GESTIÓN DE LA SEGURIDAD EN ATENTADOS TERRORISTAS DE GRAN ENVERGADURA

ANDRÉS MONTERO GÓMEZ

Consultor en Inteligencia de Seguridad. Profesor de Seguridad de la UNED

JORGE ZURITA BAYONA

Comisario del Cuerpo Nacional de Policía. Jefe de Área del Gabinete de Estudios de Seguridad Interior. Secretaría de Estado de Seguridad

Los atentados de gran envergadura generan la necesidad de diseñar esquemas públicos de coordinación multidisciplinar de prevención y respuesta de gran complejidad. A partir de los atentados de las Torres Gemelas empiezan a crearse organismos y a establecer políticas que de una forma u otra tienen por objeto articular un sistema de actuación multidimensional para hacer frente a las crisis que originan este tipo de atentados.

Los autores explican en detalle la secuencia de lo que denominan la gestión contínua del riesgo (prevención mitigación, preparación, respuesta y recuperación) para finalmente explicar cuál fue la intervención —improvisada por falta de protocolos de actuación y planes estructurados en aquel momento— en el atentado terrorista del 11 de marzo de 2004 en Madrid.

Terrorist attacks of mass destruction generate the need to design public schemes of multidiscipline coordination for prevention and highly complex responses. Since the terrorist attacks to the Twin Towers of New York, new organizations are being created and public policies are being established in order to somehow articulate a multidimensional action system to cope with the crisis caused after these kind of terrorist attacks.

The authors explain in detail the sequence of what they call «continuous risk management» (prevention, mitigation, preparation, response and recovery) and finally they explain which was the intervention —improvised due to the lack of protocols and structural planning— during the terrorist attack of March 11th, 2004 in Madrid.

1. INTRODUCCIÓN

El denominado «terrorismo yihadista» ha puesto en primer plano las necesidades a las que debería responder la seguridad pública desde una concepción multidimensional. Entre estos planes de necesidades reorientadas, el poliedro de la nueva seguridad, que pretende no sólo adaptarse sino anticiparse al terrorismo yihadista, ha revitalizado el concepto de seguridad preventiva, pero también ha introducido condicionantes a los procesos investigativos de las fuerzas de seguridad; ha obligado a priorizar labores de obtención y procesamiento de inteligencia; ha hecho visible la coordinación, la integración y la fusión de esfuerzos y de información como una de las piezas clave de la nueva seguridad antiterrorista; y, entre

otras, nos ha dirigido a replantear la gestión de la seguridad ante desastres y emergencias provocadas por atentados terroristas de gran envergadura.

En efecto, aunque tanto en España con la actividad terrorista de ETA, como en el Reino Unido con el IRA, en Israel con una serie de grupos terroristas antisemitas o en los propios Estados Unidos con atentados como el perpetrado en Oklahoma en 1995 y atribuido a milicias antisistema, ya había experiencia en la gestión de atentados terroristas en masa, con elevado número de víctimas afectadas entre la población, no es hasta el 11 de septiembre de 2001 con la cadena de atentados en EEUU cuando comienza a imponerse una concepción sistematizada de la emergencia terrorista como capítulo especializado, y sobre todo, interconectado e integrado de la seguridad pública. Y que, si bien la experiencia en la gestión de este tipo de incidentes ya existía, primero el 11-S en Nueva York pero después el 11-M en Madrid o el 7-J en Londres consiguen, más que ningún otro fenómeno anterior, dotar a nuestra concepción de la seguridad de los principios de integración multidisciplinar, de coordinación multiagencia con propósitos de respuesta integrada y de capacidades preventivas. Si algo nos enseña las actuaciones de las administraciones públicas ante el recorrido internacional de grandes atentados terroristas en masa de la última década es:

— que la respuesta ante una emergencia debe integrar los esfuerzos y las capacidades especializadas y dispares de una multiplicidad de agencias y órganos públicos y privados (bomberos, emergencias sanitarias, los distintos cuerpos policiales, jueces, responsables de transporte, ingenieros), así como de competencias sectoriales y territoriales;
— que esa respuesta debe tener tal grado de preparación y entrenamiento entre esos componentes dispares que, en el momento de ejecutarse, se convierta en una respuesta unitaria en su muldimensionalidad de manera que sea un solo órgano compuesto por múltiples piezas el que responda ante la emergencia, y no varios componentes descoordinados los que ofrezcan varias respuestas disfuncionales entre sí;
— y que la *autoridad de coordinación* debe funcionar en red, en modo paralelo y distribuido, dirigida por un centro de mando y control a su vez conectado con nodos funcionales en cada una de las dimensiones de la crisis, que sean capaces de transmitir las órdenes de actuación especializada en cada caso, momento y fase de gestión de la incidente crítico pero de forma que la suma de respuestas de cada nodo componga una integración global de la respuesta a nivel central.

La coordinación de esfuerzos en la respuesta compone un puzzle complejo en el diseño de esquemas públicos de coordinación ante atentados terroristas de gran envergadura. En primera instancia, esos esquemas de coordinación deben tener carácter estable en su planificación pero ser coyunturales en su aplicación y ejecución. Es decir, los distintos componentes de un esquema de respuesta ante grandes atentados terroristas en masa deberían tener una función asignada, haber entrenado su función específica y haberlo hecho en simulaciones coordinadas con

el resto de actores a intervenir en una eventual emergencia, pero realmente esa preparación no se convertirá en acción sobre el terreno hasta que se produzca un atentado terrorista. La creación en los EEUU de la *Federal Emergency Management Agency* (FEMA - Agencia Federal de Gestión de Emergencias) como órgano especializado del Departamento de Seguridad Interior (Homeland Security) es una aproximación a estos esquemas complejos. En segundo plano, deben adaptarse a una respuesta local, pero deben integrar todas las capacidades y competencias de lo regional y lo nacional, incluso canalizando soporte internacional en muchos de los escenarios. De este modo, la respuesta ante atentados terroristas de envergadura incorpora operacionalmente uno de los axiomas ligados a la globalización, descrito en la frase «*piensa globalmente y actúa localmente*».

2. PRINCIPIOS EN LA GESTIÓN DE CRISIS

Desde hace al menos casi tres décadas, la gestión de emergencias venía siendo un concepto que respondía a una realidad bajo la responsabilidad de los distintos servicios de protección civil de las administraciones públicas, principalmente a escala local o regional. Las crisis provocadas por situaciones de emergencias tienen en común pertenecer a la *discontinuidad* entre períodos de normalidad. A nuestros efectos, una emergencia generalmente está referida a una perturbación, en una o varias dimensiones, de la estructura social que amenaza a uno o varios de sus valores o elementos de sustentación y equilibrio (el bienestar, la salud, el aprovisionamiento, la comunicación, la economía) de la ciudadanía.

En la moderna aproximación a las emergencias y desde un plano teórico no es tan importante que una amenaza vaya a materializarse contra esos elementos de sustentación social mencionados, como el hecho de que los poderes públicos estén en condiciones de garantizar, sino que se va a poder anticipar, sí al menos que la continuidad de esos valores va a ser protegida y, caso de ser dañada, va a ser reestablecida.[1]

2.1 DE LA PROTECCIÓN CIVIL A LA SEGURIDAD CIUDADANA

Tradicionalmente, las emergencias que amenazaban la discontinuidad de los elementos de sustentación de la infraestructura social han venido definidas por desastres naturales, incendios, inundaciones, terremotos. Las emergencias derivadas de problemas medioambientales son más recientes, en cuanto a nuestra identificación como amenazas, que las ligadas a epidemias o detonantes de crisis de salud pública, que han estado presentes a lo largo de la historia de la humanidad.

