

# Estrategias de prevención: balance desde el 11-S

Antonio M. Díaz Fernández

---

**Cinco años después de los atentados a las Torres Gemelas, los servicios de inteligencia siguen envueltos en un proceso de modernización. Los nuevos riesgos exigen un uso más eficaz de la información, cooperación internacional y estrategias preventivas.**

---

Cómo si el recién estrenado milenio mostrase con retardo una de sus apocalípticas consecuencias, las ciudades de Washington y Nueva York se veían golpeadas desde el cielo. Políticos y ciudadanos miraron entonces hacia sus servicios de inteligencia buscando explicaciones con una mezcla de desconcierto y recriminación. Muchas preguntas y reflexiones comenzaron a producirse en un afán por comprender, en primer lugar, qué nos había atacado y, seguidamente, si continuaría más allá de aquel décimo primer día del mes de septiembre de 2001.

Uno de los múltiples análisis de urgencia fue el publicado en el número 84 de *POLÍTICA EXTERIOR*.<sup>1</sup> Para aquel análisis de situación solo se dispuso de unas pocas jornadas, y en él se buscaba apuntar cuáles eran los retos y las adaptaciones que debían vivir los servicios de inteligencia para conjurar los nuevos peligros que acechaban a nuestras sociedades y, por extensión, apuntaba en qué habíamos fallado para que se produjesen aquellos atentados.

Cinco años después, se intenta ahora responder si las líneas propuestas se han confirmado como válidas y, en segundo lugar, cuáles son las dificultades y retos que esta evolución presenta.

Los servicios de inteligencia se han caracterizado por tener espectaculares errores que van desde Pearl Harbour (1941) a la caída del sah (1979) pasando por la desintegración de la Unión Soviética (1989). Pero hay una cierta diferencia con el fiasco del 11-S. En las anteriores ocasiones, los fallos eran debidos a un modelo inmaduro engendrado por las urgentes e inesperadas necesidades de lo que, posteriormente, se conocería como la guerra fría.

---

Antonio M. Díaz Fernández es profesor de Ciencia Política en la Universidad de Burgos y autor de *Los servicios de inteligencia españoles*. Madrid: Alianza, 2005.

Sin embargo, los atentados contra Estados Unidos sorprendieron a los servicios de inteligencia, por primera vez en su vida, caminando hacia un modelo sobre el cual ya se había reflexionado.

Una veintena de grupos de trabajo y paneles de expertos habían estudiado el nuevo modelo desde la caída del muro de Berlín. Por citar algunos, la comisión Preparing US Intelligence for the XXI Century detallaba una serie de elementos técnicos; la Aspin-Brown, en marzo de 1996, abogaba por el fortalecimiento del director de la comunidad de inteligencia –el responsable de la CIA– en la centralización de la recolección y análisis, y la National Performance Review de 1993, que elaboró el vicepresidente Al Gore, indicaba las adaptaciones a introducir en la comunidad de inteligencia, a la que contundentemente acusaba de “haberse permitido trabajar en cuestiones que no estaban en directa relación con las necesidades de los políticos”.

Por tanto, los políticos eran conscientes de la impostergable necesidad de cambio y sabían técnicamente cómo realizarlo. Asombroso, en consecuencia, comprobar que, en vez de caminar hacia el modelo que sustituyera al de la guerra fría, muchos Estados comenzaban a dismantlar su inteligencia. De forma considerable, se recortaron los presupuestos, lo que incidió en el personal, en el despliegue exterior y en los procesos de innovación, tanto tecnológica como analítica. Canadienses o australianos, siempre muy cuidadosos con sus servicios de inteligencia, redujeron sus plantillas alrededor de un 20 por cien, en igual medida que sus presupuestos; e incluso, en un punto de paroxismo, los holandeses llegaron a dismantlar su servicio de inteligencia exterior por considerarlo innecesario.

El modelo de inteligencia establecido durante la guerra fría se deshinchaba por un extremo mientras que esos mismos hilos debían emplearse para tejer el nuevo. Éste debería haber estado listo a comienzos de siglo, pero una mezcla de disfrute de los “dividendos de la paz” y de “fin de la Historia” lo impidió. Los atentados de septiembre de 2001 fueron un punto de inflexión porque mostraron lo inaplazable de la evolución y amplificaron el lamento, si cabe con mayor intensidad, de no haber aprovechado la última década para caminar con tranquilidad hacia el nuevo modelo de inteligencia. Sin embargo, la amenaza ya se había materializado y, mientras no se dispusiera del instrumento adecuado, habría que hacerle frente con el existente que ejercería el papel de modelo refugio.

