Real Instituto Elcano
documento de trabajo

Tecnologías para la Seguridad Interior: una industria en busca de identidad

Andrés Montero Gómez

Área: Seguridad y Defensa
Documento de Trabajo 48/2009
25/09/2009

Real Instituto Elcano
Madrid – España
www.realinstitutoelcano.org

Real Instituto Elcano
documento de trabajo

Tecnologías para la Seguridad Interior: una industria en busca de identidad

Andrés Montero Gómez [*]

Índice

(1) Introducción

El proceso de globalización es contingente respecto a la revolución tecnológica y no puede entenderse la primera sin la segunda. Al mismo tiempo, conceptos como sociedad de la información y sociedad del conocimiento emergen en el proceso de globalización sustanciado a su vez por los desarrollos en tecnologías de la información y de la comunicación, tanto que de nuevo no pueden entenderse los unos sin los otros. Algún autor asegura, incluso, que la anticipación sobre el futuro y los ejercicios de previsión sólo pueden elaborarse tomando a la tecnología como *driver* central de razonamiento.[1]

Ya es un hecho aceptado que la seguridad global del siglo XXI es una seguridad distinta a la definida por el siglo XX. La despolarización de bloques, la caída del Muro de Berlín, la transnacionalización de la seguridad y la proliferación de grandes atentados terroristas, entre otros, han introducido nuevos conceptos y categorías en la seguridad internacional. La conocida "revolución en los asuntos militares" (RAM) fue el principio de una reasignación de significados a la realidad de las amenazas, de manera que lo que venía siendo un enfoque más o menos unidimensional fundado en la reacción ante una agresión interestatal de naturaleza militar dio paso a una seguridad internacional basada en la prevención y en la reacción ante riesgos multidimensionales, interestatales o no. El

[*] *Director de Thint Intelligence*

[1] N.N. Taleb, *The Black Swan: The Impact of the Highly Improbable*, Random House, Nueva York, 2007.

enemigo comunista manifestado a través de vectores de influencia geopolítica, de modelo socioeconómico y de carrera armamentística, pasó a ser un riesgo difuso, multipolar, menos apoyado en las armas que en la capacidad de hacer daño y, sobre todo, no necesariamente estatal. Sin embargo, mientras la revolución en los asuntos militares ha constituido y viene constituyendo un proceso para repensar la defensa en términos de las nuevas realidades, el ámbito de la seguridad interior todavía no ha tenido su propia "revolución de los asuntos de seguridad" (RAS).

Si el desmantelamiento de la Unión Soviética como concepto de la bipolaridad es el primer paso para la reconfiguración de la seguridad, los atentados terroristas del 11 de septiembre de 2001 en EEUU son el segundo hito hacia la composición del concepto de seguridad global. Hay una fase en la seguridad internacional de Posguerra Fría en la que se van desmilitarizando los conflictos y la fuerza se emplea para mantener la paz en beneficio del orden y la seguridad internacionales. Posteriormente, con la paulatina desaparición de las fronteras en Europa y con el incremento exponencial de los intercambios, se estructura la cooperación policial internacional como condición necesaria para la gestión compartida de amenazas transnacionales. El 11-S introduce (o subraya lo que hasta entonces demandaba menos nuestra atención) nuevos contornos semánticos para la seguridad. La seguridad exterior se impregna de elementos antes considerados de seguridad interior, como el terrorismo, el crimen organizado o la inmigración; la seguridad interior se internacionaliza a través de la cooperación policial internacional; los servicios de inteligencia se involucran de lleno en la prevención de amenazas antes consideradas criminales y por tanto policiales, mientras los servicios de policía consolidan la adopción de métodos de inteligencia. De este modo, las fuerzas armadas se embarcan en la concepción doctrinal, y en su traducción táctica y estratégica, de modelos militares de enfrentamiento (guerras asimétricas, *netwar*, *war by other means, military operations other than war, swarming*) que en su mayoría ya existían en teoría pero que ganan en aplicabilidad en la medida que las acciones de combate convencionales la pierden.

Por su parte, las fuerzas de policía y seguridad, en la misma línea, se encaminan hacia modelos de aproximación a la criminalidad impregnados de una concepción preventiva y proactiva (*intelligence-led policing*). El vuelco conceptual más importante de la seguridad global es su direccionamiento hacia una prevención no basada en la disuasión sino en la anticipación, en la capacidad de interrumpir determinadas evoluciones de la realidad que suponen un riesgo. Todas estas transformaciones apuntan a nuevos paradigmas estratégicos que, apoyándose en las nuevas estrategias de seguridad de EEUU y de la UE, a las que luego siguieron las del Reino Unido, Alemania y Francia, abundan en un dimensionamiento integrado de la seguridad, con intentos más o menos afortunados de comprender la defensa como una expresión concreta y contextual de la seguridad nacional pero revelando, como es propio de procesos de adaptación, que todavía no existe

claridad en el posicionamiento de las diversas piezas del *puzzle* sobre el tablero de la globalización.[2]

Continuando esta reflexión introductoria sobre la seguridad global, podríamos considerar que tras una primera fase en la que se deroga la seguridad de bloques, y después de una segunda en la que se acaba con la diferenciación entre las dimensiones exterior e interior, la evolución conduce a una nueva fase caracterizada por la convergencia de la seguridades física y lógica en torno a la ciberseguridad, de un lado, y por la inteligencia económica, de otro.

Las ciberamenazas ya se consideran –en cualquiera de sus manifestaciones: *cyberwar*, cibercriminalidad, ciberterrorismo…– como las fuentes con mayor potencial de riesgo para la seguridad de las sociedades del futuro. Hasta tal punto, que la Agencia Federal de Investigaciones (*Federal Bureau of Investigation*, FBI) de EEUU las considera el riesgo de seguridad más elevado, tras los escenarios de destrucción masiva por medios nucleares, biológicos, químicos o radiológicos.[3] Lo que ya comienza a ser denominado como *cybergeddon*, es decir, un ataque combinado que afecte a infraestructuras críticas y a procesos civiles, militares y económicos, viene determinado por la mayor interdependencia entre las tecnologías de la información y comunicación (TIC) y la economía. Por otro lado, la economía financiera es muy vulnerable respecto a una disrupción significativa en las arquitecturas de información y comunicación que sostienen los intercambios en la actividad bancaria. La convergencia e interacción de las fuentes de riesgo obliga a afrontar las ciberamenazas a través de enfoques de seguridad convergentes hacia modelos integrales,[4] aquellos en donde se integran de manera sinérgica la tradicional seguridad dedicada a la protección de personas y bienes (seguridad física) con la seguridad de la información (seguridad lógica) destinada a proteger los sistemas de conocimiento de las empresas, que hoy día incluyen no sólo la información sino otros activos intangibles como la imagen, la reputación o el talento.

Numerosas amenazas en el futuro procederán del ámbito de las ciberacciones ofensivas, que se concentrarán en el tejido económico y del conocimiento en sectores estratégicos para los países. Paulatinamente van siendo más numerosas las advertencias de organismos de seguridad pública que llaman la atención sobre redes criminales, de las que se sospecha esponsorización incluso de algún Estado, que fijan su blanco en las arquitecturas de información y comunicación de empresas estratégicas (que, por tanto, aportan bienestar y seguridad al ciudadano) o incluso en aparatos de defensa o de

[2] Félix Arteaga ha analizado las estrategias en varios documentos para el Real Instituto Elcano: "Roadmap for a Spanish National Security Strategy", ARI, nº 112/2008; "El concepto de seguridad nacional en el Libro Blanco de la Defensa y la Seguridad Nacional de Francia", ARI, nº 133/2008; "La Estrategia Europea de Seguridad, cinco años después", ARI, nº 15/2009.

[3] En palabras de Shawn Henry, director adjunto de la Ciberdivisión del FBI, en la *International Conference on Cybersecurity*, Fordham University, Nueva York, 6-8/I/2009.

[4] Véase Carlos Blanco Pasamontes, "La convergencia de la seguridad: la seguridad integral", ponencia en el X Congreso Internacional de Profesionales IT, Madrid, 26-27/XI/2008.

seguridad públicas[5] con fines de sustracción de información, de sabotaje o de infiltración residente. Las evoluciones de este tipo de ecuaciones de riesgo en el futuro son tan variables que es difícil trazar líneas o compartimentos estancos *a priori*, siendo esta borrosidad la que defina probablemente una de las características centrales de la seguridad "glocal".

La conexión entre economía y tecnología no es la única que involucra a la economía en la nueva seguridad global. En la medida que el bienestar y la seguridad de los ciudadanos dependen con claridad del sistema económico, éste se convierte en un objetivo de agresiones potenciales más rentable que la vida de las personas porque sus efectos alcanzan a millones de ciudadanos. La protección de la economía como parte de la seguridad ocupará nuevas funciones en el futuro. Algunas de ellas se afrontan ya desde la inteligencia económica, entendida como la manera de gestionar inteligentemente la ventaja competitiva de las empresas en un escenario global[6] y otras comienzan a afrontarse desde la protección pasiva a las infraestructuras críticas, la protección activa de las líneas de comunicación marítimas (las acciones de seguridad marítima en torno a los Estrechos de Malaca, el Golfo de Adén o el Canal de Suez donde participan buques de guerras de países regionales y extrarregionales). También se afrontan desde la óptica de la supervisión de los flujos y transacciones financieras, que se han visto potenciados por la crisis financiera de 2008 y que ha llevado a la constitución por el G-20 del Consejo de Estabilidad Financiera o del previo Consejo Europeo de Riesgo Sistémico, decidido por los ministros de Economía de la UE tomando como base el *Informe Larosière*.[7] Todo ello, la protección de procedimientos y flujos económicos, formará parte de una nueva seguridad global gestionada a través de procesos complejos sobre arquitecturas de tecnologías de información y comunicación.

Este Documento de Trabajo, que está dedicado a analizar el sector de las tecnologías para la seguridad, comenzará por explorar el espacio de transición conceptual y doctrinal (por tanto, práctico y efectivo) en que se encuentra la seguridad interior. En ese sentido, el índice del documento está destinado a desentrañar las disfunciones de una seguridad interior que intenta operar con códigos de siglo XX (territorialidad, reactividad, compartimentación) sobre un espacio de amenazas que funcionan con código de siglo XXI (globalización, transfronterizo, anticipación). Nuestra hipótesis es que los problemas que detallaremos en el sector de las tecnologías para la seguridad y en la creación de una industria de la seguridad son deudores de la débil identidad de la seguridad interior como área concreta de la seguridad pública. Nuestra propuesta es que únicamente recurriendo a nuevas doctrinas de seguridad interior –basadas en la triple integración

[5] S. Price, "Phising Warfare Against Armed Forces", *IAnewsletter*, vol, 11, nº 4, 2008.
[6] A. Montero y J. Ramírez, *Inteligencia Económica como Vector Internacional de Seguridad*, Documento de Trabajo nº 18/2008, Real Instituto Elcano. También, ligando la inteligencia económica al concepto *homeland security*, véase G. Murat, "Implications de la construction d'une 'Homeland Defense' en Europe, en matière d'intelligence économique", *Sécurité Globale*, nº 4/2008.
[7] J. de Larosière, *The High-Level Group on Financial Supervision in the European Union Report*, 2009, *http://ec.europa.eu/internal_market/finances/docs/de_larosiere_report_en.pdf.*

convergente entre (1) la seguridad física y la lógica, (2) lo local y lo global y (3) la integración de la seguridad interior con la defensa en una gran estrategia de seguridad nacional– estaremos en condiciones de construir una cultura tecnológica de la seguridad que nos permita aproximarnos a un futuro deseado de eficiencia.

(2) Buscando una nueva identidad de seguridad ¿"glocal"?