Otro tipo de crisis que originan varios niveles de emergencia son las económicas o financieras que, comenzando por la más ancestral y bursátil de 1929 y con-

1. Rosenthal, U.; Boin, R.A.; Comfort, L.K. (eds.). *Managing Crises: Threats Dilemmas, Opportunities*. Springfield: Charles C Thomas, 2001.

tinuando por las petroleras de los años setenta o las financieras de los noventa, han trasladado hacia otros ámbitos los modos propios de las emergencias más medioambientales o de salud. El concepto de emergencia ha venido estando muy asociado a la respuesta, a la capacidad de respuesta y a la posesión de esa capacidad por los poderes públicos revestidos con la responsabilidad, y por tanto con la legitimidad, de garantizar esa *continuidad* de los pilares de sustentación social.

Sin embargo, el concepto de protección civil ante emergencias no surge del afrontamiento de amenazas naturales o medioambientales, y mucho menos de la respuesta ante crisis epidemiológicas o económicas, sino de la necesidad de salvaguardar unas mínimas condiciones para la población civil en escenarios de enfrentamiento armado ode conflicto bélico.

Desde el principio básico de salvaguardar la vida de las personas, sus bienes y su entorno, el 12 de agosto de 1949 un protocolo adicional a la Convención de Ginebra instituye la protección a las víctimas de conflictos armados internacionales y define a toda una serie de acciones destinadas a sustanciar aquel principio básico (servicios de alarma o evacuación, servicios sanitarios, de salvamento, de lucha contra incendios, de descontaminación, de alojamiento y abastecimiento de urgencia, hasta llegar a la preservación de los bienes esenciales para la supervivencia o a los servicios funerarios) como propias de los servicios de protección civil. A partir de ahí, los distintos desarrollos de la protección civil, centrados en los Estados, evolucionaron para cubrir un abanico cada vez más amplio de riesgos y de emergencias generadas por la presencia de amenazas hasta llegar a asumir la idea de un servicio, siguiendo a la legislación española, destinado «a la protección física de las personas y de los bienes, en situación de grave riesgo colectivo, calamidad pública o catástrofe extraordinaria, en la que la seguridad y la vida de las personas pueden peligrar y sucumbir masivamente» para lo que «la protección civil constituye la afirmación de una amplia política de seguridad, que encuentra actualmente su fundamento jurídico, dentro de la Constitución, en la obligación de los poderes públicos de garantizar el derecho a la vida y a la integridad física, como primero y más importante de todos los derechos fundamentales».[2]

Si bien en muchas de las emergencias de corte medioambiental, o provenientes de desastres naturales, la participación de las fuerzas de seguridad, incluso de las fuerzas militares, ha venido siendo una constante, la propia conceptuación de la emergencia como discontinuación de los servicios esenciales, dotaba a la respuesta ante ella de ese carácter de protección civil. En raras ocasiones una emergencia pública era considerada un problema principalmente de seguridad, aún cuando en numerosos de los esquemas de respuesta la garantización del orden público por parte de las fuerzas policiales fuera una componente a integrar y coordinar con el resto de servicios por parte de las administraciones, incluso una condición sin la cual esos servicios no podían ser garantizados. El concepto de protección civil continuaba primando y continúa haciéndolo en las crisis derivadas de emergencias medioambientales, catástrofes naturales o de las denominadas

2. Ley 2/85, de 21 de enero, sobre Protección Civil.

«humanitarias». La emergencia del terrorismo internacional a través de atentados de gran envergadura abre una nueva conceptuación de la emergencia entendida como manifestación de un incidente crítico.

Desde un punto de vista del perjuicio a la población civil y a los elementos de sustentación de las infraestructuras sociales, un atentado terrorista de gran envergadura no es distinto en cuanto a los elementos de respuesta a demandar que una emergencia desencadenada, por ejemplo, por un terremoto o una gran inundación. En todos los supuestos, las administraciones públicas deberían ser capaces de proveer los medios para atajar incendios, explosiones, destrozos en viviendas, en líneas de transporte y conducción de comunicaciones, así como preparar la intervención con víctimas heridas o fallecidas por el desastre. Sin embargo, entre una inundación, un incendio, un terremoto o un atentado terrorista, si los suponemos a todos con víctimas mortales, ninguno de ellos salvo el último sería percibido (y por tanto su respuesta diseñada) como un problema de seguridad.

La alineación de recursos ante emergencias en torno a servicios de protección civil, cuando son producto de desastres naturales, tiene la misma lógica que hacer pivotar esos mismos recursos alrededor del sistema sanitario cuando se desencadena una crisis epidemiológica o del sistema de seguridad cuando nos encontramos con el riesgo de un atentado terrorista. Esta última amenaza difiere en su cualificación respecto de las otras desencadenantes de emergencias objeto de la protección civil, al menos, en tres elementos: se trata de ataques deliberados, suponen un ejercicio coactivo sobre la libertad individual, y los atentados constituyen un acto inscrito en un continuo de conducta, que es además un comportamiento criminal.

La circunstancia de que los atentados terroristas sean ataques deliberados contra la libertad individual, realizados desde un continuo criminal cuya última finalidad es subvertir principios de la convivencia democrática y del Estado de Derecho, los convierten en problemas netos de seguridad.

Por otro lado, el hecho de que los grandes atentados terroristas en masa involucren, además de la pérdida de vidas humanas, la interrupción de los servicios críticos para el normal desenvolvimiento de la convivencia social o incluso estén dirigidos, caso de los atentados contra infraestructuras críticas, a deshabilitarlos, configura ese problema de seguridad como un estado de desorden civil cuya resolución requiere afrontamientos integrales que incorporen a todos los actores que deben estar involucrados en la protección de la población y en la restitución de los servicios esenciales, con una conciencia de provisión de servicios para *reestablecer la seguridad de la ciudadanía*.

Por último, un aspecto que a veces se pasa por alto en la doctrina sobre intervención ante incidentes terroristas críticos: un atentado inmediatamente define la *escena de un crimen*, escena cuya preservación e inspección es responsabilidad policial y cuya jurisdicción recae en la autoridad judicial competente en conocerla. Esta particularidad condicionará, sobre todo, la cadena de mando y dirección de las acciones de primera respuesta.

Aunque a partir del último tercio del siglo XX los atentados terroristas de gran envergadura han estado presentes en ciudades europeas y de otras partes del

mundo, la conciencia de que son necesarios sistemas públicos *estables* de preparación y respuesta para la seguridad ante atentados terroristas llega el día después del 11 de septiembre de 2001. De aquella emergencia provocada por ataques terroristas en los EEUU queda la concienciación de la opinión pública internacional sobre la necesidad de disponer de *sistemas integrados de prevención y respuesta* que, si no pueden evitar los efectos, por lo menos salvaguarden la continuidad de la vida social y reparen con la prontitud que sea posible las consecuencias sobre la población de las acciones criminales. Sin disponer de los protocolos integrados de respuesta de los que después se han dotado (la respuesta a los atentados fue *necessarily improvised)*,[3] los servicios de emergencia, protección civil y seguridad de la ciudad de Nueva York respondieron con relativa eficacia al reto de contener el riesgo, atender a la población, restituir servicios esenciales, reparar lo que fuera recuperable de bienes materiales y establecer programas de acompañamiento e indemnización para las víctimas.