A pesar de no ser ideal, el modelo de inteligencia de la guerra fría era posiblemente el que mejor resultado había dado a los espías porque, realmente, se organizaba en torno a ellos y no sobre las necesidades de los centros políticos de decisión. Someramente, se basaba en la separación de cometidos entre fuerzas policiales y de inteligencia y en el uso intensivo de las

---

1. Antonio M. Díaz Fernández, “La transformación necesaria”, *POLÍTICA EXTERIOR*, núm. 84, noviembre-diciembre, 2001, págs. 1812-187.

técnicas de captación de información con poco respeto hacia los Derechos Humanos y libertades ciudadanas, lo que no implicaba mayor eficacia en su tarea de asesoramiento al decisor político.

Las capacidades tecnológicas adquiridas en la última década poco han tardado en mostrar los problemas de este modelo refugio sin un adecuado control político. Así, en los últimos cinco años, ha habido un recurso a elementos del pasado como detenciones extraordinarias en limbos legales como Guantánamo, o vuelos secretos de la CIA para transportar ciudadanos a prisiones secretas que, en su mayor degeneración democrática, eran confiados a autoridades de países poco democráticos, donde el empleo de la tortura para la obtención de información es habitual.

### **A mitad del camino**

En 2001 expuse mi concepción sobre cuál debía ser el modelo de inteligencia que sustituyera al de la guerra fría y que tendría como gran enemigo –aunque no exclusivo– el terrorismo. Para configurarlo, había que emprender ciertas modificaciones. En el plano interno, indicaba que era necesario “rediseñar los procesos de análisis de la enorme cantidad de información que los servicios de inteligencia simplemente acumulan”. En esta dirección, los servicios han proyectado reclutamientos que llevarán a que, entre 2001 y 2008, dupliquen sus plantillas de espías, lo que supone una respuesta cuantitativa al problema para simplemente recuperar los niveles del pasado. Sin embargo, esta masiva entrada de efectivos va a generar problemas nada deseñables. En un servicio de inteligencia, los superiores tienen un papel que va más allá del control: transmiten la cultura organizativa y los patrones de análisis, lo que será más difícil al disminuirse la proporción entre jefes y analistas. Este hecho va a complicar, o al menos retrasar, el logro de una de las propuestas de la comisión del 11-S: mayor imaginación y mayor agresividad en los análisis. Por esto también es necesaria una evolución cualitativa, a través de nuevos esquemas de análisis que israelíes o norteamericanos están desarrollando para la gestión del conocimiento, recurriendo a técnicas como el *data mining*, la explotación de las fuentes abiertas y las inversiones en inteligencia artificial.

Por otra parte, es necesario “mejorar la relación entre el analista y el órgano encargado de la recolección de información”. Esta mejora tiene una profunda base estructural. La inteligencia contemporánea, creada durante la guerra fría, partía de la estricta distinción entre captación y análisis. En un mundo sin Internet y sin bases de datos era incluso comprensible –sobre todo en los sistemas de mayor tamaño– la existencia de organizaciones específicas para cada una de estas tareas. Entonces, en el mejor de los casos, los recolectores obtenían información según las instrucciones de los analistas, cuando no se las inventaban según la facilidad que tuvieran para el acceso a

fuentes; la desconexión entre ambos mundos era así patente. A partir de ahora recae sobre el analista la responsabilidad de dirigir y orientar el trabajo del recolector y, evidentemente, también de hacer labores de captación, puesto que éstas ya no implican necesariamente estar sobre el terreno. Se impone un cambio en las políticas de reclutamiento y reciclaje que habrán de centrarse en buscar nuevas habilidades y competencias en los agentes.

