



25 años del 11-S: del Terrorismo Global al Nuevo Paradigma de la Seguridad

Consecuencias sobre los riesgos y amenazas, la inseguridad, el “imperio del miedo”, las libertades, las políticas de seguridad y las lecciones aprendidas

El 11 de septiembre de 2001 constituye uno de los principales puntos de inflexión de la seguridad contemporánea. Los atentados contra el World Trade Center, el Pentágono y el vuelo United Airlines 93 provocaron cerca de 3.000 víctimas y desencadenaron una transformación profunda de las políticas de seguridad de Estados Unidos y de buena parte de la comunidad internacional.



Veinticinco años después, el balance exige superar tanto la visión exclusivamente antiterrorista como la interpretación puramente histórica. El 11-S produjo una transformación estructural de los sistemas de inteligencia, seguridad interior, control fronterizo, seguridad aeroportuaria, cooperación internacional, vigilancia, intercambio de información y respuesta ante emergencias. La creación del Department of Homeland Security, la reorganización de las capacidades de inteligencia y seguridad y la aprobación de nuevas facultades de investigación constituyeron algunos de los principales resultados institucionales.

Pero esa transformación tuvo también una dimensión controvertida: la ampliación de las capacidades de vigilancia y de los poderes excepcionales planteó un conflicto permanente entre seguridad y libertad.

El presente artículo analiza esta evolución y plantea una cuestión esencial para el futuro: **¿cómo construir sociedades más seguras sin convertir el miedo en el principio permanente de gobierno de la seguridad?**

Veamos esquemáticamente la realidad de nuestra percepción y establecer un decálogo de la situación.

1 Introducción: el 11-S como ruptura histórica

El 11 de septiembre de 2001 no fue únicamente un atentado terrorista de extraordinaria magnitud. Fue una ruptura de paradigma.

Hasta ese momento, gran parte de las políticas occidentales de seguridad estaban condicionadas por la Guerra Fría, la delincuencia organizada, los conflictos regionales, el terrorismo nacional y las amenazas convencionales.

El 11-S demostró que un actor no estatal podía:

- planificar una operación transnacional;
- utilizar infraestructuras civiles como instrumentos de ataque;
- aprovechar las interdependencias tecnológicas y económicas;
- producir efectos económicos y psicológicos globales;
- atacar simultáneamente diferentes objetivos;
- utilizar la movilidad internacional como ventaja operativa;
- transformar un acontecimiento localizado en una crisis mundial.

La amenaza dejó de percibirse exclusivamente como un problema policial o militar para convertirse en un problema integral de seguridad nacional, internacional y social.

El cambio fundamental fue conceptual: La seguridad dejó de consistir únicamente en proteger territorios y pasó a centrarse en proteger sociedades, sistemas, infraestructuras, información, personas y procesos esenciales.

El 11-S demostró que la amenaza no necesitaba disponer de un ejército convencional para producir efectos estratégicos.

2

El incremento de riesgos y amenazas después del 11-S

De la amenaza conocida a la amenaza multidimensional

Uno de los principales efectos del 11-S fue la ampliación del concepto de amenaza.

El terrorismo pasó a coexistir con: radicalización, terrorismo doméstico, crimen organizado transnacional, proliferación de armas, ataques contra infraestructuras, ciberamenazas, espionaje, sabotaje, desinformación, amenazas híbridas, drones, ataques contra cadenas logísticas, amenazas biológicas, riesgos tecnológicos, conflictos geopolíticos.

La transformación del riesgo

El riesgo dejó de poder analizarse exclusivamente mediante la relación:

$$\text{amenaza} + \text{vulnerabilidad} = \text{riesgo}$$

El nuevo escenario exige incorporar:

$$\text{amenazas} + \text{vulnerabilidades} + \text{exposición} + \text{interdependencias} + \text{consecuencias} + \text{resiliencia} + \text{capacidad de recuperación}$$

Esta evolución es especialmente importante para las infraestructuras críticas.

3

De la inseguridad objetiva a la inseguridad percibida

Uno de los efectos más importantes del 11-S fue la transformación de la percepción social del riesgo.

El terrorismo demostró una capacidad extraordinaria para generar:

$$\text{pocas víctimas directas} + \text{enorme impacto psicológico} + \text{repercusión política} + \text{impacto económico} + \text{percepción global de vulnerabilidad}$$

La consecuencia fue una ampliación del concepto de inseguridad.

La sociedad comenzó a percibir que: nadie estaba completamente protegido; cualquier ciudad podía convertirse en objetivo; cualquier infraestructura podía ser atacada; los espacios cotidianos podían transformarse en objetivos; la amenaza podía aparecer sin aviso.

La seguridad pasó, por tanto, a destacar su doble dimensión:

Seguridad objetiva. Capacidad real de prevenir, detectar, responder y recuperarse ante una amenaza.