En la Unión Europea, esa conciencia de necesidad de disponer de *esquemas integrados de prevención, preparación y respuesta* llega a raíz de otro atentado terrorista en masa, el producido en Madrid el 11 de marzo de 2004. Después de que el 25 de marzo de 2004 el Consejo de la Unión hiciera pública una Declaración para Combatir el Terrorismo,[4] en lo que respecta a la gestión de emergencias derivadas de atentados, en octubre de ese mismo año la Comisión Europea emite una comunicación al Consejo y al Parlamento Europeos sobre prevención, preparación y respuesta a atentados terroristas, estableciendo las líneas maestras de una política europea en esa dirección pero, más importante, enmarcando ya desde su mismo título la estructura secuencial (prevención, preparación y respuesta) con la que debe andamiarse un sistema público ante atentados de gran envergadura.[5]

A pesar de que es difícil distinguir en la argumentación de la Comisión Europea si son los atentados terroristas los que representan una amenaza que desencadena una emergencia o si es el terrorismo como fenómeno el que resulta como motor causal de ese riesgo,[6] lo que sí deja patente en todo caso es que los sistemas de los Estados miembros deberían ser integrados por todos los actores necesarios, y constituirse con base comunitaria (local) a partir de un diálogo, de una colaboración, entre lo público y lo privado. Esta comunicación de la Comisión Europea iría seguida, en 2007, por una Decisión del Consejo instituyendo un programa de cinco años para apoyar los esfuerzos de los Estados miembros en la prevención, prepa-

3. National Commission on Terrorist attacks upon the United States (2004). The 9/11 Commission Report. New York: Norton and Co.

4. Declaración que recoge en un anexo un plan de acción revisado de siete puntos de Estrategia Europea para Combatir el Terrorismo cuyo quinto objetivo está destinado a «aumentar la capacidad de la Unión Europea y de sus Estados Miembros para gestionar las consecuencias de un atentado terrorista».

5. Commission of the European Communities. *Communication to the Council and the European Parliament on the Prevention, Preparedness and Response to Terrorist Attacks*. COM(2004) 698 final.

6. Por ejemplo, en una comunicación dirigida a la preparación ante atentados terroristas se incluye un capítulo dedicado a prevención del radicalismo en Europa, más propio de una comunicación sobre prevención del terrorismo como fenómeno.

ración, respuesta y gestión ante las consecuencias del terrorismo,[7] una prioridad ya destacada por el Plan de Acción de la Unión Europea contra el Terrorismo de junio de 2004.

Actualmente, y en general, las orientaciones hacia la gestión de emergencias han trascendido el tradicional enfoque centrado en una respuesta rápida derivado del carácter «emergente» y en cierto modo inevitable de la amenaza, para entender la emergencia como un proceso longitudinal con un «antes» que puede ofrecernos señales de alerta temprana, un «durante» que hay que gestionar hacia la recuperación de la normalidad, y un «después» enfocado en la restauración, la reparación y la detección y erradicación de futuras vulnerabilidades.

En realidad, la gestión de emergencias es hoy una variante de la gestión y evitación del riesgo[8] que conceptualmente comparte espacio doctrinal con lo que se ha venido denominando *reducción o gestión del riesgo de desastres*, entendido como «el marco conceptual relacionado con las posibilidades de minimizar las vulnerabilidades y los riesgos de un desastre en la sociedad, en orden a evitar (prevención) o limitar (mitigación y preparación) el impacto adverso de las amenazas, todo en el amplio contexto del desarrollo sostenible».[9]

2.2 LA GESTIÓN DEL CONTINUO DEL RIESGO

Desde una óptica de gestión de la seguridad, la experiencia en el manejo de emergencias relacionadas con grandes atentados terroristas en masa sugiere distinguir varios planos de realidad para conformar un esquema efectivo de gestión de la seguridad (fig. 1). En primera instancia, la gestión de la seguridad ante un atentado incorpora dos vertientes de respuesta, una ante la crisis estructural e infraestructural que provoca el incidente y otra ante las consecuencias derivadas de la aparición de esa crisis.

Internacionalmente existen varios modelos de respuesta, que pueden resumirse en dos: o bien se establece una estructura institucional específica, que luego aplicará planes operativos de gestión de emergencias, o bien se diseña un protocolo marco de actuación en donde se fija la responsabilidad de cada agencia o institución en la gestión de un incidente crítico terrorista cuando se desencadena.

En la organización institucional federal de los EEUU tras los atentados del 11-S, por ejemplo, la coordinación interagencia para cada uno de estos dos segmentos de respuestas corresponde a dos órganos distintos, la Agencia Federal de Investigaciones (FBI) del Departamento de Justicia para comandar la gestión del incidente crítico y la Agencia Federal de Gestión de Emergencia (FEMA), del

7. Decisión del Consejo de 12 de febrero de 2007 por la que se establece para el período 2007-2013 el programa específico «Prevención, preparación y gestión de las consecuencias del terrorismo y de otros riesgos en materia de seguridad», integrado en el programa general «Seguridad y defensa de las libertades»

8. Haddow, George D.; Jane A. Bullock (2004). *Introduction to Emergency Management*. Amsterdam: Butterworth-Heinemann

9. United Nations Inter-Agency Secretariat of the International Strategy for Disaster Reduction (2004). L*iving With Risk: A Global Review of Disaster Reduction Initiatives*. Ginebra: UNISDR

Departamento de Seguridad Interior, para coordinar la gestión de las consecuencias de las crisis.

De otro lado, en Francia, no existe un mandato institucional específico para cada una de esas fases pero sí un planeamiento general, un modelo de actuación operativa (Organisation de la Réponse de Securité Civile-ORSEC)[10] que marca quién tiene que intervenir y cuándo en una emergencia, poniendo las actuaciones bajo la coordinación general de prefecto local.

En todo caso, continuando con los planes de gestión en el «antes» (prevención) y el «durante» (detonación del incidente crítico) de la emergencia, en un atentado terrorista la gestión es una función de seguridad predominantemente policial que incluye medidas para identificar, adquirir y planificar la utilización de los recursos necesarios para anticipar, prevenir y/o resolver una amenaza o un acto terrorista. Ante un incidente terrorista, la respuesta policial de gestión de incidentes críticos puede incluir funciones tradicionalmente policiales como la vigilancia, las operaciones tácticas, la negociación, la actividad forense o la investigación, así como funciones de apoyo técnico de identificación, aseguramiento de personas o materiales, gestión del transporte o traslado de restos, o descontaminación de áreas. En paralelo, la respuesta de seguridad ante la crisis incorpora elementos de salud pública y protección civil integrados en la acción policial.