Aunque, como hemos mencionado, la prevención y control del terrorismo yihadista a partir de los atentados del 11-S supuso una cierta integración entre las seguridades exterior e interior tal como venían siendo entendidas, lo cierto es que ése que hemos denominado "segundo período de evolución de la seguridad global" dista de estar cerrado y concluido y todavía lo encontramos en plena transición. La reestructuración de los aparatos de seguridad para enfocarse eficientemente sobre el terrorismo yihadista internacional ha supuesto la emergencia del concepto *homeland security*, un espacio pensado para incorporar la protección de infraestructuras críticas como elemento estratégico, situar el peso del sistema en la prevención a través de la inteligencia y trascender los límites de la investigación criminal jurisdiccional ligada al territorio del Estado para combinar la cooperación policial internacional, la cooperación internacional entre servicios de inteligencia y, sobre todo, la integración en *task forces* o equipos conjuntos de medios de policía e inteligencia. Todo alrededor de la seguridad del Estado, con el acento puesto en la prevención de ataques, y enfocando doblemente *hacia el interior de las fronteras* pero incorporando el *ingrediente de visión internacional y análisis global* indispensable para evaluar el riesgo de amenazas con naturaleza transnacional. De este modo, y contra lo que venía siendo norma en el pensamiento de seguridad de toda la segunda mitad del siglo XX, la seguridad interior ya no sólo tendría que ver con el interior del territorio, con las fuerzas de policía y con la investigación de delitos. Junto a lo anterior, ahora la seguridad interior interconectaría al territorio del Estado a la red transnacional de las amenazas, integraría o interactuaría (dependiendo de los casos y países) con las agencias de inteligencia e incluso tendría en cuenta la acción de fuerzas militares en el exterior en las estrategias de seguridad interior (las acciones estadounidenses o británicas en Iraq y Afganistán no son ajenas a la seguridad interior frente al yihadismo). Además, la expansión afectaría también a la prevención de los delitos y riesgos, complementando la investigación del delito con la inteligencia preventiva, adelantando incluso sobre etapas preparatorias de la conducta criminal la acción represiva del derecho penal. De alguna manera, como señalamos, se ha querido ver la idea de *homeland security* como espacio de convergencia de todos esos "alineamientos evolutivos", pero esta pretensión o esperanza, hay que expresarlo con toda rotundidad, no se ha materializado todavía. Lo que parece estarse articulando es una *homeland security* centrada en la prevención y recuperación ante ataques a infraestructuras críticas y una seguridad interior concentrada en la investigación policial criminal y antiterrorista. El problema con este planteamiento es que, mientras las amenazas demandan más integración en seguridad pública, la concepción de una *homeland security* concentrada en la protección (preparación y recuperación) contra ataques a las

infraestructuras críticas, pero desligada de los servicios y agencias de investigación/inteligencia en seguridad interior, puede traducirse en algunos países en *otra* agencia que contribuya a mayor desorientación, mayor dificultad de coordinación y, en definitiva, a una respuesta más embarullada ante las amenazas.

La seguridad interior y la *homeland security* no han convergido todavía hacia un todo conceptual que integre ambas ideas, y puede que no lo hagan. De hecho, en este camino de transición y de búsqueda de una identidad de seguridad "glocal" (doméstica o local en cuanto se entiende para el interior de los Estados pero global en cuanto es necesariamente interconectada e interdependiente),[8] lo que se ha producido es la emergencia de la protección de infraestructuras críticas como núcleo alrededor del cual constituir departamentos de seguridad más o menos coordinados con las estructuras policiales y/o de inteligencia tradicionales. En esta línea se encuentra también la doctrina defendida por la RAND Corporation de EEUU, según la cual la *homeland security* tendría cinco misiones específicas:[9] (1) el apoyo a la preparación del sistema de defensa civil ante ataques terroristas de envergadura; (2) asegurar la continuidad del gobierno; (3) asegurar la continuidad de las operaciones militares; (4) la defensa de las fronteras; y (5) el sistema nacional de misiles, entendido como infraestructura crítica. El resultado orgánico de esta conceptualización funcional es el *Department of Homeland Security* de EEUU, que aglutina capacidades en esas líneas pero no integra a agencias de la investigación o inteligencia con competencias en amenazas de seguridad interior como el terrorismo o el crimen organizado, ya sean el FBI, la ATF (*Alcohol, Tobacco, Firearms and Explosives*) o la DEA (*Drug Enforcement Administration*), que permanecen en el Departamento de Justicia.

En Europa la idea del *homeland security* no ha fructificado institucionalmente, creando una nueva organización, sino que se ha enfocado hacia la constitución de centros de coordinación para la protección de infraestructuras críticas en sintonía con el Plan Europeo de Protección de Infraestructuras Críticas (*European Programme for Critical Infrastructure Protection*, PEPIC) y la propuesta de la Comisión Europea sobre la *Critical Infrastructure Warning Information Network* (CIWIN). Estos centros, como el británico *Centre for the Protection of National Infrastructure* (CPNI), el español Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) o el *Kritis* del Ministerio Federal del Interior en Alemania, incrustados en los Ministerios de Interior de los países. En el Reino Unido, por ejemplo, el CPNI reporta directamente al director del Servicio de Seguridad (MI5), al igual que lo hace el director del departamento de análisis de la amenaza terrorista, el *Joint Terrorism Analysis Centre* (JTAC). El modelo estadounidense de *homeland security* ha tenido pues su paralelo europeo en organismos de coordinación pero enfocados en exclusiva hacia la protección de infraestructuras críticas.

[8] "Glocal" como referido a "glocalización", un término que quiere significar "piensa globalmente y actúa localmente" y cuyo uso se remonta a principios de los 90 del siglo pasado por los sociólogos Roland Robertson y Keith Hampton. En español y para la seguridad, ha sido introducido por Jaume Curbet en *La glocalización de la (in)seguridad*, Instituto Nacional de la Administración Pública, Madrid 2006.
[9] E. Larson y J.E. Peters, *Preparing the US Army for Homeland Security: Concepts, Issues and Options*, RAND, Santa Monica, 2001.

Aunque no hayan contribuido a definir mejor los límites de una identidad de seguridad interior en transición, los organismos de protección de infraestructuras críticas sí han aportado al menos un par de líneas sustanciales de apuntalamiento a la seguridad del Estado. La primera de ellas tiene que ver con la asunción de la cultura de la gestión del riesgo como vía de afrontamiento de las amenazas. Los centros de protección de infraestructuras críticas forman un tándem preventivo con los centros de análisis de la amenaza, de momento fundamentalmente de índole terrorista, de manera que unos se dedican a intentar detectar señales para la prevención de atentados (centros de análisis como el CNCA en España y el JTAC británico) y otros, los centros de infraestructuras, a prepararse para un atentado terrorista de gran envergadura, simulando sus consecuencias y manteniendo engrasados los dispositivos de respuesta.[10] La combinación en la gestión del riesgo es prevención, preparación, respuesta y recuperación.

La segunda de las líneas que han introducido los centros de protección de infraestructuras críticas en el redimensionamiento de la seguridad del Estado es no ya la cooperación, sino la integración en el esquema de la seguridad pública del componente empresarial e industrial ligado a las infraestructuras. De los catálogos nacionales de infraestructuras consideradas críticas para la seguridad del ciudadano (porque sostienen la normalidad de las dinámicas sociales y cuya disrupción por atentados supondría un impacto grave al mantenimiento de esa normalidad), la inmensa mayoría están gestionadas y son propiedad de empresas privadas que ofrecen un servicio de interés público. Sin ser exhaustivos, pensemos en el suministro y conducción de agua y electricidad, en líneas de telecomunicaciones, en infraestructuras de transporte y en sistemas informáticos, por ejemplo, del sector bancario. La protección eficaz de estas infraestructuras es inviable sin la integración de las empresas propietarias y de los operadores en la porción correspondiente del esquema nacional (y europeo en el caso del catálogo de infraestructuras críticas en el espacio común) de seguridad pública. La integración de este componente empresarial, por lo que supone de elaboración de plantes propios, de coordinación, de participación activa y, sobre todo, de conciencia de pertenecer y contribuir decisivamente a una dimensión de la seguridad pública desde la sociedad civil representa uno de los hitos conceptuales más importantes para la seguridad interior en su reorientación desde el 11-S de 2001.

Por tanto, aunque el concepto *homeland security* ha sido beneficioso para robustecer la seguridad del Estado introduciendo toda una filosofía de gestión del riesgo ante una amenaza compleja y transnacional como el terrorismo, desde luego no ha servido para construir una identidad de seguridad doctrinalmente sólida que incorpore e integre las reorientaciones de la nueva seguridad global (o, si se quiere, "glocal"). En la actualidad, la impresión general es que la seguridad interior es una cuestión policial, que está internacionalizada a través igualmente de la cooperación policial internacional y que tiene

[10] A. Montero y J. Zurita, "Gestió de la Seguretat en Atemptats Terroristes de Gran Envergadura", *Revista Catalana de Seguretat Pública*, nº 19, 2008.

que ver con la comisión de delitos. No obstante, esta percepción es bastante continuista y no resiste el mínimo contraste con la realidad. Es cierto, sin embargo, que la introducción de departamentos de coordinación para la protección de infraestructuras críticas que hemos señalado ha discurrido en paralelo al desarrollo de centros de fusión, de coordinación y análisis dedicados a desarrollar inteligencia criminal integrada frente a las distintas tipologías de amenazas complejas. Por ejemplo, en España se han situado en la Secretaría de Estado de Seguridad un Centro de Inteligencia contra el Crimen Organizado (CICO), un Centro Nacional de Coordinación Antiterrorista (CNCA) y un Gabinete de Estudios de Seguridad Interior. Sin embargo, mientras en el CNCA existe una presencia integrada del Centro Nacional de Inteligencia para coordinar la acción antiterrorista, en el CICO no ocurre lo mismo, lo que lleva a suponer que el crimen organizado no es una amenaza transnacional, que el CNI no interviene con inteligencia preventiva en ella o que la red de cooperación policial internacional es suficiente para conocer, comprender y cambiar el fenómeno. Cualquiera de estas últimas suposiciones, de nuevo, no resiste un contraste riguroso con la realidad de las amenazas. ¿Tiene algo que decir el CNI en seguridad interior en España, o la CIA en EEUU?

Un país que desde hace tiempo ha resuelto esta disyuntiva con mayor coherencia que el resto ha sido el Reino Unido, que cuenta con un servicio de inteligencia de seguridad interior, el *Security Service* (MI5), que integra sus poderes de inteligencia con las capacidades de investigación de los servicios especiales de las policías (*Special Branches*) y con el *homeland security* del aparato de seguridad pública. No obstante, en el Reino Unido queda pendiente la coordinación entre el MI5 y la SOCA (*Serious Organized Crime Agency*), una institución integradora e híbrida, que combina competencias en inteligencia y policía y que está enfocada con especificidad hacia el crimen organizado. Esta demanda de coordinación está siendo especialmente subrayada en la gestión de las ciberamenazas, donde las competencias están repartidas entre agencias. Lo beneficioso del modelo británico es que con la puesta en marcha del SOCA, el MI5 deja de ser competente en la prevención del crimen organizado (desde su nuevo territorio competencial, el MI5 lo considera una *former threat*, una antigua amenaza de la que ya no se ocupa porque lo hace otra agencia), estableciéndose un claro reparto de funciones en un modelo nacional de seguridad *intelligence-led*. En la mayoría de los países de nuestro entorno la integración del *puzzle* de la seguridad pública no está tan trabajada.