Consecuentemente, también se están produciendo intensos y profundos cambios en las estructuras de los servicios de inteligencia. Internamente se está consolidando la división en tres ramas: administración, inteligencia y operaciones, que comenzó a surgir a mediados de la década de los noventa. Pero las innovaciones más llamativas e interesantes son los procesos de especialización. Cabe destacar el de los países nórdicos. En ellos, las policías siempre han albergado una pequeña estructura que generaba inteligencia contra el terrorismo, el crimen organizado y el tráfico de drogas, cubriéndose de esta forma la necesidad de inteligencia estratégica, al tiempo que se asegura una rápida comunicación de la inteligencia a la fuerza policial para llevar a cabo operaciones. Liderados por los suecos, se está estudiando la posibilidad de que la inteligencia cobre vida propia y se convierta en un servicio de inteligencia separado. No obstante, esta posibilidad no será muy factible. Vecinos como Estonia o Letonia –e incluso algo más distante como se plantea República Dominicana– también han optado por este tipo de agencias, lo que supone un refuerzo de este modelo y dificultará el cambio. Además, un país clave, EE UU, no ha logrado que el FBI deposite sus competencias en inteligencia en un servicio separado de esta policía federal.

Otra de las innovaciones estructurales se produce con la creación de centros antiterroristas específicos, extrayendo estas competencias de otras agencias con la misión de realizar análisis, asesoramientos y, algunos de estos centros, también operaciones contra el terrorismo internacional. Ejemplos de esta innovación son el National Counterterrorism Center (EE UU), el Joint Terrorism Analysis Centre (Reino Unido), los Joint Counterterrorism Intelligence Coordination Unit y National Threat Assessment Centre (Australia), el Integrated National Security Assessment Centre (Canadá), el Combined Threat Assessment Group (Nueva Zelanda) o el Centro Nacional de Coordinación Antiterrorista (España); si bien es difícil encontrar un Estado que no haya creado algún tipo de centro de análisis antiterrorista con funciones de fusión y coordinación, aunque carezca de responsabilidades operativas. Ésta era una de las recomendaciones de la comisión del 11-S que mayor predicamento ha tenido, no así la de crear una agencia especializada contra la proliferación de armas de destrucción masiva (ADM), solo existente en EE UU y en estudio en Reino Unido.

En tercer lugar, “el poder político debería indicar con claridad a los servicios cuáles son sus prioridades, considerando la posibilidad, probabilidad y peligrosidad de las amenazas”. Los ciclos de los acontecimientos y

crisis son hoy sustancialmente más cortos que en la última década. Esto requiere una mayor relación entre las agencias de inteligencia y los políticos. Las primeras necesitan saber cuáles son las necesidades de los decisores para poder suministrarles la inteligencia adecuada y tomar así decisiones con la frecuencia que requieren. Habitualmente esto se hacía a través de la fijación anual de objetivos, pero ahora el flujo debe ser forzosamente más intenso. La comisión delegada del gobierno para Asuntos de Inteligencia es la unidad sobre la que debería recaer en España este papel; algo que ejerce el Joint Intelligence Committee en Reino Unido, el Comité Ministériel du Renseignement et de la Sécurité en Bélgica o el Comité Interministériel du Renseignement en Francia.

Además de la asignación de objetivos y misiones, algunas de estas organizaciones se han convertido en centros de fusión de la pluralidad de informes para proporcionar un asesoramiento único al decisor político. Una obligada consecuencia de la generación de esta inteligencia más aplicable –y algo alejada de su tradicional dimensión estratégica– es la imprescindible necesidad de la evaluación de su uso, eficacia y utilidad por parte de los decisores para que, consecuentemente, ésta se pueda reorientar. Surafricanos, australianos y británicos ya están analizando de forma sistemática su eficacia a través de las valoraciones que los consumidores hacen de la inteligencia que reciben, indicando a los analistas cuál es el uso que se efectúa de la inteligencia y el formato más idóneo para recibirla. Es un camino al que tarde o temprano todos los servicios van a tener que incorporarse a riesgo de ser arrinconados y “puenteados” por los políticos. No olvidemos que, a diferencia de las últimas décadas, en la actualidad sí hay otras fuentes alternativas de las que beber en busca de información, y los consumidores de inteligencia se consideran capacitados para hacer sus propios análisis.

En cuarto lugar, “establecer mecanismos para solucionar la fatiga que puede producirse entre las alertas que emiten los servicios y las decisiones de los políticos para que este mecanismo no quede saturado”. La mayor frecuencia de las crisis y lo “multifacético” de las amenazas requiere la colaboración de los ciudadanos con el aparato de seguridad, suministrándoles información sobre aquello que les parezca inusual en su entorno. En un nivel restringido, el recurso al ciudadano se hace a través de las conocidas “reservas de inteligencia”. Debido a que el servicio no puede abarcar todas las fuentes de riesgo ni albergar en su seno todos los conocimientos necesarios, se configuran estas reservas compuestas por académicos, periodistas, empresarios, misioneros... a quienes es preciso tener localizados y en contacto con el servicio de inteligencia, suponiendo un nuevo reto, del que al-

---

*La creación de centros específicos antiterroristas ha sido la innovación más extendida tras el 11-S*

guien en el servicio deberá hacerse cargo volviendo a un argumento previo: la necesidad de desarrollar perfiles diferentes entre el personal.