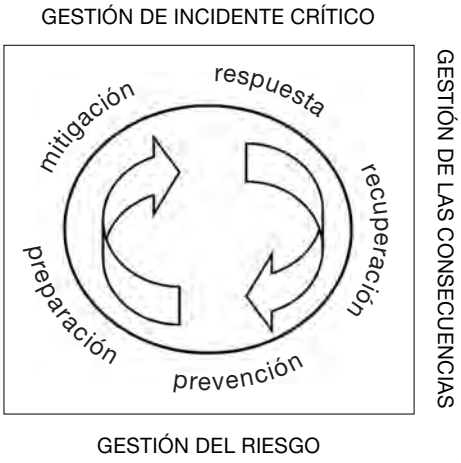
Por su parte, la gestión de las consecuencias de la crisis (el «después») tiene que ver con las medidas para proteger la salud y el bienestar de la ciudadanía, con la restauración de servicios esenciales y con el aporte de cuidados y reparaciones a las personas, colectivos, instituciones y empresas afectados por las consecuencias del atentado. En ese sentido, la gestión del riesgo y del incidente crítico caería conceptualmente bajo las responsabilidades de los aparatos públicos de seguridad, mientras la gestión de las consecuencias, la recuperación de la normalidad excluidas las evidentes labores de investigación policial a que se diera lugar, entraría más en el campo de los servicios de protección civil, sociales y sanitarios.

Por otra parte, en la gestión de emergencias es imprescindible la adecuada preparación (*preparedness*) de los actores involucrados para desarrollar esa respuesta cuando sea necesario. Una de las lecciones aprendidas extraíble de la respuesta ante los atentados terroristas del 11-S ha sido que no es suficiente disponer de oficinas públicas para la coordinación de emergencias, sino que esas oficinas tienen que funcionar con poder ejecutivo y con mandatos de integración de esfuerzos, y que todos los actores que coordina deben haber simulado y entrenado sus misiones operativas hasta haberlas interiorizado lo suficiente: *emergency response is a product of preparedness* (la respuesta a una emergencia es en función de su preparación).[11]

10. Direction de la Défense et de la Sécurité Civiles (2004). *Guide ORSEC Départemental. Méthode Général.* Ministere de L'Interieur et de L'Amenagement du Territoire.

11. Tal como refleja el informe de la Comisión del 11-S, el alcalde de Nueva York Rudolph Giuliani había creado ya en 1996 la Office of Emergency Management and Interagency Preparedness. Esa oficina, que debía de haber servido como centro de operaciones para la ciudad en la emergencia del 11-S no fue capaz de controlar ni de coordinar a los servicios de la policía de Nueva York (NYPD) ni a los bomberos (NYFD), dos de las agencias que más participaron en el esfuerzo de contención del riesgo y recuperación y que, según el dictamen de la Comisión del 11-S, funcionaron de forma completamente autónoma.

Figura 1. *Esquema de gestión de la seguridad*



Como ya hemos apuntado, en un atentado terrorista la gestión de la crisis comienza antes de que la propia amenaza se materialice, incluso antes de que la amenaza esté en condiciones de suponer un riesgo cierto. Esa, más o menos reciente, filosofía de la anticipación en seguridad es en buena parte responsable de que la gestión de las emergencias esté evolucionando hacia una gestión del continuo del riesgo.

Así las cosas, en la secuencia de operaciones ante un atentado terrorista de gran envergadura pueden distinguirse varias fases:

2.2.1 Prevención

La necesidad de anticipar lo que pueda ocurrir antes de que ocurra se está dando en casi todas las crisis desatadas por agentes medioambientales (terremotos, inundaciones), pero es imprescindible en la gestión del riesgo en incidentes críticos por atentados terroristas. Únicamente en el espacio común europeo y financiados por fondos comunitarios existen al menos cuatro programas[12] de investigación destinados a dotar a los Estados de capacidades para prevenir la traducción de amenazas a incidentes críticos, principalmente causados, aunque no sólo, por atentados terroristas.

12. En concreto, el programa VITA (Vital Infrastructures Threats and Assurance), dedicado a anticipar riesgos desastres naturales sobre infraestructuras críticas, que incluye además el desarrollo de capacidades de simulación de consecuencias; el programa ROBIN, concentrado en prevenir ataques deliberados contra infraestructuras críticas de información y comunicación; el programa ORCHESTRA, una arquitectura georreferenciada para crear una malla interoperable entre autoridades de gestión de emergencias en Europa, enfocada sobre todo en la gestión operativa de los incidentes críticos; y el programa TRIPS (Transport Infrastructures Protection System), destinado a producir modelos de gestión del riesgo específico de ataques terroristas a infraestructuras críticas de transportes por medio del estudio amenazas, vulnerabilidades y consecuencias de los atentados.

En la prevención de atentados terroristas, con independencia de las técnicas que se utilicen, el objetivo está puesto en identificar marcadores y señales que anticipen la materialización de una amenaza terrorista. En la identificación de esos marcadores, que permitirían una acción anticipatoria de desactivación de la amenaza o de protección contra ella, se desarrollan tres tipos de análisis:

— los dirigidos a identificar y modelizar el comportamiento de amenazas;
— los destinados a identificar y modelizar vulnerabilidades de los sistemas que pueden ser objetivo potencial de la acción de esas amenazas;
— los encaminados a simular las consecuencias de los atentados cruzando el comportamiento de amenazas confrontadas o engarzadas con las vulnerabilidades de los sistemas.

En la prevención del riesgo de incidentes críticos por atentados terroristas destacan los sistemas de *early warning* o de alerta temprana. Estos sistemas están basados en la doctrina *indication and warning* (alerta por indicadores), desarrollada en la primera mitad del siglo pasado y sistematizada en los años setenta por Cynthia Grabo[13] en el ámbito militar en los EEUU para introducir previsión en la evaluación del riesgo de agresión. Desde su marco metodológico ya extendido a todo tipo de previsiones de riesgo en ámbitos sociales,[14] se tiene en cuenta no sólo el análisis de un volumen extenso de datos históricos sobre el objeto de evaluación, sino señales que en el presente pueden indicar o marcar la emergencia de un riesgo. El método desarrolla una serie de indicadores alimentados por datos cuantitativos y cualitativos sistemáticamente recogidos sobre el terreno de análisis, determina la clase de eventos críticos que pueden apuntar a un riesgo específico y lo hace determinando las clases de eventos críticos que pueden apuntar a un riesgo específico, haciendo pasar a toda la información disponible por un continuo proceso de revisión y calibración desarrollado por un equipo dedicado de expertos. Los sistemas de alerta temprana son siempre subsidiarios de una adecuada evaluación del riesgo (amenazas x vulnerabilidades) sobre los espacios u objetos de estudio donde pretenden implantarse. La preexistencia de mapas y escenarios de riesgo es esencial para desarrollar esquemas de alerta temprana.

En términos funcionales, los sistemas de alerta temprana están llamados a emitir indicadores de riesgo en áreas o segmentos sociales concretos (p.ej. las infraestructuras críticas) que pueden ser objetivo de una amenaza terrorista. Adicionalmente, aunque con mayor dificultad de aplicación en el ámbito antiterrorista, los sistemas de alerta temprana pueden enfocarse no sólo sobre riesgos, sino sobre la detección temprana de oportunidades, inscritos en dinámicas de prospectiva prescriptiva.

13. Para una revisión publicada, ver Grabo, C. (2004), *Anticipating Surprise: analysis for strategic warning*. Lanham: University Press of America.

14. Cf. Gurr, J.L. y Davies, T.R. (1998). *Preventive Measures: Building Risk Assessment and Crisis Early Warning Systems*. Lanham: Rowman & Littlefield

Haciendo un planteamiento ideal, un sistema de alerta temprana incorpora procedimientos de evaluación del riesgo y está conectado a procesos, más o menos protocolizados, de toma de decisiones. En concreto, los indicadores de riesgo deberían canalizarse a través de dos tipos de respuesta: una preventiva para evitar o gestionar un riesgo; y otra de contención una vez que el riesgo, en función de la comunión de una amenaza con una o varias vulnerabilidades, se ha traducido en un peligro emergente para la ciudadanía y es necesario producir una respuesta reactiva.