(3) La Inteligencia de Seguridad como vía de convergencia

Así pues, la inteligencia es precisamente el territorio donde se están manifestando la mayor parte de las tensiones derivadas de la evolución de la seguridad tradicional hacia una seguridad global. Por su propia naturaleza de instrumento y de proceso dedicado a conocer, comprender y cambiar la realidad, la inteligencia de seguridad, en sus distintas expresiones, recoge por un lado la necesidad de desarrollar una nueva visión ante las amenazas globales y, por otro, las resistencias organizacionales y culturales al cambio. Este tipo de resistencias quedan patentes en los pocos ejercicios de evaluación que se han

hecho sobre la reorganización de los servicios públicos de inteligencia y seguridad tras el 11-S en EEUU. En noviembre de 2008 la Oficina del Director Nacional de Inteligencia (*Office of the Director of National Intelligence*, ODNI), cuyo inspector general es el responsable de integrar a la comunidad de inteligencia para hacerla más eficiente ante el riesgo, publicó un informe desclasificado en donde concluía, entre otras cuestiones, que la mayoría de los funcionarios de las 15 agencias de inteligencia del país desconocían la labor de la ODNI, sentían su labor esencialmente como perjudicial y, en consecuencia, continuaban desarrollando la tendencia a "ir por libre" respecto del resto de las agencias.[11]

De manera que la seguridad interior actual progresa en medio de tensiones entre lo policial y la inteligencia, entre prevención y respuesta represiva reactiva, entre delito y riesgo. En seguridad pública, principalmente en lo que a las denominadas amenazas a la seguridad nacional se refiere, la doctrina más o menos escrita ha venido marcando que los servicios de inteligencia de corte civil o militar se venían ocupando de adoptar un enfoque preventivo respecto a los riesgos, mientras que los servicios de información de las fuerzas de seguridad incorporaban la vertiente represiva e investigativa propia de la protección de la ciudadanía ante el delito.[12]

El planteamiento doctrinal argumentaba que los servicios policiales recogen *evidencias* sobre la comisión de un hecho (delictivo), es decir sobre el pasado, mientras que los servicios de inteligencia recogen *indicios* sobre el futuro, sobre la paulatina conformación de un riesgo. Esta segmentación funcional, con las lógicas diferencias entre países según sus diversas traducciones jurídicas y composiciones institucionales pero casi siempre ajustándose a esa perspectiva bidimensional de prevención-represión, ha sido especialmente visible en la forma de afrontar el terrorismo hasta la última década del siglo pasado. En efecto, todavía hoy subsisten las nociones de antiterrorismo y contraterrorismo, la primera para denotar los esfuerzos destinados a desactivar las distintas esferas del terrorismo desde cualquiera de sus planos (social, político, financiero, ideológico), principalmente implementando medidas preventivas, y la segunda enfocada esencialmente al plano penal y dirigida a desarticular la amenaza criminal a través de la acción policial y judicial (y militar, si contamos las operaciones contraterroristas en Afganistán o Iraq).

Con todo, al igual que ha venido ocurriendo con los conceptos de seguridad interior y seguridad exterior,[13] progresivamente difusos tras el 11-S, la división entre antiterrorismo

[11] Office of the Director of National Intelligence (2008), *Critical Intelligence Community Management Challenges*, *http://graphics8.nytimes.com/images/2009/04/02/us/02intel-report.pdf*.

[12] Carlos Ruiz Miguel considera que la distinción entre servicios de inteligencia y servicios de información "no tiene fundamentación científica" alguna y que más bien responde a la parcelación de intereses corporativos. Véase C. Ruiz, "Problemas actuales del derecho de los servicios de inteligencia", *Inteligencia y Seguridad: Revista de Análisis y Prospectiva*, 2, 13, p. 46, 2007.

[13] J. Avilés, "Por un concepto amplio de seguridad", *Monografías del CESEDEN*, nº 55, CESEDEN, Madrid, 2002.

y contraterrorismo está siendo revisada. Todas estas líneas de reconceptualización de la seguridad –la exterior y la interior, la preventiva y la represiva, anti y contraterrorismo– coinciden con la aproximación (y en algunos casos solapamiento) de funciones e intereses entre los servicios de inteligencia de los Estados y los servicios de información de las policías. Esta aproximación ha sido potenciada por dos vectores: (1) la progresiva implicación de los servicios de inteligencia en la lucha contra las amenazas de naturaleza criminal; y (2) la paulatina incorporación de métodos y técnicas de inteligencia criminal en la acción policial unido a su progresiva internacionalización mediante la cooperación policial.

Con la convulsión en las políticas de seguridad que ocasionó la irrupción del terrorismo yihadista en la agenda internacional, este proceso de convergencia entre mecanismos (policiales y de inteligencia) de la seguridad pública está buscando soluciones de integración que están encontrando su máxima resistencia, precisamente, en el terreno de la inteligencia aplicada a la seguridad. Es en este terreno donde se están produciendo las principales fricciones entre los servicios de inteligencia del Estado y los servicios de información policiales, especialmente en esas líneas fronterizas que mencionábamos pero principalmente en la incorporación de un enfoque preventivo en la actividad contraterrorista de las fuerzas de seguridad, entrando al menos teóricamente en un espacio que se entendía ocupado más o menos en exclusiva por la acción (internacionalizada, además) de los servicios de inteligencia involucrados en la aplicación de las estrategias antiterroristas.

De esta manera, los servicios de información contraterroristas de las fuerzas de seguridad operan con doctrinas y metodologías importadas de los servicios de inteligencia y con un enfoque operacional que, sin dejar de tener como objetivo final la desarticulación de bandas terroristas y la recopilación de pruebas para un proceso judicial, entronca cada vez más con la idea de prevenir la comisión de un delito. Este despliegue –hacia atrás, preventivo– de las fuerzas de seguridad hasta situarse en las actividades preparatorias del continuo que representa la conducta criminal introduce condicionantes incluso en la técnica legislativa antiterrorista, pues podría apuntarse que la previsión policial no debería ir más acá de lo que abarque la conducta delictiva en su recorrido (¿debería la policía llegar en su labor preventiva hasta antes de que se inicie una conducta que pudiera considerarse legalmente como delictiva?).

Sin embargo, la evolución de la técnica jurídica antiterrorista, por ejemplo con la introducción de figuras conceptuales como la conspiración para delinquir o la pertenencia a banda armada, están haciendo rentable y –legitimo– adentrar la acción policial en el terreno de la prevención en una secuencia temporal cada vez más amplia de conducta criminal, desde la ideación hasta la comisión de un atentado. En esas primeras etapas del riesgo, en donde una serie de individuos comienzan a pensar en conspirar para realizar actividades criminales, es donde los servicios de información policiales están solapándose con los servicios de inteligencia y no sólo porque las fuerzas de seguridad se hayan

movido hacia la prevención, sino que también lo han hecho los servicios de inteligencia hacia el terreno de la investigación judicial de lo criminal.[14]

Del mismo modo que está sucediendo con la acción anti/contraterrorista está ocurriendo, con distintos matices, con la prevención e investigación de la delincuencia organizada global. Desde hace casi ya dos décadas en España, con un ritmo similar al de otros países, está siendo desarrollada la inteligencia criminal por los órganos de policía judicial de las fuerzas de seguridad como una disciplina específica, de forma que puedan ser más eficientes anticipándose al comportamiento de las redes criminales organizadas. De esta forma, la inteligencia criminal toma prestados, de nuevo, doctrina y métodos de los servicios "tradicionales" de inteligencia, tanto para el tratamiento y análisis de la información necesaria para comprender el fenómeno criminal como en el empleo de procedimientos y técnicas operativas como la infiltración.

A escala internacional, esta revolución conceptual y metodológica en la investigación policial de la delincuencia organizada se ha plasmado en desarrollos que van desde doctrinas y esquemas operativos con identidad de inteligencia como los que aplican desde su constitución el *Federal Bureau of Investigation* (FBI) estadounidense y la *Bundeskriminalamt* (BKA) alemana, al diseño y adopción de modelos de inteligencia criminal como el *Criminal Intelligence-led Model* británico,[15] o en la propia creación de agencias supranacionales de policía como Europol (cuyo modelo de inteligencia criminal es de inspiración británica).[16]

Pues bien, a pesar de todas las capacidades de inteligencia que despliegan los Estados, la primacía de la prevención y de la orientación hacia los riesgos no se ha materializado hasta la llegada del Siglo XXI y en respuesta al terrorismo yihadista. Incluso se ha venido cuestionando que los servicios de inteligencia estuvieran (estén) del todo preparados para afrontar un tipo de amenazas de fisonomía tan cambiante y que requiere el desarrollo de capacidades flexibles, en el marco de las cuales la eventual rigidez, la aversión al riesgo y las patologías en el procesamiento de la información de los servicios de inteligencia tendrían poca conciliación.[17]

La cuestión última es si es posible desarrollar seguridad preventiva sobre amenazas complejas y si nuestros servicios de inteligencia (policiales o no) están en sintonía

[14] Por ejemplo, algunas de las actividades de investigación del CNI español se han judicializado con el nombramiento de un juez especial del Tribunal Supremo para autorizar y fiscalizar técnicas como la intervención telefónica o el registro domiciliario sobre sospechosos, todo en virtud de la Ley Orgánica 2/2002 reguladora del control judicial del CNI.

[15] *The National Intelligence Model*, National Crime Intelligence Service (NCIS), Londres, 2000.

[16] H. Brady, "Europol and the European Criminal Intelligence Model: A Non-state Response to Organised Crime", ARI, nº 126/2007, Real Instituto Elcano.

[17] B. Jenkins, "Redefining the Enemy", *Rand Review*, vol. 28, nº 1, 2004, pp.16-23; R. Johnston, *Analytic Culture in US Intelligence Community*, Center for the Study of Intelligence, Washington DC, 2005; y A. Montero, "Psicología del terrorismo e inteligencia contraterrorista", *Papeles del Psicólogo*, nº 88, 2004.

metodológica, institucional y, en definitiva, cultural hacia ese horizonte. Lo que puede estar ocurriendo es que nos encontramos en un momento de transición, en donde el logro de una acción preventiva de seguridad a través de la inteligencia y por medio de la implantación de una identidad prospectiva en las instituciones públicas especializadas tenga que superar constricciones corporativas y culturales que retrasan la adopción de nuevas visiones y metodologías de trabajo.

(4) La revolución tecnológica de los asuntos de seguridad

En medio de todo este desafío conceptual alrededor de la seguridad en general y de la seguridad interior en particular, aparecen la ciencia y la tecnología como ingredientes sin los cuales ningún planteamiento de seguridad global tiene sentido. Y aparecen sin que, en muchos países, exista una cultura y mucho menos una industria de seguridad interior organizadas para dar respuesta a una demanda que ni siquiera estaba conformada. En este ámbito, en el de la integración de la tecnología en la cultura de seguridad, también nos encontramos en período de transición.

No obstante, es patente que la conformación del concepto de *homeland security* como integración de la seguridad exterior e interior para constituir un espacio de *seguridad de la nación o de la patria*, aunque todavía no definida del todo doctrinalmente, ha tenido su inmediato reflejo en los departamentos de desarrollo de negocio de las empresas dedicadas a la provisión de tecnología para la defensa y la seguridad. La mayoría de estas empresas han constituido la *homeland security* como una línea de negocio y han creado direcciones departamentales con esa misma denominación. Sin embargo, todo esto es muy reciente y nos encontramos, precisamente, en el momento de su definición y constitución.

En España se ha tenido que esperar hasta 2004 para constituir una Dirección General de Infraestructuras y Material de Seguridad en el Ministerio del Interior, que incorpora una subdirección para las tecnologías de información y comunicación en seguridad. Con anterioridad no existía un plan integrado de tecnologías de seguridad y cada necesidad se iba sustanciando por los actores institucionales de la seguridad pública en función de sus propios programas. En esto vamos más o menos en línea con otros países, aunque con nuestras propias peculiaridades y, desde luego, con mayor retraso como veremos en I+D+i de seguridad.

Cuando se desarrollaron los trabajos para la elaboración del Plan Nacional de I+D+i 2008-2011 durante 2007, se establecieron varios paneles temáticos de expertos para elaborar las líneas subvencionables en el marco del plan. En realidad, la elaboración de un plan a futuro es un ejercicio de prospectiva y los paneles de expertos trabajan con esa metodología. En el panel de expertos en seguridad y defensa –una línea temática y, por tanto, combinada–, la representación de la seguridad interior estaba en una proporción desfavorable de 1 a 10 con respecto a la de defensa. Ese escenario no hacía más que

reflejar la tradicional dedicación de la defensa al I+D+i, la existencia de una industria ya estructurada y con programas de certificación de empresas trabajando para defensa y de sus tecnologías, mientras que los asuntos de seguridad interior comenzaban a incorporarse a tal ecosistema.