En un nivel más general, a los ciudadanos se les ha implicado directamente en este combate de diferentes formas. Por una parte, haciéndoles partícipes de informes de inteligencia más o menos politizados para recabar su apoyo para una guerra, algo no nuevo pero sí olvidado. Por otra, a través de los códigos de colores que alertan del riesgo de acciones terroristas y que, en esencia, muestran a los ciudadanos el grado de inseguridad. En España se está desarrollando uno en la presidencia del gobierno, y la Unión Europea se plantea establecerlo en breve. Sin embargo, este sencillo e intuitivo código de colores puede ser utilizado para manipular y asustar al ciudadano con una finalidad política o electoral como filtraciones desde la Casa Blanca han demostrado, con lo que su utilidad decae drásticamente.

El 11-S nos debería enseñar la lección de que las sociedades siempre están amenazadas, por esto es una prioridad “vigilar nuevos campos que hasta ahora pasaban desapercibidos”. Un vistazo al último siglo muestra cómo las amenazas cada vez mutan más rápidamente, son más silenciosas y se presentan más destructivas cuando se materializan. Esto va a suponer que parte del trabajo de las agencias de inteligencia se dirija hacia algo tan evidente como incrementar su labor prospectiva escrutando emergentes fuentes de riesgo y desactivándolas en sus estadios iniciales. Estas amenazas son lo que el secretario de Defensa de EE UU, Donald Rumsfeld, ha denominado los *unknowns unknowns*, es decir, aquellas amenazas que aún no se han convertido en tales, pero que pueden serlo en algún momento. Aunque la necesidad de dedicarles recursos para conocerlas y combatirlas es fácil de argumentar teóricamente, para los políticos no es tan sencillo justificarlas con unos recursos siempre escasos y cuando los ciudadanos ven que las amenazas reales, y no potenciales, se materializan en sus ciudades.

En caso de no abordar este cambio en la forma de trabajar, nos encontraremos en el futuro con escenarios muy complejos y con enemigos simultáneos que coexistirán, y no como hasta ahora donde simplemente un nuevo enemigo surgía cuando otro perdía su lugar. En su punto extremo, una concepción desmesurada del papel de la inteligencia nos lleva a la guerra preventiva (*pre-emptive war*) recogida en la Doctrina de Seguridad Nacional de EE UU. Pero de igual forma que las acciones encubiertas son consideradas por la doctrina estadounidense como un último recurso cuando falla la política exterior, en este escenario tan complejo, tampoco podemos cargar a la inteligencia con misiones que son policiales, de cooperación internacional para el desarrollo o simplemente de mediación social entre minorías étnicas o religiosas.

Finalmente, “mejorar la coordinación y colaboración con el resto de la administración del Estado”, lo que necesariamente pasa por desarrollar la comunidad de inteligencia. La idea de comunidad se gestó en 1947 cuando

se creó el sistema de inteligencia norteamericano. Sin embargo, prácticamente ningún Estado la ha desarrollado. Por esto es una expresión manida y un deseo, más que una realidad. Aunque no se ha logrado plasmar, debemos comprender que su filosofía y verdadera naturaleza se basaban en tener controladas a las organizaciones y en custodiar la información más que en distribuirla.

Los países latinoamericanos, que reformaron sus servicios de inteligencia en los últimos años, establecen unos denominados “sistemas de inteligencia” que, lejos de suponer la verdadera configuración de la comunidad de inteligencia, representan poco más que una carcasa política. Posiblemente estemos ante una copia literal del sistema norteamericano, o incluso del portugués. Sin embargo, en una dinámica diferente, los países de Europa del Este que también han adoptado este modelo en sus reformas tras los procesos de democratización, tampoco han dado mejores resultados, lo que muestra el largo camino por recorrer.

Partimos, por tanto, casi de cero para configurar esta necesaria comunidad de inteligencia. En primer lugar, será necesario comprender que, sin la colaboración de todos los sectores de la administración, unos miles de espías no pueden por sí solos afrontar las nuevas amenazas. Uno de los debates tradicionales era si la comunidad debía estar coordinada por una organización de inteligencia o por un político.