La alerta temprana para riesgos y oportunidades está construida sobre una base de indicadores que marcan, anticipadamente, a esos riesgos. Esos indicadores de riesgo son fórmulas cualitativo-cuantitativas compuestas por los elementos que se supone conforman cada uno de los riesgos —y/u oportunidades— que pueden detectarse o preverse en el área de estudio.

La elaboración de indicadores es una tarea exhaustiva y su calibración un proceso continuo. Los conjuntos funcionales más complejos de indicadores para una unidad de seguridad pública encargada de su evaluación están limitados sólo por el foco que quiera ponerse en el análisis y los recursos permanentes que se pretenda invertir. Los más completos —pero también los más exhaustivos e intricados— son las estructuras de indicadores compuestas por variables de naturaleza cuantitativa y por elementos de índole cualitativa procedentes, al menos, de la monitorización selectiva de las denominadas coordenadas política, económica, social, tecnológica, ambiental y legal (PESTEL) que puedan integrar la ecuación de actuación de la amenaza terrorista.

La estructura de indicadores de un sistema de alerta temprana está montada sobre capacidades de gestión del conocimiento provistas para recoger información de todas las fuentes de interés, almacenarla y relacionarla, y trasladarla en canales automáticos o semisupervisados a un equipo de análisis destinado a calibrar la fuerza de cada indicador con respecto a umbrales de riesgo y oportunidad definidos. Cuanta mayor capacidad exista de cuantificar variables, mayor posibilidad habrá de utilizar modelos computacionales o algoritmos para basar los indicadores en ecuaciones matemáticas. Sin embargo, aunque éstas puedan aplicarse, sobre todo, a modelos econométricos o financieros, la experiencia en inteligencia de indicadores demuestra que, ante fenómenos sociales, los indicadores de riesgo deben contener tanto elementos cuantitativos como cualitativos, siendo en todo caso de naturaleza cualitativa la integración e interpretación finales, así como humana la variable crítica de análisis final; siguiendo a Sorensen, la capacidad interpretativa humana es la clave de un sistema de indicadores, por muy elevada tecnología (absolutamente necesaria por otra parte) que se haya aplicado a la arquitectura de prevención.

Otra de las líneas de desarrollo en la secuencia de previsión de atentados terroristas de gran envergadura, común a los sistemas de protección de infraestructuras críticas, son los simuladores de consecuencias. Los modelos de simulación de consecuencias están llamados a presentar escenarios anticipados de cómo y de qué manera la destrucción de, por ejemplo, una infraestructura crítica del transporte debido a un atentado terrorista en masa va a afectar al normal desenvolvimiento de los servicios y de la vida de la ciudadanía.

Los esquemas de simulación no buscan sólo emular los efectos que produce el impacto del atentado terrorista sobre servicios esenciales, sino la *simulación de la interdependencia*, es decir, cómo ese componente (una infraestructura) se relaciona con otras, afectándolas y creando disfuncionalidad en cascada, y hasta dónde y qué consecuencias tendrán esas disfuncionalidades generadas. Bednar y Page consideran que «los modernos métodos de simulación permiten un uso bastante completo de perspectivas cualitativas (como la cultura) y de información cuantitativa (como las actividades de grupos violentos) como para abordar problemas sociocomportamentales soslayando (con esos modelos) las limitaciones cognitivas humanas».[15]

Un par de ejemplos de aplicación de arquitecturas de simulación de efectos en atentados terroristas lo constituyen los modelos dinámicos tridimensionales para la simulación de consecuencias de atentados terroristas con bombas sucias o la modelización basada en agentes (*agent-based modelling*) que el Programa de Computación Avanzada del Departamento de Seguridad Interior de los EEUU está llevando a cabo para anticipar las consecuencias económicas en su territorio de atentados terroristas de gran envergadura.

2.2.2 Mitigación

La mitigación es una componente de la todavía acción preventiva de gestión del riesgo destinada, concretamente, a reducir las oportunidades de que una amenaza se materialice o, si lo hace, a conseguir que sus efectos nocivos queden reducidos al mínimo. En ese sentido podría formar parte de la primera de las fases de la secuencia de gestión del continuo del riesgo. Sin embargo, doctrinalmente, puede considerarse una componente separada por cuanto no está tanto destinada a anticipar el riesgo sino, una vez identificado, a tomar decisiones y desarrollar acciones para reducirlo o eliminarlo. En algunas ocasiones, la mitigación también se aplica a la fase de recuperación de las consecuencias de un atentado, una vez que el incidente crítico se ha materializado y es necesario atenuar sus efectos.

Las medidas de mitigación suelen ser estructurales o no-estructurales. Entre las primeras se cuentan multitud de soluciones técnicas o tecnológicas aplicadas, entre otras, a las infraestructuras críticas, como la redundancia de sistemas de información. Entre las segundas, las más extendida es la promulgación de legislación, las indemnizaciones y los seguros.

2.2.3 Preparación

Este segmento del continuo de la gestión de incidentes críticos por terrorismo se ha revitalizado, junto a los dos anteriores ya mencionados, desde el 11-S. En palabras de Howitt y Pangi aquellos atentados «demostraron claramente las limita-

15. Bednar, J. y Page, S. (2007). Can Game(s) Theory Explain Culture?: The Emergence of Cultural Behavior within Multiple Games. *Rationality and Society*, 19(1): 65-97

ciones de las instituciones y dejaron patente la necesidad de establecer el foco en la prevención y en la mitigación del impacto del terrorismo, así como en el desarrollo de mejoradas capacidades en la respuesta de emergencia».[16]

La preparación está fundamentalmente compuesta por acciones educativas e informativas a la comunidad (los semáforos de alerta antiterrorista en EEUU serían un elemento), con un foco concreto en su comportamiento ante un incidente crítico; y por acciones de capacitación, entrenamiento y simulación a los actores públicos y privados llamados a intervenir. Es decir, la preparación está relacionada esencialmente con la conducta de los actores involucrados en un incidente crítico por atentado terrorista (población, profesionales, voluntarios, expertos, etc.).

La columna vertebral de la preparación es un «*plan de respuesta ante incidentes críticos por atentados terroristas*» que contemple todos los escenarios posibles, las distintas jurisdicciones territoriales involucradas, los diversos actores locales, regionales y nacionales llamados a actuar, su protocolo de interactuación y la cadena de mando para lograr una respuesta integrada.

Habitualmente, los planes de respuesta ante amenazas por atentados terroristas de gran envergadura, deben combinar la necesaria flexibilidad para ajustarse a distintas configuraciones de escenarios de intervención, con un cierto nivel de estandarización y protocolización de procesos, de manera que pueda montarse un esquema de respuesta al incidente en el menor tiempo posible porque todos los involucrados conocen cual es el rol que tienen que jugar en el protocolo de actuación.

Los esquemas de respuesta ante un incidente crítico tienen la particularidad de ser sistemas *ad-hoc*, que se tienen que constituir justo para el momento de la respuesta y desmantelarse después. En los esquemas así, que no son residentes ni de estructura permanente más allá de su emergencia coyuntural, la preparación que indique cómo tienen que ensamblarse las piezas que lo compongan y de qué manera tiene que fluir la acción, es capital.