La situación del escenario emergente tiene, evidentemente, su lógica. Mientras en el ámbito de defensa la ciencia y la tecnología y, por tanto, una cultura institucional y empresarial, surgieron alrededor de la progresiva tecnificación de la guerra, del armamento y de su precisión, la modernización tecnológica de la seguridad interior ha venido determinada por la tecnificación de la criminalidad. Por supuesto que la tecnología ya estaba presente en el trabajo de las fuerzas policiales antes de constituirse en el Ministerio del Interior español un órgano especializado en tecnologías de seguridad. Basta mencionar, entre otros, avances tan sustanciosos como el Sistema Integral de Vigilancia Exterior (SIVE) para la monitorización inteligente de la frontera sur de la UE a punto de cumplir una década de implantación y desarrollo, la utilización de bases de datos relacionales en la lucha contra el terrorismo, con más de 15 años de progresivas evoluciones,; los sistemas de huellas dactilares y la arquitectura de bases de datos de inteligencia criminal en el Cuerpo Nacional de Policía, que comenzó a operar en 1994. Incluso, a principios de la década del 2000, ya se estaba conceptualizando el diseño del observatorio de seguimiento de nuevas tecnologías utilizadas por las organizaciones criminales (OSUNT), un proyecto alojado en la Secretaría de Estado de Seguridad.

Todos ellos son desarrollos tecnológicos ya incorporados a las misiones de la seguridad pública en función de las necesidades. Sin embargo, la conciencia de revolución tecnológica llegó a partir de 2001 con la reorientación antiterrorista de la seguridad global, de tal modo que podemos considerarlos procesos o revoluciones sinérgicas. Y lo consideramos un proceso revolucionario en los asuntos de seguridad porque a partir de entonces se produce un cambio incremental dinámico y geométrico, por contraposición a la evolución lineal y más o menos aritmética que se registraba hasta la década del 2000. También lo es porque una revolución requiere un nuevo modelo de interiorización cultural de esos cambios en las corporaciones de seguridad, hacia una suerte de cultura tecnológica de la seguridad que, en definitiva, hace que hoy sea impensable afrontar la criminalidad sin tecnología, especialmente si se pretende afrontar de forma preventiva.

Podemos resumir en tres los ingredientes tractores que impulsan la revolución tecnológica para los asuntos de la seguridad, apellidada ésta de Interior o del Estado:

(1) La necesidad de anticipación de las amenazas y la consiguiente gestión del riesgo para evitar ataques terroristas de gran envergadura, que obliga a realizar esfuerzos en la detección de señales, simulación, análisis y modelización de patrones, visualización y, sobre todo, en la gestión de estructuras multifactoriales de datos que den cuenta de la presencia y evolución de fenómenos sociales complejos.

(2) La progresión geométrica de la difusión de información y de las comunicaciones ligada al fenómeno Internet, que no sólo multiplica los intercambios y abre múltiples vías para las organizaciones criminales, incluso para la aparición de nuevos tipos delictivos (*phising, pharming*, ciberacoso) y la potenciación de otros (pornografía infantil), sino que complica el tratamiento y análisis de información, necesarios para realizar interpretaciones afinadas de la realidad criminal, introduciendo lo que se ha venido en llamar intoxicación por información (*infoxication*).
(3) La tecnificación de la criminalidad, indisolublemente ligada en sus instrumentos y procesos a la evolución de la sociedad industrial hacia la sociedad de la información y de ésta a la sociedad del conocimiento.

Esta conciencia de encontrarnos en una fase de transición *kuhniana* hacia otro paradigma de la seguridad tecnificada requiere tres ingredientes constituyentes para su traducción efectiva: (a) una cultura tecnológica de la seguridad, principalmente en el sector de la seguridad del Estado; (b) una I+D+i para tejer una ciencia de la seguridad; y (c) una industria de la seguridad con identidad gremial, que participe del esfuerzo de investigación, desarrollo e innovación y que sea la proveedora de soluciones tecnológicas para la seguridad pública. Cada uno de estos ingredientes constituyentes se encuentra en un grado de desarrollo diferente, pero puede afirmarse que en realidad ninguno de ellos llega a pasar de una etapa incipiente de germinación.

Respecto a la necesidad de una cultura tecnológica de la seguridad, resulta indispensable para que los individuos y organismos de seguridad tomen conciencia de esos tres ingredientes tractores que reseñábamos más arriba e interiorice nuevos procesos de trabajo derivados de nuevos modos de pensar.[18]

En cuanto a la investigación, desarrollo e innovación en tecnologías para la seguridad, es decir, el pilar científico del esfuerzo tecnológico, es necesario disponer de planes estratégicos de capacidades y necesidades, de un lado, y de programas de financiación, de otro, además de una serie de centros de investigación orientados y con vocación de

[18] Tal como ha subrayado Alicia Álvarez, la subdirectora a cargo de tecnologías de información y comunicación para la seguridad del Ministerio del Interior español, "la cultura tecnológica de seguridad la componen dos vectores interrelacionados. El primero de ellos tiene que ver con la interiorización que cada una de las personas de las organizaciones e instituciones de seguridad, y cada organización e institución con sus directivos al frente, hacen de los medios y recursos tecnológicos como instrumentos auxiliares de su propia capacidad de crear e interpretar realidades. El segundo vector está enfocado en los proveedores, en las empresas, en la industria tecnológica y en su capacidad de entender las necesidades de los usuarios y de diseñar y componer soluciones ergonómicas, es decir, que sean sinérgicas y convergentes con las habilidades que debe poner en práctica el usuario para desplegar su potencial de actuación sobre el entorno de seguridad. Es decir, la cultura a la que me estoy refiriendo parte de un mayor y más eficiente diálogo entre proveedores industriales y usuarios, convirtiendo a estos últimos en tecnólogos de sus propias necesidades y a aquellos primeros en diseñadores de usabilidad" (ponencia sobre "La Convergencia de la Seguridad: perspectivas desde las administraciones públicas", presentada en la III Jornada de Empresa y Seguridad de la Fundación ESYS sobre Convergencia de Seguridad Física y de Seguridad Lógica, Madrid, 4/III/2009).

seguridad nacional. En España, el desarrollo de la estructura orgánica dedicada a tecnologías en el Ministerio del Interior en 2004 iba acompañado, precisamente, de esos dos componentes de financiación y tejido investigador. Tal como ha anunciado el propio ministro del Interior, Alfredo Pérez Rubalcaba, y tal y como recoge el programa electoral del partido político que sostiene al gobierno en la IX Legislatura, el gobierno instituirá un Instituto de Investigación e Innovación Tecnológica en Seguridad (tejido investigador, ciencia) y comprometerá un Plan Cuatrienal de Inversiones (financiación) para la dotación tecnológica de la seguridad del Estado. Aunque ambos instrumentos quedan por desarrollar, probablemente retrasados por la coyuntura económica, su incorporación a los planes políticos de la seguridad pública ya pone a España en línea con la corriente dominante en nuestros socios europeos y transatlánticos.

Esta corriente internacional puede ligarse a la participación de la sociedad civil en la seguridad pública, a través de la implicación de empresas que gestionan infraestructuras críticas para la seguridad. La habilitación del concepto *homeland security* ha derivado en un considerable impulso a la investigación en nuevos métodos y tecnologías para la seguridad del Estado, sobre todo en EEUU y, con mucho menos éxito, en los programas de financiación de I+D+i en la UE. Aunque detallaremos más adelante los parámetros de los programas europeos, baste ahora señalar que el *Department of Homeland Security* (DHS) de EEUU ha creado un programa plurianual de inversión en investigación, desarrollo e innovación que no sólo se materializa en una cuantiosa financiación sino en la constitución de los denominados centros de excelencia en investigación. Este esfuerzo está incluso legislado a través de uno de los instrumentos de acompañamiento de la Ley Patriótica de 2002 bajo el acrónimo de *SAFETY ACT* (*Support Anti-Terrorism by Fostering Effective Technologies Act*). La ley *SAFETY* es tan relevante porque introduce en la conciencia y en las operaciones de *homeland security* la idea de que un ingrediente imprescindible para la eficiencia de la prevención y gestión del riesgo es la disposición y aplicación de tecnología. En función de la ley *SAFETY* se designan de interés para la seguridad de los ciudadanos de EEUU toda una serie de desarrollos tecnológicos y sus procesos de diseño e implementación financiados consiguientemente. De manera que el DHS estadounidense no sólo promociona e invierte en investigación científica básica o adquiere tecnologías en desarrollo o ya desarrolladas, sino que lo hace todo al mismo tiempo en un verdadero esfuerzo político e institucional de I+D+i para una seguridad del Estado, esfuerzo distinto y adicional al ya conocido, multimillonario e instalado desde hace décadas programa que EEUU tiene en Defensa. En lo que ha investigación científica-tecnológica se refiere, los mencionados centros de excelencia se localizan en universidades que conducen investigaciones multidisciplinares sobre soluciones de seguridad y que son elegidos por el DHS a través de un proceso competitivo que culminará en una designación por el Congreso de EEUU.[19]

[19] Aunque sea extensa, merece la pena dedicar una nota a reseñar estos centros, para dejar patente lo ambicioso y comprehensivo de la iniciativa. Actualmente los centros de excelencia en I+D+i son: el Centro para la Seguridad de Fronteras e Inmigración, con la Universidad de Arizona y la Universidad de Texas; el Centro para la Detección, Mitigación y Respuesta ante Explosivos, con las Universidades de Boston y de

Por lo que se refiere al desarrollo de una industria tecnológica de la seguridad en los contextos europeo y español y de la toma de conciencia de una identidad gremial como tercer ingrediente del cambio de paradigma que proponíamos, las empresas del sector están dando pasos en su construcción pero todavía con tímidos resultados. La mayoría de las empresas que avanzan en esa dirección lo están haciendo por tres caminos, a veces interrelacionados: (1) unas provienen del ámbito de defensa y han abierto líneas de trabajo en seguridad e Interior, sumándose al mercado emergente; (2) otras son empresas que estaban trabajando ya en desarrollos para necesidades tecnológicas *ad hoc* de las fuerzas de seguridad y aprovechan esa experiencia para consolidar e impulsar una línea de negocio en seguridad; y (3) otras son nuevas empresas que comienzan ya directamente ofertando soluciones tecnológicas para *homeland security*, en la mayoría de los casos relacionadas con el ámbito de las TIC. Cualquiera de estas aproximaciones entendemos que es legítima y beneficiosa para comenzar a conformar un espacio de trabajo fructífero en colaboración con las administraciones públicas. Sin embargo, queda un importante camino por recorrer.

El primero de los pasos que la industria debe potenciar es la toma de conciencia de su existencia como tal. Aunque pudiera vincularse esa toma de conciencia a la existencia de parámetros más instrumentales, como por ejemplo vías y líneas de financiación, lo cierto es lo primordial para construir esa conciencia es la existencia de un mercado. Y ese mercado existe desde el momento en que se exponen unas necesidades por parte de un cliente, sobre todo cuando esas necesidades, como veremos en ejemplos de España y EEUU, se difunden y comunican al tejido empresarial estructuradas y sistematizadas. Sin embargo, como aludíamos cuando reseñábamos la descompensación de presencia entre seguridad y defensa en la elaboración del Plan español de I+D+i, seguridad e Interior todavía no comprenden una industria con identidad propia. Es cierto que pueden tomarse, incluso extrapolarse directamente, avances ya consolidados en la industria de defensa, como el proceso de certificación de empresas y tecnologías, pero otros tendrán que observarse para después desarrollarse con peculiaridades propias para el espacio de negocio, como por ejemplo el asociacionismo gremial.