El patrón que está triunfando es que sea un político o una comisión quien se ocupe de congregar a las distintas organizaciones que tienen algo que decir en el asunto de la seguridad, y que va desde el propio servicio de inteligencia, al de aduanas o al servicio exterior. Estos órganos asignarán objetivos y distribuirán recursos teniendo en cuenta la aportación específica de cada organización, lo que implicará que la comunidad de inteligencia genere un producto sustancialmente diferente al del mero agregado de las agencias que la componen. Asimismo, será necesario que la información no quede cautiva, sino que todas las agencias puedan disponer de ella cuándo y cómo lo consideren oportuno y no solo cuando quien la posee decida o crea que alguien la puede necesitar. En esta nueva forma de concebir el trabajo en equipo, las nuevas tecnologías de la información van a ser esenciales, como la red Intelink norteamericana o la Scope británica que permiten un consumo de inteligencia mucho más racional.

La segunda adaptación de la inteligencia reside en el plano exterior. En *El Príncipe*, Maquiavelo sostenía que quien tenía buenas armas y buenos amigos podía garantizarse su seguridad hacia el exterior, y quien contaba con lo primero generalmente también se aseguraba lo segundo. Quizá ha-

---

*El trabajo en  
equipo y la  
cooperación con  
otros países son  
bases de la nueva  
inteligencia*

bría que revisar el pensamiento del florentino y concluir que, a partir de ahora, la relación sea más “sinalagmática”, y buena información y buenos amigos establecerán una relación circular.

La cooperación es, así, un instrumento clave y se configura, no ya como un aditamento más de los mecanismos de seguridad, sino como un instrumento con carta de naturaleza propia. Como indicaba en 2001, los Estados deben ser conscientes de que parte de su seguridad recae en otros países. Pero con matices. Los fallos de estimación sobre la posesión de ADM por parte del régimen de Sadam Husein se debieron, según las comisiones alemana, estadounidense, británica o israelí, a marcos de análisis anticuados y a la politización de la inteligencia para justificar unas determinadas decisiones, pero también a la carencia de fuentes diversas en las que justificar un análisis adecuado, si éste hubiera sido el deseo de los gobiernos implicados.

La cooperación en inteligencia siempre ha existido con marcos más o menos formales, como el Grupo de Trevi o el Ukusa, aunque, sin duda, ha sido en la cooperación bilateral sobre la que se ha construido este nuevo instrumento. Ha permitido el incremento de las relaciones de confianza y cimentado un interesante proceso de ósmosis desconocido hasta ahora. Desde instancias internacionales como las Naciones Unidas o la UE, se han adoptado decisiones y medidas que han uniformado las prácticas de los Estados. De igual modo que el modelo de la guerra fría solo era sostenido por unas cuantas potencias, al nuevo modelo le ocurrirá lo mismo, ya que no todos los países tienen igual poder ni las mismas necesidades de inteligencia. Por esto se configurará un núcleo central de potencias y, en un largo *continuum*, los demás países, que beberán en diferente medida de los postulados y opciones que tomen los grandes Estados.

En nuestro entorno, con independencia de las especiales relaciones que todos quieren mantener con EE UU, este núcleo central lo integrarán los países del G-6: Reino Unido, Francia, Alemania, Italia, España y Polonia. Estas prácticas permiten que la colaboración se active con celeridad, como sucedió tras los atentados de 7 de julio de 2005, cuando equipos españoles acudieron a Londres para ayudar a la policía y a la inteligencia británicas y se pudo rastrear a uno de los terroristas en su huida hasta Italia.

Huelga mencionar que la estricta distinción entre seguridad interior y exterior se ha difuminado; motivo por el que se producirá una clara especialización de países por zonas y asuntos. Pero este difuminado escenario tendrá importantes implicaciones sobre las organizaciones existentes. Los servicios de inteligencia exterior –en aquellos Estados que disponen de ellos– están perdiendo algo de peso e influencia, pues no son como antaño el exclusivo canal de comunicación de ese país con las organizaciones de otros países. Además, la confianza en las capacidades tecnológicas ocasionó en muchos países el repliegue de las redes humanas y, sobre todo, no permitió actualizarlo según las nuevas zonas de interés. Es por ello necesario recupe-

rar el posicionamiento sobre el terreno ya que, en la actualidad, no más del 20 por cien de los efectivos de los servicios está en el exterior, desempeñando el resto funciones de análisis.