Cada actor, habitualmente dedicado en situación de normalidad a una serie de tareas bajo una estructura operativa concreta, debe haber interiorizado que en una emergencia en la que participe debe cumplir un rol concreto ateniéndose a un protocolo flexible pero claro.

Un adecuado plan de respuesta debería contener un concepto de estructura de mando y un sistema de coordinación entre servicios públicos de todo tipo (asistenciales, médicos, protección civil, bomberos, policiales, judiciales) llamados a intervenir en el incidente.

2.2.4 Respuesta

La respuesta ante un incidente crítico es, evidentemente, el punto más crítico de toda la cadena de gestión de la emergencia. Es donde, aunque se haya mitigado

16. Howitt, A.M. y Pangi, R.L. (eds), (2003). *Countering Terrorism: Dimensions of Preparedness.* Cambridge, MA: M.I.T Press.

de algún modo por inversiones proactivas, el atentado terrorista ha producido un perjuicio a la población. También es la fase en que la preparación de los esquemas de respuesta ante incidentes críticos se van a traducir de manera eficiente o no.

Los primeros en la respuesta (*first responders*) en un escenario de emergencia terrorista suelen ser sanitarios de emergencias, bomberos, agentes de policía y equipos especializados en desactivación de explosivos o de contención anticontaminante, pero también la autoridad judicial. Todos ellos constituyen el primer nivel de reacción ante el desencadenamiento de la crisis por la materialización total o parcial de una amenaza.

La mayoría de los recursos institucionales de gestión de emergencias en los países de nuestro entorno están programando inversiones e investigaciones para dotar al *first responder* de tres tipos de capacidades: acción, comunicación y conocimiento situacional.

En lo que respecta a la acción o actuación del *first responder* se pretende que no se realice aisladamente sino que forme parte integrada de una *malla de actuación de primera respuesta*. En esa malla, cada componente de primera respuesta sería un elemento que ejercería acción sinérgica con los demás, de manera que la acción de suma de las partes fuera más importante que la suma de las acciones individuales (el caso típico de integración está entre los agentes de policía, emergencias sanitarias y bomberos en una actuación ante la explosión de una bomba en un edificio). En ese marco, la acción integrada es completamente dependiente de que todos los agentes dispongan de tecnologías portátiles de información y comunicación interoperables,[17] compatibles entre agencias y dispuestas para conformar una *malla táctica* adaptada a las necesidades específicas definidas por la propia situación de emergencias. Esa comunicación, aparte de para la acción coordinada, debe de servir para desarrollar la tercera capacidad a la que aludíamos, el conocimiento situacional.

En efecto, en una situación de emergencia ante un atentado terrorista los mejores sensores de transmisión de información para que los responsables de la toma de decisiones en la gestión continua del riesgo tengan el conocimiento situacional de mayor calidad posible son los agentes que integran los equipos de primera respuesta.

Las propuestas de inversión e investigación que se están realizando en la Unión Europea para desarrollar y mejorar las condiciones del agente de primera respuesta ante emergencias están insistiendo, además de en la logística de la acción, en las comunicaciones, en la necesidad de habilitar adecuados dispositivos de protección tanto a su actuación sobre el terreno (contra explosivos o contaminaciones) como a las condiciones para salvaguardar su bienestar psicofisio-

17. En 2005 finalizó de implantarse en España el Sistema de Radiocomunicaciones Digitales de Emergencia del Estado (SIRDEE), una malla que comparten las Fuerzas de Seguridad del Estado pero a la que no están adscritas, por ejemplo, ni la Unidad Militar de Emergencias ni los dispositivos autonómicos o los locales. A ese respecto y como ejemplo de la situación, en Cataluña la RESCAT integra todas las comunicaciones de seguridad y emergencias de los servicios dependientes de la Generalitat de Cataluña, pero a ella no están adscritas los que dependen del Ministerio del Interior.

lógico[18] y la resiliencia (capacidad de protegerse del sufrimiento o recuperarse de él).[19] En este último vector desde hace varias décadas se vienen realizando avances mediante la aplicación de la *Critical Incident Technique* (técnica del incidente crítico). La CIT es un protocolo de análisis del comportamiento, descrito por primera vez en 1954 por John Flanagan,[20] que funciona como la aplicación de un ciclo de recogida y tratamiento de información sobre el comportamiento humano, no sólo de *first responders* sino también de decisores críticos sobre el terreno, de cuyo análisis se derivan esquemas de capacitación y preparación para los profesionales ante nuevas emergencias. En ese sentido, es una especie de protocolo de aprendizaje basado en la evidencia que extrae las mejores prácticas de anteriores situaciones de emergencia y prepara más eficientemente al equipo humano de intervención para enfrentarse a futuros incidentes críticos.

La capacidad de los agentes de primera respuesta para contener la incidencia crítica, proteger a la población y abrir la senda para la recuperación de la normalidad, va a depender en gran medida de los recursos para conocer con la máxima precisión qué está sucediendo y cuándo, transmitiendo la información a la cadena de decisión en el teatro de las operaciones.

El conocimiento situacional es una capacidad de los sistemas de gestión de emergencias y evaluación de riesgo destinado a tener una visión integrada y continua del estado del riesgo en una determinada configuración espacial. Desde que los esquemas de gestión de la seguridad ante atentados terroristas se han generalizado con un enfoque preventivo, los primeros desarrollos del *situational awareness* han estado centrados en disponer de una imagen lo más fidedigna posible de las infraestructuras críticas en un espacio territorial local, regional o nacional que pudieran constituirse en objetivo potencial de un atentado terrorista.

El impacto de acciones terroristas sobre infraestructuras críticas se ha considerado prioritario para el establecimiento de órganos de evaluación de riesgo en la seguridad pública, debido a que produce una erosión en el normal funcionamiento de los sistemas de sostenimiento.

En España esta función de monitorización de las infraestructuras críticas para obtener un conocimiento situacional permanente de su estado y vulnerabilidad está encomendada al Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), en la Secretaría de Estado de Seguridad. El CNPIC opera en estrecha comunicación con el Centro Nacional de Coordinación Antiterrorista (CNCA) que realiza una evaluación periódica de la amenaza terrorista. La combinación entre evaluación de la amenaza y el estado de vulnerabilidad de las infraestructuras produce una evaluación del riesgo.

En los EEUU, el Terrorist Threat Warning System (sistema de alerta sobre amenaza terrorista) del FBI realiza evaluaciones de riesgo en cooperación con los cen-

18. Para una revisión del estado de la cuestión, Jackson, B.A.; Peterson, D. J.; Bartis, J.T.; LaTourrette, T.; Brahmakulam, I. (2002). *Protecting Emergency Responders: lessons learned from terrorist attacks*. Santa Monica: RAND.

19. Commission of the European Communities. 7th Framework Programme: Security.

20. Flanagan, J.C. (1954). The Critical Incident Technique. Psychological Bulletin, 51(4)

tros de conocimiento situacional o centros de fusión de inteligencia de los Estados Federales.

En lo que a la Unión Europea se refiere y por lo que respecta a la protección de infraestructuras críticas ante atentados terroristas la Comunicación de la Comisión Europea COM/0698 de 2004 sobre «Prevención, Preparación y Respuesta a Ataques Terroristas» y el «Programa de Solidaridad de la UE sobre Consecuencias de Amenazas y Atentados Terroristas», endosados ambos por el Consejo de la Unión en diciembre de 2004, respaldan la intención de la Comisión de proponer un Programa Europeo de Protección de Infraestructuras Críticas (EPCIP) y apoyan el establecimiento de una Red Informativa de Alerta sobre Infraestructuras Críticas (CIWIN).