El asociacionismo gremial es clave para entender el grado de conciencia de un sector y sus líneas estratégicas de avance. En España, mientras son clásicas las asociaciones de

Rhode Island; el Centro para la Seguridad Marítima, Portuaria e Insular, con la Universidad de Hawaii y el Instituto Stevens de Tecnología; el Centro sobre Desastres Naturales, Infraestructura Costera y Gestión de Emergencias con las Universidades del Norte de Carolina y la Estatal de Jackson; el Centro Nacional de Seguridad en el Transporte, con sede en Connecticut y siete sedes universitarias comprometidas; el Centro sobre el Riesgo y el Análisis Económicos de Acciones Terroristas con la Universidad del Sur de California; el Centro para la Protección y Defensa Alimentaria, con la Universidad de Minnesota; el Centro para la Defensa contra Amenazas Zoonóticas y Animales, con la Universidad de Texas; el Consorcio Nacional para el Estudio del Terrorismo y la Respuesta ante el Terrorismo, con la Universidad de Maryland; el Centro para el Estudio de la Preparación y la Respuesta ante Catástrofes, con la Universidad John Hopkins; Centro para la Evaluación Avanzada de Riesgos Microbiológicos, con la Universidad de Michigan; los cinco Centros Afiliados al Instituto de Ciencias Discretas; y los seis Centros Regionales para Visualización y Análisis.

empresas colaboradoras y proveedoras de tecnologías para la Defensa, como la clásica AFARMADE (Asociación Española de Fabricantes de Armamento y Material de Defensa y Seguridad) o la recién creada AETEDAE (Asociación de Empresas Tecnológicas Españolas de Defensa, Aeronáuticas y Espacio), no puede decirse lo mismo de la industria de la seguridad aunque, como esperemos haya quedado claro con el estado de evolución de la propia identidad de seguridad interior en el ámbito público, es perfectamente normal que así sea y vamos al ritmo de lo que está marcando la tendencia global liderada –hay que reconocerlo– por EEUU. En esta línea, algunos foros facilitadores que ya venían trabajando en Defensa (como el Círculo de Tecnologías para la Defensa y la Seguridad), en las administraciones públicas (la Fundación Dintel) u otros que llevan años aplicándose en el sector de las TIC (Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España con su Plataforma Tecnológica Española de Tecnologías para la Seguridad y Confianza) han asumido la seguridad como uno de sus espacios de trabajo y están promoviendo acciones de definición y promoción de la industria. Esto demuestra que la industria se está moviendo en una fase de transición hacia el encuentro de un espacio propio y, desde las administraciones públicas, a la espera de las anunciadas medidas de potenciación de las tecnologías para la seguridad interior (el instituto, el plan cuatrienal), también se están constituyendo nodos tractores para la seguridad desde el Instituto Nacional de Tecnologías de la Comunicación (INTECO).

Otro de los vectores sinérgicos importantes que impulsarán la identidad de seguridad interior en el futuro, tanto en lo que se refiere a lo público como a lo industrial, tiene que ver con la seguridad en las tecnologías de la información, la tradicionalmente denominada seguridad lógica o de la información y que hoy comienza a entenderse junto a la seguridad física incluida en el concepto de "seguridad convergente" o integral. El sector de la seguridad pública se verá incorporado a la tendencia, ya observada en la provisión de soluciones de seguridad de la información para grandes empresas y PYMES, de conformación de la oferta de seguridad alrededor de un mercado de servicios.[20] En efecto, algunas empresas han enlazado con la seguridad pública vía participación en proyectos de segurización de redes y sistemas, y otras lo han hecho trasladando a la seguridad pública, por su aplicabilidad, tecnologías de seguridad desarrolladas en sectores como la seguridad de comunicaciones en banca. Al final, cada de uno de esos espacios necesariamente tiene que conectar con el resto, puesto que la red de infotecnologías en empresas financieras forma parte de las infraestructuras críticas a salvaguardar de amenazas terroristas o del crimen organizado… *ergo*, como es característico de la seguridad "glocal", lo que inicialmente está constituido como un segmento de seguridad privada tiene también implicaciones sustantivas de seguridad pública. Expresado de otra manera, el hecho de que un banco sea capaz de proteger sus infraestructuras críticas de información o de que una compañía telefónica reduzca el riesgo de ataques a sus redes de distribución ya no sólo afecta al banco o a la telefónica,

[20] *Estudio sobre el sector de la seguridad TIC en España,* Observatorio de la Seguridad de la Información, León, septiembre de 2008, p. 41.

sino a todos los ciudadanos, convirtiéndose en una porción de la seguridad pública. Por tanto, para la seguridad pública sería bastante eficiente disponer de un repertorio de tecnologías críticas en sistemas de información y comunicación que, aun habiéndose desarrollado en y para otros sectores, sean útiles para mantener los trabajos de preparación y prevención en seguridad del Estado. Este tipo de tecnologías podrían contar con avales públicos en I+D+i (algunos ya se están concediendo en España vía CDTI, pero no existe una línea especializada en seguridad) y ser incorporadas, como instrumentos, al catálogo de infraestructuras críticas (el catálogo no sólo debería incluir las propias infraestructuras, sino las tecnologías encargadas de protegerlas).

(5) Los capítulos tecnológicos de la seguridad

Esencialmente a partir de la incorporación del concepto *homeland security*, pero sobre todo en línea con el progresivo proceso de toma de conciencia respecto a la revolución tecnológica en seguridad que ya hemos discutido, los aparatos de seguridad pública comienzan a elaborar repertorios de tecnologías que bien responden a necesidades a cubrir, bien a líneas estratégicas que conviene desarrollar. Estos listados de necesidades tecnológicas están elaborados por los Ministerios del Interior o seguridad de los Estados y están dirigidos a la comunicación con la industria, a armonizar las necesidades y capacidades de los aparatos públicos de seguridad con el I+D+i de las empresas del sector. Por tanto, la mayoría del contenido de estos repertorios es abierto, manteniéndose no obstante clasificados y restringidos algunos capítulos por obvias razones de no proporcionar ventaja a los grupos e individuos al margen de la ley.

Al igual que analizábamos cuando reflejábamos las dos aproximaciones al concepto de seguridad emergente de interior tras el 11-S (recordamos: una alrededor del *homeland security* y la otra combinando centros de coordinación de infraestructuras críticas con centros de análisis), en lo que respecta al establecimiento de necesidades tecnológicas, como es natural, se reproducen las mismas orientaciones. Tomando como ejemplo dos países con experiencia antiterrorista contrastada como EEUU y España, en el primero es el *Department of Homeland Security* el que publica unos capítulos de interés tecnológico muy centrado en su mandato (que excluye la inteligencia criminal o la inteligencia contraterrorista, por ejemplo), mientras en España es la Dirección de Infraestructuras y Material para la Seguridad el que ha difundido sus necesidades tecnológicas, que incluyen epígrafes para todas las tecnologías relacionadas con la seguridad interior. Así, en EEUU las necesidades de tecnologías de comunicación, información, investigación e inteligencia para agencias adscritas al Departamento de Justicia como el FBI (antiterrorista y contrainteligencia), la DEA (drogas) o la ATF (armas, explosivos) siguen su propia senda diferenciada del DHS, mientras en España las prescripciones tecnológicas de la seguridad del Estado en cualquiera de sus vertientes están diseñadas por el nuevo (desde 2004) departamento especializado del Ministerio del Interior.

En la dotación de tecnologías de información y comunicación, el Ministerio del Interior ha comunicado en abierto a la industria un programa de trabajo que está enfocado sobre seis planos de desarrollo interrelacionados para mejorar la seguridad de los ciudadanos, la de las infraestructuras, la de las misiones internacionales, la de las comunicaciones, mejorar la lucha contra el crimen organizado y la seguridad de los ciudadanos que se describen a continuación. Este repertorio de necesidades es posterior al vigente programa nacional de I+D+i 2008-2011 y no se deriva de él, lo cual genera una disfuncionalidad conceptual, pues se supone que el I+D+i debería ser dirigido en parte por las necesidades. En todo caso, es de suponer que empresas e instituciones de investigación se alinearán a las necesidades de Interior canalizando sus presupuestos y demandas de financiación en I+D+i a los epígrafes marcados por la seguridad pública. La expectativa es que en los próximos trabajos preparatorios del Plan de I+D+i 2012-2015 seguridad interior y defensa tengan subcapítulos propios dentro de un epígrafe único dedicado a la seguridad nacional y que el Ministerio del Interior tenga protagonismo activo en el primero.

(5.1) Tecnologías para mejorar la seguridad de los ciudadanos

La pregunta de partida para desarrollar esta línea de actividades es la de cómo pueden incrementarse los niveles de bienestar de los ciudadanos por medio de inversiones, sobre todo, en tecnologías de la información y la comunicación. En esta línea, se incluyen:

- Las tecnologías de prevención NRBQE (nuclear, radiológica, bacteriológica, química y explosivos), aquéllas que incorporen sistemas de detección e identificación de sustancias, así como en su integración en sistemas robotizados y monitorizados. Estos desarrollos se pretende vayan en paralelo a avances en las comunicaciones y en la protección del personal que interviene en este tipo de desastres NRBQE.
- Los sistemas de mando y control, y conocimiento situacional, que sirvan para la recogida, integración y computación de toda la información disponible con asistencia de arquitecturas informáticas de gestión del conocimiento en los entornos complejos de toma de decisiones.
- Las técnicas de detección y visualización donde se desarrollan técnicas que permitan extraer huellas latentes en la inspección de escenarios, pero también en aquellas de documentoscopia que permitan detectar la unidad de texto y firma en documentos, o la orden de sucesión de trazos, tan importante para establecer secuencias de escritura en procesos de investigación. Las pericias informáticas, con cada vez más casos criminales en donde se hace uso de soportes digitales de almacenamiento, son una especialidad que se fortalecerá tecnológicamente, desarrollando *software* con técnicas de esteganografía para la extracción de contenidos o aquél que nos posibilite realizar análisis forense de los cada vez más extendidos dispositivos de agendas personales (*Personal Digital Assistant*, PDA). En tecnología de imagen, por ejemplo, el horizonte a medio plazo está en identificar un dispositivo a partir de alguna de las imágenes que ha producido como si éstas fueran huellas de aquél, construir tecnologías de interpretación de píxeles para dotar de significado a imágenes de baja calidad, o avanzar en sistemas de identificación facial de imágenes en 2D. En este campo de la

identificación facial, precisamente, se busca disponer de sistemas de reseña en tres dimensiones que resuelvan los actuales problemas de falta de claridad de las imágenes y de variabilidad ante las distintas posiciones del sujeto.

- La antropología y balística forenses, con métodos, técnicas y tecnologías que exploren antigüedades, de huesos en antropología y de disparos en balística. En esta última, en balística, se prestará atención a las herramientas informáticas que asistan al cálculo de trayectorias y a su reconstrucción tridimensional.

(5.2) Tecnologías para la seguridad en infraestructuras

Además de la seguridad de la ciudadanía, otra de las áreas donde la investigación tecnológica se centrará en los próximos años es en la seguridad de infraestructuras y servicios públicos, la línea más aproximada al concepto estadounidense de *homeland security*. A finales de 2007 se instituyó en la Secretaría de Estado de Seguridad el Centro Nacional de Protección de Infraestructuras Críticas, para el cual se ha promovido el desarrollo de una arquitectura informática de intercambio seguro de datos sobre el estado del catálogo español de infraestructuras críticas, compuesto en la actualidad de varios miles de puntos cuya localización y naturaleza, por razones evidentes, han sido declarados secretos. Las arquitecturas tecnológicas desplegadas para la prevención de riesgos en infraestructuras críticas deberán ser capaces de apoyar el proceso de evaluación de sus amenazas y vulnerabilidades, así como de simular anticipadamente las consecuencias de una disfunción o perjuicio en una o varias de estas infraestructuras. Del mismo modo se promoverá la vigilancia inteligente de fronteras, principalmente ampliando el SIVE hacia dos direcciones especialmente: la integración multisistema en los puntos de control y la configuración de sistemas de mando, control, comunicaciones, vigilancia, inteligencia y reconocimiento. La integración multisistema deberá permitir desplegar consolas de conocimiento situacional en donde los profesionales que tienen que decidir sobre un riesgo en nuestras fronteras tengan, como si dijéramos en una sola pantalla, toda la información sobre los diferentes mecanismos de detección e identificación disponibles, tanto sobre personas como sobre mercancías. Esta integración posibilita tomar decisiones ajustadas sobre la mejor información disponible. Del mismo modo, los sistemas de mando, control e inteligencia, instalados sobre comunicaciones robustas y seguras, y beneficiándose de la integración mencionada así como de la suma de plataformas de sensores múltiples de carácter móvil, deberían permitir observar todo lo que ocurre en un área de vigilancia concreta, proporcionando señales anticipadas que permitan tomar decisiones que minimicen el riesgo sobre la frontera.