### **Una agenda de retos**

Con algunas variaciones debidas a situaciones y fenómenos nacionales concretos, las características que configurarán el nuevo modelo de inteligencia en, al menos, la primera mitad de siglo serán las siguientes. Un modelo basado en hacer la inteligencia más operativa, más fluida, más preventiva y más apta para gestionar las situaciones de crisis que desgraciadamente se producirán. En esencia, se trata de un modelo iluminado bajo los principios de especialización, colaboración y dirección. Un modelo para cuya configuración son imprescindibles inversiones económicas, la entrega a los servicios de nuevos instrumentos legales, la clara separación de las funciones policiales de las de inteligencia y la suficiente flexibilidad para la incorporación de nuevas técnicas de organización, gestión y análisis.

Para concluir, es imprescindible avanzar en algunos riesgos potenciales que se están corriendo. Descuidar cualquiera de los elementos apuntados para hacer avanzar el modelo sería uno de estos riesgos, pero quizá el más preocupante sea la focalización de los esfuerzos y recursos en el contraterrorismo, dejando de lado una más silenciosa amenaza como es el crimen organizado. El informe de la UE de mayo de 2000 sobre el crimen organizado ya alertaba sobre esta amenaza y de su capacidad para pudrir las instituciones del Estado. Por su parte, el informe de 2002-03 del comité parlamentario de los servicios de inteligencia británicos avisaba de que esta monopolización de recursos supone un “riesgo inaceptable para la seguridad nacional”. Y este aviso no es una mera elucubración. Repasando los informes de actividad de los servicios de inteligencia y de sus comités de control, de al menos una veintena de países, se observa que el terrorismo internacional centra en la actualidad alrededor del 60 por cien de su actividad y otras amenazas como el crimen organizado no llegan al cinco por cien, en el mejor de los casos. No sería agradable que, en una o dos décadas, cuando tengamos bajo control la amenaza terrorista, nos encontremos con que las instituciones que pretendíamos defender están putrefactas.

El segundo gran reto es el control. Ya hemos comprobado el potencial de la inteligencia para penetrar en la esfera íntima del ciudadano y qué sucede cuando además se dispone de mecanismos tecnológicos. El informe de Statewatch de marzo de 2004 analiza las medidas antiterroristas adoptadas en la cumbre extraordinaria de la UE de ese mismo mes y concluye que solo 27 de las 57 medidas diseñadas están directamente relacionadas con el contraterrorismo. Por otra parte, Cortes Constitucionales de distintos Estados

han declarado la inconstitucionalidad de diversas leyes que expandían los poderes de los servicios de inteligencia a niveles no adecuados, al autorizar medidas como el almacenamiento ilimitado de datos, el control biométrico de viajeros o la vigilancia sobre zonas y no sobre domicilios concretos e incluso el uso judicial de informaciones de inteligencia sin desvelar la fuente ni respetar el principio de contradicción.

Uno de los mayores dislates encontrados –fruto del 11-S– está en el artículo 8 de la ley del Valstybės Saugumo Departamentos, el servicio de inteligencia lituano; allí se establece que “se emitirá una advertencia oficial cuando exista suficiente base para creer, según la información obtenida, que aquella persona puede cometer infracciones que vayan en detrimento de la seguridad del Estado”; esto es, un empleo coercitivo de la inteligencia hasta ahora reservado solo a la policía.

Si alguna lección tendríamos que haber aprendido de la guerra fría debería ser la de no garantizar la seguridad pisoteando los derechos y las libertades ciudadanas. Fueron los Parlamentos nacionales quienes, en aras de la inmediata utilidad política, permitieron un uso abusivo de la cláusula de seguridad nacional; algo que no restringieron hasta que a finales de los años setenta vieron cómo sus servicios de inteligencia cobraban vida propia y controlaban incluso a la propia élite política al sospechar de su lealtad, un papel autónomo de la inteligencia que ahora vuelve a recrearse por las intensas demandas de inteligencia a la carta que, a cualquier coste, están realizando los políticos.

Pero nos queda una segunda lección. La insuficiencia de confiar en la potente capacidad de reacción del aparato del Estado y lo equivocado de eludir el combate de nuestras amenazas cuando éstas aún se encuentran en su momento embrionario. Sin duda, nuestra seguridad no tendrá otra posible articulación que reposar en las estrategias de prevención.