En noviembre de 2005, la Comisión Europea promulgó el Libro Verde sobre un Programa Europeo de protección de Infraestructuras Críticas que proporcionaba directrices políticas sobre cómo la Comisión podría establecer el EPCIP y la CIWIN. En diciembre de 2005 el Consejo de Justicia y Asuntos de Interior llamó a la Comisión a efectuar una propuesta sobre el EPCIP, que se materializó en diciembre de 2006 en la elaboración de una directiva sobre la identificación y designación de una Infraestructura Crítica Europea y la evaluación de necesidades sobre su protección, así como en la comunicación de un EPCIP que contuviera un plan de acción. La directiva establecería procedimientos comunes para la identificación de infraestructuras críticas y para la evaluación de necesidades de protección, así como una guía para la producción de medidas de protección sectoriales específicas para estas infraestructuras.

El conocimiento situacional, que en sí mismo tiene naturaleza y objeto anticipatorio de una crisis, está conectado a los mecanismos de respuesta sobre el terreno por otro concepto, la *common operational picture* (COP - visión operacional conjunta). La COP proporciona, a los escalones de mando y control, un esquema de gestión de crisis con una posición unificada de los recursos que operan sobre los riesgos, en una vertiente de actuación anticipada, o sobre el daño causado cuando la amenaza se ha materializado.

Tanto la COP como los dispositivos de conocimiento situacional están soportados en arquitecturas tecnológicas específicas de información y comunicaciones.

Un primer paso para lograr el COP son los Puestos de Mando Avanzado (PMA) que en España han estado desarrollando las comunidades autónomas para, inscritos en planes regionales de gestión de emergencias, responder a incidentes críticos coordinando las actuaciones sobre el terreno. El inconveniente de todos estos PMA es que, en el mejor de los casos, son de ámbito regional y pretenden coordinar las actuaciones de un solo actor sobre el terreno (p.ej. los bomberos), sin saber siquiera si el PMA de una agencia podría comunicarse y ser interoperable con el PMA de otra, ni si un conjunto de PMA operativos podrían acoplarse a una malla integrada en un PMA de coordinación operacional.

2.2.5 Recuperación

Habitualmente ejecutada por servicios especializados locales o regionales, también usualmente con apoyo financiero de los gobiernos nacionales o federa-

les, la recuperación está destinada a restaurar la normalidad en el escenario donde se han producido los efectos del atentado terrorista y reparar, en la medida de lo posible, el daño ocasionado a las víctimas.

Al igual que el resto de fases de gestión del incidente crítico, la recuperación debería formar parte, más o menos estipulada, de un plan de respuesta a incidentes críticos que contemple la manera en que deben complementarse las piezas locales, autonómicas y nacionales. Si la capacidad nacional de respuesta a incidentes críticos está bien estructurada, la fase de recuperación estaría conectada con la simulación de consecuencias de atentados (que ofrecería caminos de restauración por donde avanzar, sobre todo en la recomposición de la interdependencia de servicios) y también con la preparación de los actores de recuperación para integrarse recibiendo el relevo del equipo de primera respuesta. Esta última vertiente se pone de manifiesto, especialmente, cuando existen un número elevado de víctimas heridas o fallecidas, para las que hay que habilitar áreas de contención, derivación de heridos y apoyo psicológico y social, amén del depósito y traslado de cadáveres determinado por la autoridad judicial, acciones que sin solución de continuidad conectarán con los esfuerzos de recuperación y rehabilitación.

Hasta aquí una revisión muy general de las fases en las que idealmente podría dividirse la secuencia de gestión de incidentes críticos ante atentados terroristas. Conviene tener presente que esta secuencia, como hemos señalado ya, es un continuo, y los continuos dimensionales sobre el terreno a veces se resisten a aceptar la segmentación delineada sobre el plano.

Al mismo tiempo, es útil ser consciente de que algunos de los elementos en la «doctrina de las fases» pueden muy bien solaparse entre ellas (prevención y mitigación), o tener componentes que estando bien encuadrados en una fase pueden encajar en otra (el conocimiento situacional, por ejemplo, tanto en prevención como en respuesta). Lo que sí resplandece en la doctrina es la necesidad de prepararse y planificar la gestión de incidentes críticos y de que los mecanismos de acción se ajusten, en la mejor medida posible, a la realidad.

3. GESTIÓN DE LA SEGURIDAD EN UN GRAN ATENTADO. ESTUDIO DE CASO

3.1 INTRODUCCIÓN

Uno de los autores de este trabajo coordinó las actuaciones sobre el terreno del atentado terrorista del 11 de marzo de 2004 en Madrid, en su localización de la calle Téllez, donde, a unos setecientos metros de la estación de ferrocarril de Atocha y procedente de Alcalá de Henares, explosionó un convoy de viajeros con focos de detonación en cuatro de sus seis vagones.

El caso es particularmente significativo porque requirió el establecimiento sobrevenido e improvisado de una respuesta de emergencia autoorganizada sobre el terreno, en ausencia de protocolos de actuación y planes estructurados.

En este atentado, como se recordará, entre las 7:37 y las 7:39 de la mañana, detonaron diez cargas explosivas en cuatro trenes, produciéndose ciento noventa y ún fallecidos y más de mil ochocientos heridos.

El comisario Zurita transitaba por la zona de camino diario a su puesto de trabajo y, ante el incidente, se detiene y comienza a hacerse una composición de la magnitud de la catástrofe, procede a contactar con los distintos profesionales presentes en la zona y a recabar información para dibujar mentalmente un perfil de conocimiento situacional.

3.2 EVACUAR HERIDOS Y PRESERVAR VIDAS

La primera acción, una vez evacuados los heridos y tras el reconocimiento de la zona, es la de comprobar si queda alguna persona viva en el interior de los vagones o en las proximidades para, posteriormente, conformar un equipo de seguridad con agentes del Cuerpo Nacional de Policía y de la Policía Municipal de Madrid, auxiliados por personal de seguridad privada presentes en el lugar.

El objetivo de este equipo es desalojar la zona de personas, detectar elementos de riesgo (se observa una mochila sospechosa en un vagón) y establecer una zona de seguridad.

Al mismo tiempo se requiere la presencia de un equipo de desactivación de explosivos (TEDAX) para inspeccionar el lugar y asegurar actuaciones posteriores.

Hasta la llegada de los TEDAX, se va generando una malla improvisada de comunicaciones, informando del estado de la situación a responsables policiales, contactando con el Centro Operativo de Comunicaciones de la Policía, con los responsables de los TEDAX y de Policía Científica, así como con especialistas de otros servicios de emergencias que estaban operando de manera autónoma sobre el terreno (Policía Municipal, Emergencias Sanitarias, Bomberos, Protección Civil y Cruz Roja). Se imparten instrucciones sobre el procedimiento a seguir para la recuperación de los cadáveres. De este modo, se visualiza e interioriza por los demás la figura de un mando operativo unificado de gestión del incidente.

Se imparten las primeras instrucciones

3.3 RECUPERAR VÍCTIMAS FALLECIDAS

Una vez inspeccionada el área por los TEDAX, hasta la llegada de la comisión judicial y de los técnicos de Policía Científica, se autoriza a los bomberos para que realicen un estudio técnico de situación y hagan un recuento de cadáveres. El objetivo es ir diseñando una visión operacional conjunta (COP).