(5.3) Tecnologías para seguridad en misiones internacionales

En un mundo donde la seguridad y la inseguridad se manifiestan localmente pero se alimentan globalmente, la participación de la seguridad española en proyectos y misiones internacionales se ha multiplicado. Algunas de estas misiones son teatros de operaciones para el mantenimiento de la paz en áreas de conflicto con fuerzas policiales tipo gendarmería integradas en dispositivos militares, y otras responden más a un esquema de cooperación policial internacional en misiones civiles. En estos escenarios, se potenciarán

sistemas, apoyados en tecnología, que sirvan tanto para proteger de los efectos de un incidente como para restablecer la normalidad cuando un incidente crítico se haya materializado. Las necesidades en este punto se concretan en proteger al personal y a sus infraestructuras (vehículos, edificios) ante ataques por arma de fuego o por explosivos. Aparte de los blindajes por chaleco de nuevos materiales para las personas o por materiales a los vehículos, en términos de localización y comunicación el propósito es balizar y georeferenciar todas las unidades móviles y aumentar la calidad y potencia de las comunicaciones en zonas de operación, tanto en transmisión de voz como de datos. En el ámbito de misiones internacionales es igualmente interesante profundizar en la dotación de traductores portátiles personales, de sistemas cartográficos para reconocimientos del terreno y en el desarrollo de sistemas de almacenamiento y bases de datos de apoyo a investigaciones policiales que han de ser desarrolladas por los profesionales sobre el terreno.

(5.4) Integración, interoperabilidad e interconexión

En línea con los estándares y las mejores prácticas más distinguidas a escala internacional, otra de las áreas de actividad del programa tecnológico del Ministerio del Interior español pretende lograr una mejora continuada de la integración, interoperabilidad e interconexión de las arquitecturas tecnológicas para la seguridad. En un entorno global e interconectado los sistemas deben poder "hablarse" y "entenderse" los unos con los otros, para ofrecer un máximo aprovechamiento de los datos obtenidos y una mayor, por tanto, capacidad de decidir de manera inteligente. Claramente concienciados con estas exigencias y principios, el programa se propone lograr un tratamiento integrado de toda la información obtenida en interceptaciones judiciales de las comunicaciones, de manera que la informática posibilite detectar con la máxima rapidez las palabras que sean de interés en grandes volúmenes de datos, traducirlas de diversos idiomas, y transcribirlas de audio a texto con el máximo nivel de automatismo.

En la interceptación de comunicaciones se pide avanzar cada día en la seguridad y auditoría de nuestros sistemas, de manera que sean invulnerables a filtraciones o exposiciones indeseadas. Para ello, es privativo fortalecer continuamente la criptografía de los flujos de información, mejorando la infraestructura de clave pública para la comunicación entre órganos policiales en España y con el exterior. Por supuesto, en localización y seguimiento judicializado de personas investigadas el objetivo es lograr dispositivos cada vez más pequeños, indetectables, de bajo consumo y con la mayor sensibilidad de envío de señal. A fin de mejorar la cobertura de la recepción del seguimiento de un objetivo por la geografía española, existiendo el mínimo riesgo de pérdida del rastro o la señal, se solicita diseñar una red de estaciones de control que transporten la señal y la envíen, asegurando el continuo, a un centro de control donde los equipos de investigación judicial de la policía tengan acceso al geoposicionamiento del objetivo.

(5.5) Tecnologías contra el crimen organizado y el terrorismo

En la respuesta al crimen organizado y al terrorismo se persiguen sistemas integrados de inteligencia, centros de fusión de datos que permitan análisis tanto operativos como estratégicos integrando información multifuente y multilenguaje, posibilitando búsquedas multiplataforma de información, habilitando repositorios unificados de inteligencia, y posibilitando accesos seguros a partir del principio actualmente esencial en la cooperación policial internacional de "necesidad_de_compartir". Estos sistemas de inteligencia deben tener las propiedades tecnológicas y funcionales suficientes como para conectarse de manera segura a arquitecturas tecnológicas supranacionales de comunicación e información, como las dispuestas para operaciones multinacionales de investigación criminal o a aquéllas implantadas para desactivar diversos tipos de tráficos ilegales.

(5.6) Tecnologías para la seguridad de los ciudadanos

La última pero no la menos importante línea de desarrollo en tecnologías de seguridad tiene que ver con la seguridad y la sociedad, con los esenciales equilibrios entre seguridad y libertad, entre seguridad y privacidad. En este epígrafe interesa mucho la seguridad preventiva como política de seguridad y, en ese sentido, el Ministerio del Interior de España promocionará todas las tecnologías y recursos destinados a previsión de escenarios futuros, que sean capaces de contemplar e integrar áreas de amenazas derivadas del terrorismo y las distintas vertientes del crimen organizado. Especialmente, preocupan signos de radicalización social, con lo que los sistemas que asistan a la evaluación y anticipación de riesgos en ese ámbito parecen contar con interés preferente. Del mismo modo, la protección del ciudadano en comunidades virtuales ligadas a Internet es objeto de preocupación y atención, pues el crimen organizado y el terrorismo operan en el ciberespacio, ya sea utilizándolo de manera instrumental para apoyar sus actividades, ya sea directamente para cometer ciberdelitos. En cualquier caso, el ciudadano afronta nuevos riesgos por las manifestaciones de la criminalidad a través de Internet y será un campo de trabajo tecnológicamente denso en el futuro próximo reducir los espacios de impunidad criminal en el ciberespacio y las vulnerabilidades del ciudadano ante ellos.

Hasta aquí el repertorio de necesidades publicadas por el Ministerio del Interior. Haciendo un paralelo simplemente como referencia, en EEUU el DHS ha publicado sus prioridades sobre necesidades tecnológicas,[21] que como hemos mencionado están limitadas dentro de los contornos del *homeland security* tal como es entendido, es decir, dejando la investigación e inteligencia criminales y la inteligencia contraterrorista para las agencias federales de Justicia. La propuesta estadounidense clasifica las necesidades en doce categorías coincidentes con los mandatos departamentales del DHS. Estas categorías son: (1) seguridad de fronteras; (2) seguridad de la carga; (3) defensa química/biológica; (4) ciberseguridad; (5) seguridad de transportes; (6) defensa contra artefactos explosivos improvisados (*Improvised Explosive Devices*, IED); (7) gestión de incidentes; (8)

[21] *High-PriorityTechnology Needs, v2.0*, Science and Technology Directorate, DHS, junio de 2008.

compartición de información; (9) protección de infraestructuras; (10) interoperabilidad; (11) seguridad marítima; y (12) identificación y detección (*screening*) de personas.

El planteamiento tecnológico del DHS estadounidense está enfocado hacia la adquisición y articulación de capacidades para la seguridad y, para ello, priorizarán tecnologías que puedan ser desarrolladas, maduradas, entregadas y comercializadas como un estándar en plazos no superiores a los tres años. Aunque más completo y detallado el estadounidense, las tecnologías representativas de cada uno de los capítulos no varían demasiado de las consideradas en el programa español. Si acaso, pueden subrayarse: las tecnologías no invasivas de inspección de carga y las técnicas de detección automática de objetivos en cargas anómalas (que en el caso español corresponde la competencia a Aduanas, aunque la Guardia Civil tenga poderes de inspección como resguardo fiscal del Estado); paradigmas y sistemas de detección para amenazas biológicas emergentes, modificadas o novedosas; todas las relacionadas con ciberseguridad, como protocolos de seguridad en Internet, modelización y simulación de efectos de ciberataques; estándares para la gestión de identidades o modelos de detección de amenazas internas en sistemas de información, que están ausentes del programa español probablemente debido a las competencias del CNI en ciberseguridad; las tecnologías sobre IED; y centros de fusión de datos para ofrecer *common operational pictures* (perfiles de conocimiento situacional), que son tecnologías avanzadas integradas en sistemas de mando y control presentes en la Unidad Militar de Emergencias (UME) española y en centros de emergencias de las Comunidades Autónomas.

En conclusión, por tanto, si bien las prioridades tecnológicas para seguridad interior, aunque más detalladas por un lado y restringidas por otro en el caso estadounidense, nos revelan que los horizontes de desarrollo científico y tecnológico están más o menos alienados globalmente, las variaciones se producen en el revestimiento estratégico del enfoque. Como apreciamos inmediatamente, cuando sumamos los centros de investigación científica del DHS con el sentido que le confiere a sus prioridades tecnológicas para la seguridad, la permanencia estratégica y la búsqueda de técnicas y tecnologías que procuren estándares de seguridad son parámetros constituyentes de su cultura tecnológica de seguridad. En la perspectiva española no se explicita suficientemente esa vocación estratégica, ya sea porque la fase de transición en esa revolución de los asuntos tecnológicos para la seguridad lleva otro ritmo, porque la cultura tecnológica en Interior está menos desarrollada que la implantada en Defensa desde hace décadas o bien porque las restricciones presupuestarias han ralentizado la inversión en ciencia tecnológica para la seguridad. Esa falta de concreción estratégica también es visible en el siguiente conjunto de capítulos relativos a la tecnología, aquellos del I+D+i, es decir, de la investigación científica y de su financiación.

(6) Capítulos de I+D+i y financiación

Como hemos procurado insistir, en una adecuada cultura tecnológica de seguridad interior no es conveniente avanzar en los desarrollos tecnológicos instrumentales sin una sólida base de investigación científica. La financiación de la investigación científica en tecnologías de seguridad tiene, desde España, dos posibilidades inmediatamente visibles y una menos explorada. Las dos visibles son el capítulo de seguridad del 7º Programa Marco de la Comisión Europea, por un lado, y el Plan Nacional de I+D+i 2008-2011, por otro. La menos explorada, aunque existente, es la iniciativa de ciencia y tecnología de la OTAN, la *Research and Technology Organisation* (NATO-RTO) que prorroga una dilatada cultura de promoción de la investigación científica dentro de esa organización.[22]

Comenzando brevemente por la última posibilidad reseñada, la NATO-RTO fomenta la investigación científica cooperativa y el intercambio de conocimiento técnico entre los 26 Estados miembros y los 38 asociados a la Alianza Atlántica, atribuyéndose una red de 3.000 científicos apoyados desde un organismo ejecutivo, la RTA (*Research and Technology Agency*), con sede en las inmediaciones de París. La investigación de la agencia está bastante concentrada, entre otros, en la modelización y en la simulación y tiene paneles técnicos destinados a cuestiones de interés para la seguridad interior como la integración de sistemas pero sigue al margen de los Ministerios de Interior debido a que la OTAN se considera como una organización exclusivamente dedicada a la cultura de defensa. Es cierto que esto ha venido siendo así, aunque la propia OTAN ya reconoce desde 1991 que los riesgos a los que se enfrenta son globales, muldimensionales y complejos. Sin embargo, con la última cumbre estratégica de la Alianza tras su 60 aniversario y, sobre todo, con su enfoque antiterrorista tras el 11-S, la OTAN ha constituido dos programas de investigación sobre terrorismo, el *Nato Counter-Terrorism Technology Development Programme* (NTCTDP) y el *Defence Agains Terrorism* (DAT), donde gana peso la función colectiva de seguridad preventiva en sintonía con las reorientaciones estratégicas de los aliados con más peso. En esta línea, son todavía tímidas aunque firmes las voces que piden alimentar la OTAN con un componente de seguridad interior, con la participación de los Ministros de Interior.[23] Como bien subraya Arteaga, la función de la OTAN es emplear la fuerza para defenderse ante amenazas, y sobre ese fundamento general los Aliados determinarán en cada momento la naturaleza de esas amenazas y de qué manera utilizarán la fuerza para prevenirlas o reducirlas.[24]

[22] F. Carvalho-Rodrígues, "NATO's Science Programs: Origins and Influence", *Technology in Society*, vol. 23, nº 3, 2001, pp. 375-381.

[23] Entre ellas, la de F. Portero, *Presente y Futuro de la OTAN*, conferencia impartida en el Instituto Gutiérrez Mellado, 30/XI/2006, *www.iugm.es/ARCHIVOS/otan/Conf-51.pdf*. También lo ha considerado el ex presidente del Gobierno español, J.M. Aznar en "El Futuro de la OTAN: una oportunidad para España", *ABC*, 6/IV/2009, http://www.abc.es/20090406/opinion-tercera/futuro-otan-oportunidad-para-20090406.html.

[24] F. Arteaga, "La cumbre de la OTAN en Estrasburgo-Kehl: ¿revisar sus fundamentos tras 60 años?". ARI, nº 56/2009, Real Instituto Elcano.

