratégicos con vocación prospectivista. Al final se persigue combinar las capacidades públicas de obtención de información con la mejor interpretación para construir modelos que permitan decidir sobre realidades criminales cuando comiencen a causar mínimos perjuicios. En este intento, obtener información es tan importante como acceder a ella e interpretarla. De nada sirven sofisticados sistemas de obtención de información por satélite si nuestros analistas interpretan los datos presa de miedos institucionales, sesgos de procesamiento de información o deficiencia en habilidades metodológicas y de razonamiento.

De momento, en España, la inteligencia prospectiva de seguridad es, en sí misma, un futurible. Hay contados profesionales en instituciones, como la Secretaría de Estado de Seguridad, el CNI o el MADOC del Ejército, que o bien llevan tiempo trabajando irregularmente en este campo sin demasiada repercusión orgánica o funcional en sus corporaciones, o bien están comenzando un camino en paralelo a la emergencia de una cierta curiosidad facilitadora por parte de sus directivos. Lo cierto es que el planteamiento de “unidades de futuros” –que sería la denominación más apropiada– o de servicios de prospectiva con mandato a tiempo completo para desarrollar líneas de análisis anticipatorio o preventivo es mucho más sencillo de lo que parece. Ocurre que hay que dejar de pensar en términos burocráticos y hacerlo con enfoque funcional y flexible. De entrada y tiempo completo, no son necesarios más que dos profesionales por institución, con capacidad para constituir equipos temporales de trabajo *ad hoc*.

[8] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States,* W.W. Norton, Nueva York, 2004.

[9] Prospint es un programa de la Secretaría de Estado de Seguridad del Ministerio del Interior español dirigido por el responsable de su Gabinete de Análisis y Prospectiva, Modesto García García.

Tanto el análisis estructural como el morfológico, y posteriormente el trazado de escenarios, deberían planearse y desarrollarse en equipo. Es muy dudosa la viabilidad de conducir estas etapas prospectivas en la soledad de un analista. Al tratarse de fases cuyo propósito es describir la naturaleza y composición detallada de un problema complejo, es poco probable encontrar un analista individual que, una vez determinado el problema, sea capaz de producir un repertorio amplio de variables evitando sus propios sesgos teóricos y errores de procesamiento; que tenga un volumen tal de conocimiento del problema que sea capaz de construir, sin aportaciones ajenas, una teoría sobre su funcionamiento que guíe el análisis; y que, además, sea un excelente metodólogo conocedor del instrumental necesario. Además de ser poco probable el caso, es ineficiente.

Las unidades de futuros, o prospectivas, tienen vocación horizontal, es decir, deberían poder aplicarse al estudio de cualquier problema de seguridad. Para ello, deberían constituirse en equipos con un núcleo estable pero con periferias flexibles. La combinación de unidades tipo *staff* y tipo *task force* es la ideal para ello. Como hemos mencionado, una unidad adscrita a las direcciones de inteligencia o de operaciones con una plantilla de dos profesionales, uno de los cuales debe ser un director de equipos con conocimiento avanzado de análisis e iniciado en la prospectiva, que ejercerá de director de orquesta en cada estudio que se ponga en marcha; y el otro un metodólogo, quien aportará el rigor científico e instrumental al análisis. Estas dos figuras pueden estructurar perfectamente el *staff* de una unidad de futuros para comenzar a producir inteligencia prospectiva de seguridad. Sin embargo, con necesarios, no son suficientes para emprender un análisis prospectivo. En cada encargo, debería constituirse un equipo de tarea con los siguientes componentes: uno o dos especialistas en el tema objeto de estudio (por ejemplo, terrorismo yihadista o trata de seres humanos); un especialista en tratamiento y análisis de información. Para cada estudio, la dirección de inteligencia o de operaciones debería otorgar las habilitaciones de seguridad necesarias, práctica que en España está fuera de costumbre pero en la que ya avanzaremos cuando no quede más remedio.

Conclusiones

Las sociedades democráticas ya no demandan que los poderes públicos arresten e impongan una pena a un terrorista que ha cometido un atentado: exigen, además, que las instituciones de seguridad sufragadas con impuestos estén en condiciones de conocer las amenazas y, a partir de ese conocimiento, prevenir su comportamiento para evitar que un atentado terrorista, aunque se planifique, jamás llegue a ejecutarse. No sólo esto, sino que, si es posible, la libertad democrática demanda que la delincuencia organizada no llegue a implantarse en un determinado territorio de manera que reduzca el bienestar de los ciudadanos. Hacia esta orientación preventiva, las policías y agencias de seguridad sólo pueden desarrollar órganos de inteligencia que construyan conocimiento y anticipen el comportamiento de las amenazas. No basta con obtener información del interior y alrededores de cada amenaza, sino que es necesario procesar la información para interpretarla, para descifrar la amenaza, para elaborar modelos de realidad que permitan la acción preventiva. Después de avanzar durante años en el análisis de información, las agencias de seguridad deben prepararse para el análisis anticipado de la realidad, para adentrarse en el territorio de las conjeturas científicas, de la construcción de futuribles. Este camino, que requiere un cambio importante en la cultura reactiva de las organizaciones de seguridad, aún está comenzando.