Los bomberos realizan un estudio técnico de la situación y cuentan los cadáveres

Las víctimas fallecidas son cubiertas con mantas, para que queden protegidas de miradas indiscretas de curiosos, fotógrafos y reporteros.

Se realiza un reportaje fotográfico y una video grabación de la zona con propósitos forenses y se autoriza a Protección Civil la instalación de un «centro mortuorio temporal» que acoja a los cadáveres una vez se determine su levantamiento por la autoridad judicial.

En paralelo, se solicita el suministro de sacos mortuorios que alojen a los cadáveres y sus pertenencias, con vistas a facilitar su traslado.

Centro mortuorio temporal

Con la llegada de la comisión judicial se procede a la extracción, recuperación y traslado de las víctimas fallecidas. La coordinación entre los diferentes servicios de primera respuesta es total.

En la recuperación y traslado de los cuerpos la coordinación es absoluta

En el centro mortuorio temporal se realizan las labores básicas de preidentificación por el equipo forense y los técnicos de Policía Científica.

Los cadáveres finalmente son transportados a una localización centralizada, común a todos los focos del siniestro del 11M (Pabellón nº 6 de IFEMA).

Traslado de las víctimas fallecidas al Pabellón 6 de IFEMA

3.4 PRESERVAR EVIDENCIAS Y VOLVER A LA NORMALIDAD

Recuperados los sesenta y cuatro cadáveres, vuelven a pasar los TEDAX para hacer toma de muestras y, posteriormente, se recogen todos los objetos personales que se encuentran dispersos por la zona, tarea que realizan los bomberos.

Se autoriza el paso a empleados de RENFE y ADIF, para que realicen los estudios técnicos correspondientes.

Se establece un servicio de vigilancia y salvaguarda de la zona, con el fin de preservar las evidencias y las pruebas.

Se da paso a los distintos servicios de limpieza y reconstrucción para la recuperación de la normalidad tras el incidente crítico.

El responsable operativo de la crisis cesa en su función.

4. ESQUEMA DE GESTIÓN DE LA SEGURIDAD

Tanto la doctrina internacional generada a partir de la experiencia en atentados terroristas de gran envergadura como la práctica nacional en este tipo de incidentes críticos aconsejan prestar atención a una serie de componentes mínimos que debería contener una capacidad de gestión de crisis en grandes atentados terroristas:

1. Un atentado terrorista compone el escenario (a veces un macroescenario o un escenario múltiple) de un crimen y, por tanto, requiere ser tratado profesionalmente como un problema de seguridad.
2. Puesto que lo consideramos el escenario de un crimen, la autoridad Judicial debería estar involucrada, al menos, en la fase de respuesta integrada al incidente crítico.
3. Los efectivos de primera respuesta a un incidente crítico proceden, normalmente, de servicios locales de emergencia, dependientes la mayoría de las veces de corporaciones municipales. Pero también pueden proceder del ámbito regional o nacional.
4. Ante grandes atentados, la respuesta más eficiente siempre procede de la integración de esfuerzos multiagencia en un esquema unitario.
5. La eficiencia de la respuesta y de la recuperación ante un atentado terrorista de gran envergadura depende de que todos los servicios y actores involucrados se encuentren preparados y hayan interiorizado su misión operativa en función de un plan de respuesta a incidentes críticos.
6. En un incidente crítico provocado por un atentado todos los servicios involucrados deben responder a una autoridad operativa de gestión del incidente, que en la fase de crisis será un responsable de la seguridad pública integrado en lo posible en un puesto de mando avanzado. En el caso de España, debería ser un directivo de la policía autonómica en aquellas comunidades con cuerpo de policía integral, o un alto mando de las fuerzas y cuerpos de Seguridad del Estado en las demás (Cuerpo Nacional de Policía o Guardia Civil).
7. La autoridad operativa debería disponer de capacidad de conocimiento situacional y acceder a una visión conjunta e integrada (COP) del escenario de crisis. Este conocimiento debería ser suministrado por el Centro de Coordinación de Emergencias a través del puesto de mando avanzado, vía tecnologías de la información y comunicación por malla integrada.

La combinación de todos estos ingredientes debería perseguir la composición de un esquema integral de respuesta y recuperación ante incidentes críticos (figura 2). La última legislación española sobre emergencias declara a la Unidad Militar de Emergencias como la competente para dirigir y desplegar capacidades en los incidentes críticos, incluidos atentados terroristas, declarados de nivel 3 (emergencia nacional) o en aquéllos otros definidos por el presidente del Gobierno.[21] La UME dispone de sus propias capacidades tanto en dirección operacional como en despliegue táctico, además de sus propias mallas de tecnologías de información y comunicación y de los medios necesarios para establecer una componente de conocimiento situacional y de visión operacional integrada.

En incidentes críticos que conduzcan a emergencias de nivel 2 (autonómicas) o locales (nivel 1), un atentado terrorista es, como ya se ha referido, el escenario de un crimen que compone un problema de seguridad en donde tienen que intervenir servicios muldisciplinares de primera respuesta. El estudio de caso que hemos descrito más arriba y la doctrina acumulada coinciden en ponernos de manifiesto la relevancia de integrar comunicaciones e información desde un Centro de Coordinación de Emergencias para ponerlas al servicio de una autoridad operativa de gestión de la crisis, convenientemente dotada de un puesto de mando avanzado. La mayoría de las comunidades autónomas disponen de centros regionales de Coordinación de Emergencias, que con su potencia de integración de información y comunicaciones, así como con la posibilidad de aglutinar en su seno representantes residentes de todos los servicios de primera respuesta ante las emergencias, se constituyen en el núcleo más apropiado para coordinar operacionalmente la respuesta a una crisis.

En esa respuesta, la visión de lo que está sucediendo procede primordialmente de quien está actuando sobre el terreno, de ahí la importancia de los actores locales y la conveniencia de escuchar a los agentes *in situ* direccionando desde abajo las decisiones hacia arriba.[22] Esos agentes de primera respuesta deben estar intercomunicados con el PMA y éste con el Centro de Coordinación de Emergencias.

La respuesta a incidentes críticos por atentados terroristas debería estar protocolizada a través de un plan específico, armonizado con los ya existentes planes regionales de gestión de emergencias en la mayoría de comunidades autónomas. Esos protocolos deberían dejar claro cómo la Secretaría de Estado de Seguridad de Interior (Centro Nacional de Coordinación Antiterrorista y el Centro Nacional de Protección de Incidentes Críticos) puede apoyar la coordinación operacional, cómo se conectan las distintas piezas en el puzzle de la respuesta y cómo se componen los distintos recursos de información y comunicación para asegurar las mejores capacidades desplegables sobre el terreno para unos incidentes de baja frecuencia pero de alto impacto como los atentados terroristas de gran envergadura.

21. Real decreto 399/2007, del Ministerio de la Presidencia, de 23 de marzo de 2007, por el que se aprueba el Protocolo de Intervención de la Unidad Militar de Emergencias

22. Kayyem, J.N. y Pangi, R.L (eds), (2003). *First to Arrive: State and Local Responses to Terrorism*. Cambridge: The MIT Press

Figura 2. *Esquema integral de respuesta y recuperación ante incidentes críticos.*