Aparte de la alternativa eventual de la OTAN en tecnologías para seguridad, la financiación, y por tanto las líneas, de investigación científica tienen en el 7º Programa Marco de Investigación y Desarrollo Tecnológico 2007-2013 de la Unión Europea un referente visible. El 7PM-UE tiene 50.000 millones de euros de presupuesto y está estructurado en cuatro programas específicos: cooperación, personas, ideas y capacidades. Con independencia de que alguna investigación pueda ser alojada en otros programas (por ejemplo en ideas, donde se financiación investigaciones innovadoras que se sitúen en las fronteras del conocimiento), el programa de cooperación cuenta con un área temática específica de seguridad, dotada con 1.400 millones de euros en total. Si utilizamos las cifras de adjudicación financiera como baremo de la importancia otorgada a los capítulos, tendremos que decir que de las 10 áreas temáticas del programa de cooperación, la seguridad ocupa el octavo lugar, sólo por delante de la investigación sobre el espacio y las ciencias socioeconómicas y humanidades, las últimas en dotación. La diferencia entre el capítulo de seguridad y el primero en la lista, tecnologías de información y comunicación, es de alrededor de 7.500 millones de euros. No sabemos si este baremo refleja el estado de la cultura de investigación en seguridad en Europa, la importancia concedida por la Comisión Europea a este tópico, ambos, o la influencia de terceras variables.

En todo caso, los 1.400 millones de euros para seguridad en el 7PM-UE se ejecutan a través de convocatorias anuales, en las que se otorga prioridad en cada ocasión a determinadas líneas. Las prioridades generales tienen, como es natural, conexión conceptual con las necesidades y capacidades expresadas por los Estados en lo relativo a tecnologías para la seguridad. En concreto, el área de seguridad está estructurada en las siguientes líneas:

- Incremento de la seguridad de los ciudadanos: soluciones tecnológicas para la protección civil, la bioseguridad, la protección contra el crimen y el terrorismo.
- Incremento de la seguridad de infraestructuras: segurización de las infraestructuras en áreas tales como las TIC, el transporte, la energía y los servicios en los sectores administrativo y financiero.
- Vigilancia inteligente y seguridad fronteriza: tecnologías, equipamiento, herramientas y métodos para proteger las fronteras europeas por tierra y mar.
- Restauración de la seguridad en caso de crisis: tecnologías, comunicación y coordinación en apoyo de tareas de recuperación y rescate civil y humanitario.
- Mejora de la integración de los sistemas de seguridad, interconectividad e interoperabilidad: recolección de información para la seguridad civil, protección de la confidencialidad y trazabilidad de las transacciones.
- Seguridad y sociedad: aspectos socioeconómicos, políticos y culturales de la seguridad, ética y valores, aceptación de soluciones de seguridad, medioambiente social y percepciones de la seguridad.

- Coordinación y estructuración de la investigación en seguridad: coordinación entre los esfuerzos de investigación europeos e internacionales en áreas civiles, de seguridad y defensa.

Como puede comprobarse, el espectro temático es lo suficientemente amplio como para abordar cualquier aspecto de investigación científica sobre la seguridad, y su variedad e importancia obliga a interrogarse sobre si el hecho de que la dotación presupuestaria para investigar en seguridad ocupe el octavo lugar en prioridades es debido a la fortaleza o la debilidad de la industria de seguridad en Europa o a la mayor o menor implantación de una cultura de la seguridad entre sus ciudadanos. A este último respecto, un mandato claro del 7PM-UE en su área de seguridad es contribuir a la seguridad de los ciudadanos de la Unión al mismo tiempo que impulsar la competitividad industrial en el ámbito de la investigación científica. De manera que, sobre el tópico de la seguridad, el núcleo filosófico y operativo del 7PM-UE es la industria de la seguridad en Europa. Así, a mayor desarrollo de esta industria y de un tejido de I+D+i adyacente, se supondrá un mayor aprovechamiento del potencial del 7PM-UE.

La elaboración de los tópicos financiables dentro del área de seguridad en el 7PM-UE sigue un procedimiento similar al desarrollado para la elaboración de los planes nacionales de I+D+i, esto es, configuración de paneles de expertos y expertas que, aplicando metodología prospectiva y en función de las necesidades de los Estados a futuro, son capaces de determinar las líneas que alojarán las prioridades de investigación. En esos trabajos de preparación del repertorio de áreas de investigación para el 7PM en seguridad, en la UE destaca el informe[25] elaborado por el *European Security Research Advisory Board* (ESRAB), un amplio panel de expertos que combinaba representantes institucionales, científicos, una nutrida presencia de la industria y también de los usuarios finales (*end-users*) de los desarrollos tecnológicos, todo en un fructífero intento de proporcionar un encuentro entre la oferta y la demanda de tecnologías de la seguridad. El resultado es una completa agenda de investigación en tecnologías para la seguridad y en varios parámetros concordantes de la sociología de la seguridad, que se trasladarían después casi sin excepciones a la estructura del área de seguridad del 7PM.

Otro de los cuerpos europeos que tratan de impulsar específicamente la ciencia en seguridad en general, con el peso correspondiente a desarrollo tecnológico, es el *European Security Research and Innovation Forum* (ESRIF). El ESRIF es un laboratorio de ideas que trata de funcionar como espacio de diálogo principalmente entre la industria y el sector público de usuarios finales, incorporando también componentes universitarios de investigación. Desde su constitución en 2007 a partir de las conclusiones de la II Conferencia Europea de Investigación en Seguridad celebrada en Berlín, el ESRIF es un foro de composición relativamente abierto que se ha estructurado en un plenario con representantes nominados por los Estados miembros y 11 grupos de trabajo (prospectiva;

[25] *Meeting the Challenge: the European Security Research Agenda*, ESRAB (09/2006), Office for Official Publications of the European Communities, Luxemburgo.

amenazas NBQRE; espacio; identificación de personas y bienes; gestión de crisis; innovación, industria y base tecnológica; gobernanza y coordinación; seguridad de los ciudadanos, contraterrorismo y crimen organizado; seguridad de fronteras; seguridad de infraestructuras; y dinámicas humanas y sociales de la seguridad) en donde se materializa ese diálogo fundacional entre lo público y lo privado. Junto a ESRAB, el ESRIF ha contribuido con su pensamiento a la estructura de categorías del 7PM-UE en el apartado de seguridad, aunque la opinión general es que su potencial como foro de comunicación integral no ha sido todavía ni siquiera medianamente aprovechado.

El ejercicio europeo del ESRAB intentó trasladarse en España a la estructura prospectiva facilitadora para construir el VI Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica para el período 2008-2011. Como se ha apuntado, se constituyó un panel de expertos donde coincidieron representantes de la industria, de las instituciones y de la universidad, con una presencia marginal de usuarios finales, bajo el paraguas de la Fundación Española de Ciencia y Tecnología (FECYT) con un mandato de la Comisión Interministerial de Ciencia y Tecnología. Mientras el esfuerzo ESRAB se concentraba en seguridad específicamente, en el caso español el panel del I+D+i nacional combinó la seguridad con la defensa, con la lógica descompensación y el sesgo resultante hacia la segunda componente debido a su mayor cultura, experiencia y dedicación en orientación investigadora. Esto no quiere decir que el aparato de la seguridad deba ignorar por completo los desarrollos en defensa sino que, como ha demostrado la labor en la UE, aconseja la propia ESRAB y sugiere la idiosincrasia de la seguridad interior, lo más eficiente es que la seguridad pública desarrolle su propia cultura de I+D+i, estableciendo puentes de comunicación con defensa para beneficiarse de su experiencia y, al mismo tiempo, compartir la investigación en tecnologías comunes de base para producir sinergias. Es decir, que se debe fomentar es un juego de suma variable donde el crecimiento de un sector beneficie al otro, en lugar de uno de suma cero donde todo lo que gane un sector se logre a costa del otro.

El desarrollo de los capítulos financiables del Plan Nacional español del I+D+i en seguridad y defensa tuvo en cuenta tanto el estado de la investigación científica, el desarrollo tecnológico nacional y el desarrollo industrial en cada materia para ponderar los índices que finalmente identificarían cada línea de investigación a sugerir incluir en el Plan. En el programa español, el sector de la seguridad y defensa es uno de los 11 sectores clave en el área de desarrollo e innovación tecnológica sectorial dedicada a "facilitar a los sectores industriales los instrumentos y programas necesarios para acometer las actividades dirigidas al diseño de productos, procesos o servicios nuevos, modificados o mejorados. El fin último es la mejora de la competitividad empresarial mediante la resolución de los problemas identificados en los sectores de interés para el desarrollo socioeconómico del país".[26] Sin embargo, ni la seguridad (ni la defensa) son consideradas

[26] El Plan Nacional de I+D+i está estructurado en cuatro áreas: (1) generación de conocimientos y de capacidades científicas y tecnológicas, destinada a la investigación a largo plazo no finalista en términos de demanda y cuyo objetivo es la propia generación de nuevo conocimiento, incluida la realizada por el sector

como áreas horizontales sobre las que se deban promover la investigación básica (área 1) o las acciones estratégicas (área 4) y no cuentan con un programa nacional específico dentro del plan. El problema de este planteamiento es que, si bien es cierto que la investigación en seguridad y defensa tiende a ser eminentemente aplicada –como nos recuerda el documento de necesidades del DHS estadounidense cuando sitúa en tres años el límite temporal para un desarrollo tecnológico a contratar–, lo que de verdad genera conocimiento y poso investigador en un sector, y cultura científica, es una base de investigación a largo plazo con acciones tales como las definidas en el área 1 del Plan estratégico español. Del mismo modo, parece cuestionable no considerar a la seguridad una acción estratégica de investigación y sí hacerlo, por ejemplo, con la salud, aunque probablemente sea un efecto de (in)maduración del período 2008-2011, el futuro próximo nos mostrará cómo cada vez más la seguridad pasa a considerarse un capítulo social horizontal con repercusiones en muchas facetas de la vida diaria del ciudadano.

Desde su inauguración en 2007, se han producido tres convocatorias del área de seguridad del 7PM-UE, una de ellas conjunta con el área TIC. En el caso español, ha sido de momento una la convocatoria[27] que involucra a proyectos de investigación en seguridad y defensa, a través del Programa Nacional de Proyectos de Investigación Aplicada del Plan Nacional de I+D+i y donde, por cierto, la seguridad comienza a ser considerada un subsector específico.

En definitiva, sobre el papel tanto la UE –en calidad de marco aglutinador– como España cuentan con programas de I+D+i en seguridad, con (complejos y nutridos en la Unión) espacios de reflexión y prospectiva acerca de los nuevos escenarios y los nuevos desarrollos que requerirán, con repertorios de necesidades de usuarios finales más o menos clarificados y, en general, con la conciencia de que las tecnologías son indisolubles de la *seguridad glocal* del presente. Sin embargo, y a pesar de que los dos planes principales en los dos niveles, el 7PM en la UE y el Plan 2008-2011 en España están construidos sobre plantillas estratégicas, ninguno de los dos tiene conexión estratégica, es decir, no se derivan de estrategias integrales de seguridad cada uno en su escala. En el caso español, tal precepto es de momento impracticable porque el Estado carece de momento de Estrategia Nacional de Seguridad aunque se están dando pasos en esa dirección. En el caso de la UE la excusa es más difícil de encontrar, pues la Estrategia Europea de Seguridad data del año 2003, tres años antes de finalizar los trabajos para el 7PM-UE. Sin embargo, una pista para esta desconexión del I+D+i respecto de la gran estrategia nos la puede dar el hecho de que la palabra "tecnología" sólo se cite dos veces

privado; (2) fomento de la cooperación en I+D; (3) desarrollo e innovación tecnológica sectorial, con el objetivo de poner a disposición de los sectores industriales los instrumentos y programas necesarios para llevar a cabo sus actividades de desarrollo e innovación tecnológica; y (4) las acciones estratégicas, dar cobertura a las más decididas apuestas del Gobierno en materia de I+D+I, con un concepto integral en el que se pongan en valor las investigaciones realizadas, así como su valorización y transformación en procesos, productos y servicios para la sociedad. Las acciones estratégicas identificadas corresponden a sectores o tecnologías con carácter horizontal (son cinco los sectores considerados).

[27] BOE 79, 1/IV/2009, p. 31151, *http://www.boe.es/boe/dias/2009/04/01/pdfs/BOE-A-2009-5486.pdf*.

en el documento estratégico de la Unión, una en la introducción para ratificar que supone un desafío y la otra para mencionarla respecto a la amenaza relacionada con los misiles. Tampoco existe, en ninguno de los supuestos y que se conozca, un plan estratégico industrial en seguridad, que ponga al fragmentado tejido empresarial en armonía con el pensamiento a futuro de la seguridad pública, en la que participan de facto a través de sus desarrollos tecnológicos. Tal vez influya el hecho de que el entramado tecnológico-industrial de la Unión está muy orientado a la Agencia Europea de Defensa, mientras la seguridad sigue una vía diferenciada, desligada y con todas las limitaciones que hemos señalado en una UE donde seguridad y defensa no están integradas. Con todo, después de la revisión de este escenario de "debilidad estratégica", lo cierto es que tanto las necesidades de los usuarios como (al menos los planteamientos de) la investigación están bastante alienadas entre la UE y uno de sus Estados Miembros como España, y entre estos y EEUU. No sabemos si es un efecto mimético o el resultado de que (al menos en los planteamientos) el horizonte está bastante claro para todos.

(7) Conclusiones y prospectiva

En enero de 2007, la Fundación Círculo de Tecnologías para la Seguridad y la Defensa constituyó un foro de debate multidisciplinar bajo la denominación de "Iniciativas para el fomento de la investigación, la transferencia tecnológica, la innovación y la competitividad internacional del sector de la Seguridad". Las conclusiones publicadas[28] de ese encuentro de trabajo nos sirven bien para ilustrar someramente el estado de la industria, el desarrollo tecnológico y la base de cultura tecnológica de seguridad en el momento actual:

- En el modelo anglosajón la inversión en tecnologías está más orientada hacia la creación de capacidades, mientras que en países como España, y en general aquellos de un modelo continental de la seguridad, la inversión en tecnología ha estado enfocada hacia las necesidades.
- Existe una dependencia tecnológica importante del exterior, que es más relevante todavía cuando se piensa en procesos de estandarización: en muchos casos en Europa se siguen estándares estadounidenses por requerimientos de interoperabilidad.
- Los operadores industriales desarrollan sus líneas de negocio en un ambiente estratégico débil por parte de los usuarios finales.
- Si bien muchas de las TIC que se emplean tienen elevados estándares de seguridad, a veces la vulnerabilidad llega por los sistemas de gestión encargados de operar esas TIC.
- El sector empresarial está fragmentado y formado esencialmente por PYMES, circunstancia que corrobora el diagnóstico hecho por la FECYT en la introducción al Plan Nacional del I+D+i.

[28] *Iniciativas para el fomento de la investigación, la transferencia tecnológica, la innovación y la competitividad internacional del sector de la Seguridad*, Fundación Círculo de Tecnologías, Madrid 2007.

- Los sectores de seguridad y de defensa necesitan capacidades diferentes y, por tanto, desarrollos tecnológicos específicos, pero debe haber comunicación en todo caso, e integración de esfuerzos cuando tengan que ver con tecnologías comunes.
- Destaca la importancia de la innovación como motor del sector, proponiéndose estructuras comunes de I+D+i, mejorándose la interlocución público-privada y fomentándose la interacción en *clusters* empresariales que eviten fragmentación.
- Traducir los foros de reflexión en plataformas tecnológicas efectivas.
- Los procedimientos de contratación de las administraciones públicas son extraordinariamente complejos, con profusión de trámites burocráticos.

Después de revisar las particularidades del progreso tecnológico en seguridad interior, puede concluirse que el vertebrador más claro del escenario de convergencia entre la revolución tecnológica y la que podemos considerar revolución de los asuntos de seguridad ante las amenazas globales (el término de convergencia sería revolución tecnológica de los asuntos de seguridad), es claramente cultural. Como señala la FECYT: "la falta de tradición científica y tecnológica en la sociedad española" es un factor que dificulta la utilización de las tecnologías en empresas y administración pública,[29] aunque cabe añadir que la falta de tradición tecnológica y de investigación científica en los asuntos de Interior es un elemento que introduce lentitud en el ritmo de progreso del universo tecnológico para la seguridad. Esas constricciones culturales, que lo son en el sentido de percepción de una determinada realidad y no en la preparación académica, influyen directamente en la debilidad del sector industrial español en seguridad. Con todo, esa debilidad no está estimada, es decir, no está cuantificada. Un interesante estudio a promover sería evaluar, precisamente, la solidez, el sentido de la identidad y los vectores potenciales de desarrollo de una eventual industria española de la seguridad.

La insuficiente cultura tecnológica de la seguridad en empresas y administración pública tiene vinculaciones con la débil conexión estratégica de los programas de I+D+i en seguridad, ya sean españoles o europeos. A su vez, es factible ligar la combinación de insuficiencia cultural (o del significado que se le otorga a las tecnologías y a la seguridad) y superficialidad estratégica con, ésta sí, carencia de una política industrial en tecnologías de seguridad que impulsada desde el sector público sea definida junto al sector privado. El resultado más inmediato de esta concatenación de vulnerabilidades estratégicas es que se ha invertido poco en el definitivo diseño de capacidades que prepararán a la seguridad pública para afrontar con eficiencia tecnológica y metodológica los desafíos de las amenazas globales, aunque se hayan definido y detallado las necesidades tecnológicas para la seguridad interior. Conviene ir encaminándose, por tanto, hacia un diseño en donde las capacidades sean necesidades y éstas se traduzcan eficazmente en prescripciones y requisitos técnicos. Y a este fin coadyuvaría la traducción de la voluntad política en directrices políticas de orientación del sector, una especie de directiva nacional

[29] *Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica*, Comisión Interministerial de Ciencia y Tecnología, 2008.

de seguridad, del mismo modo que existe una directiva de defensa nacional, y derivada de la Estrategia de Seguridad Nacional todavía pendiente.

El estado actual de las tecnologías aplicadas a la seguridad interior se encuentra en un período de transición en donde convergen varios procesos paralelos y complejos. Entre ellos están: la internacionalización de la propia seguridad interior y su imbricación con la seguridad exterior; la conexión entre seguridad y defensa, con la progresiva conformación estratégica de la defensa como una función de seguridad; la aproximación de la seguridad interior y de la investigación policial hacia metodologías de los servicios de inteligencia, debido a la paulatina incorporación de la seguridad preventiva a las fuerzas de policía; la convergencia entre seguridad de la información y seguridad de las personas y bienes; la apertura de una dimensión propia de seguridad en el ciberespacio que requiere, ya no sólo convergencia, sino ciberseguridad; y la conexión entre economía y bienestar del ciudadano y entre inteligencia económica y seguridad.

Todos estos procesos y su interacción determinarán nuevas estructuras de seguridad, que ya no serán domésticas o interiores ni internacionales o exteriores, sino propias de una seguridad "glocal", definida por una malla mundial en red que sea capaz de evaluar integralmente las amenazas para diseñar globalmente soluciones de eficiencia local o doméstica pero incardinadas a su vez en la red de interdependencia global. Hasta tanto esos procesos interactivos maduren, la seguridad interior está en tránsito de reformulación de su identidad y eso repercute, directamente, en una suerte de revolución tecnológica de los asuntos de seguridad.

La conformación multipolar de las amenazas y las vulnerabilidades pero, sobre todo, la materialización global de una de ellas en forma de terrorismo yihadista ha acelerado el proceso de transición de la seguridad interior hacia lo global. De esa aceleración ha surgido un concepto, *homeland security*, que se ha incorporado a los modelos de seguridad de algunos Estados a través de estructuras intercomunicadas pero no integradas. Aun así, y con denominaciones distintas, se han constituido o reformulado, por un lado, las agencias o centros de fusión o de análisis e inteligencia, unas veces con poderes de investigación y otras no y, por otro, los centros o agencias de protección de infraestructuras críticas. Ambos tipos de centros se han conectado pero todavía no se han integrado, aunque es cierto que las disfunciones potenciales son menores cuando todos los centros se encuentran bajo una sola dependencia (los Ministerios de Interior, por ejemplo) o reportan a un mismo responsable (como el MI5 británico). En todo caso, como resultado más o menos presente en unos casos o en otros, tenemos: (1) diversidad de enfoques tecnológicos; (2) necesidades no armonizadas; y (3) ausencia de cultura tecnológica común.

La estructura tecnológica de la seguridad depende de la calidad y permanencia a largo plazo de tres tejidos: el universitario (investigación), el industrial (desarrollo e innovación) y el institucional (uso final y planteamiento estratégico). La relación entre

ellos muchas veces se produce en el marco de programas de financiación, a partir de convocatorias en donde se combinan varias piezas especializadas constituyendo consorcios. En este punto, la legislación de contratos en la administración pública española se está revelando como un verdadero factor de vulnerabilidad para la concurrencia del sector público y del sector industrial y tecnológico de seguridad en los programas europeos de I+D+i, y también en los nacionales. La densa, burocratizada y compleja maquinaria de contrataciones de la administración pública española se viene denunciando en foros especializados como un obstáculo para la concurrencia de empresas a convocatorias de contratos públicos (algunas de ellas, las más experimentadas, tienen especialistas dedicados exclusivamente a elaborar la documentación necesaria para "pasar" las exigencias burocráticas), con lo que la complejidad burocrática desincentiva la presencia en el 7PM-UE de consorcios de investigación basados en un sólido componente nacional. Incluso, si reciben financiación como incentivo, el dinero se ingresa en una cuenta del Tesoro Público y es prácticamente irrecuperable para el departamento involucrado si no es tras un *vía crucis* burocrático, por lo que de hecho, algunos responsables del sector manifiestan en privado tal y como está el sistema de contrataciones renuncian a considerar su concurrencia a programas europeos *porque no les merece la pena*.

Otro elemento que no está siendo contemplado en los procedimientos españoles es la evaluación de riesgo tecnológico, presente en otros países. Desde ESRIF se ha propuesto la *European Security Label* para las tecnologías como un proceso de certificación y garantías. De momento es una propuesta. Sin embargo, la propia interoperabilidad contemplada como elemento de prescripción tecnológica en los repertorios de necesidades que hemos revisado en este Documento de Trabajo no es un axioma que se tenga en cuenta, no ya en los pliegos de prescripciones técnicas de adquisiciones –en donde generalmente figura como concepto teórico– sino en la práctica de los desarrollos tecnológicos. En el ámbito de comunicaciones se ha avanzado desde hace unos años, aunque por ejemplo sin tenerse en cuenta (como condición necesaria) la interoperabilidad entre las policías nacionales con las autonómicas o las locales, lo que puede suponer un problema a la hora de afrontar emergencias o crisis. En otras TIC, como los sistemas de inteligencia o apoyo a la decisión, puede darse perfectamente el caso de que dos departamentos de unidades de seguridad desarrollen sistemas de bases de datos distintos o directamente incompatibles. Desde luego que esos sistemas podrían intercomunicarse eventualmente, pero construyendo un puente tecnológico por encima de ellos, casi un nuevo y tercer sistema de bases de datos. Del mismo modo, en los procesos de compra de infotecnologías de las instituciones de seguridad, aunque intrincados administrativamente, no se contempla la evaluación de lo que se denomina *technology acquisition risk* (riesgos de adquisición), una serie de protocolos de toma de decisiones ya implantados en la cultura tecnológica de defensa.

En definitiva, la revisión del estado de la cuestión en lo que a tecnologías en asuntos de seguridad interior se refiere nos deja numerosos interrogantes cuyo camino a la

resolución muy bien pasaría por la elaboración de un análisis tipo DAFO, en donde se determinaran con claridad las amenazas y las oportunidades para el sistema español, sus debilidades y fortalezas. Puesto que estamos en un momento de *transición revolucionaria* y dado que la posición española no está demasiado retrasada con respecto a los países de nuestro entorno, parece sugerente acometer ese análisis como primer paso hacia la búsqueda de una identidad tecnológica en la seguridad interior española.

Andrés Montero Gómez
Director de Thint Intelligence