Seguridad subjetiva. Percepción individual y colectiva de protección o vulnerabilidad.

Esta diferencia resulta esencial para comprender el denominado “**imperio del miedo**”.

4 El impacto sobre las libertades públicas

La tensión seguridad-libertad

Después del 11-S apareció con especial intensidad una cuestión: ¿Hasta dónde puede llegar un Estado para proteger a sus ciudadanos?

La respuesta estadounidense incluyó una expansión considerable de las capacidades de investigación y vigilancia.

El USA PATRIOT Act amplió las herramientas disponibles para investigar amenazas terroristas y facilitó el intercambio de información entre inteligencia y fuerzas de seguridad. (Departamento de Justicia)

Posteriormente, algunas de sus disposiciones fueron modificadas, limitadas o dejaron de estar vigentes, pero el modelo institucional creado después del 11-S tuvo una duración mucho mayor.

Vigilancia y sociedad digital

El desarrollo tecnológico multiplicó posteriormente las capacidades de vigilancia.

En 2001 la información digital disponible era limitada comparada con la actual.

Veinticinco años después existen: teléfonos inteligentes; reconocimiento facial; inteligencia artificial; análisis masivo de datos; geolocalización; biometría; videovigilancia inteligente; análisis de redes sociales; sensores; plataformas digitales; tecnologías predictivas.

La infraestructura de vigilancia desarrollada después del 11-S se integró posteriormente en un ecosistema digital mucho más amplio.

La pregunta actual ya no es únicamente: **¿puede el Estado vigilar?** sino: **¿qué datos puede utilizar, con qué finalidad, durante cuánto tiempo, bajo qué controles y con qué mecanismos de supervisión?**

5 El cambio radical en las políticas de seguridad

Del modelo fragmentado al modelo integrado

Inteligencia compartida. La cooperación pasó a ser un elemento central.

Se desarrollaron: centros de inteligencia; grupos conjuntos; mecanismos de intercambio de información; cooperación federal-estatal-local; colaboración público-privada; inteligencia antiterrorista; análisis de amenazas.

El principio pasó a ser:

«Necesidad de saber» → «Necesidad de compartir».

Es decir, pasar de proteger la información mediante compartimentos estancos a compartirla cuando ello sea necesario para prevenir una amenaza.

Seguridad aeroportuaria y fronteriza

La seguridad del transporte experimentó una transformación profunda.

La seguridad aeroportuaria se convirtió en un ejemplo paradigmático de cómo una amenaza concreta puede transformar completamente una actividad cotidiana.

De la seguridad antiterrorista a la seguridad integral

Una de las principales consecuencias indirectas del 11-S fue el reconocimiento de que las amenazas no pueden abordarse exclusivamente mediante una dimensión.

La seguridad moderna integra: seguridad física; seguridad electrónica; ciberseguridad; inteligencia; seguridad de la información; seguridad de las personas; seguridad operacional; protección de infraestructuras; continuidad de negocio; gestión de crisis; protección civil; resiliencia.

Esta convergencia constituye actualmente uno de los pilares de la protección de las infraestructuras críticas y estratégicas.

6 De la prevención del atentado a la resiliencia

El 11-S generó inicialmente un paradigma muy orientado a:

prevenir → detectar → neutralizar

Pero las amenazas contemporáneas han obligado a evolucionar hacia:

prevenir → detectar → responder → resistir → recuperar → aprender → adaptarse

Es el paso desde la **protección** hacia la **resiliencia**. Una organización no puede aspirar únicamente a impedir todos los incidentes.

Debe ser capaz de: continuar operando; funcionar degradadamente; recuperar servicios; mantener funciones esenciales; aprender del incidente; adaptarse a nuevas amenazas.

7 La transformación de la amenaza terrorista

La amenaza también evolucionó. El modelo inicial de grandes organizaciones centralizadas dio progresivamente paso a: células; actores individuales; radicalización online; propaganda digital; financiación descentralizada; ataques de bajo coste; utilización de vehículos; drones; herramientas digitales; manipulación informativa.

La consecuencia es fundamental: **La reducción de la capacidad de las grandes organizaciones terroristas no significa la desaparición del riesgo terrorista.**

La amenaza se ha vuelto más distribuida, adaptable y difícil de detectar.

8 Del terrorismo global a las amenazas híbridas

Veinticinco años después, el principal aprendizaje es que el terrorismo ya no puede estudiarse aisladamente.

La seguridad contemporánea está condicionada por la convergencia de: terrorismo; crimen organizado; ciberataques; guerra híbrida; sabotaje; espionaje; desinformación; conflictos geopolíticos; ataques contra infraestructuras; dependencia tecnológica; vulnerabilidades de las cadenas de suministro.

El adversario puede no buscar destruir una infraestructura. Puede buscar: **degradarla, paralizarla, manipularla, desacreditarla o hacerla dependiente.**

9 Las infraestructuras críticas como nuevo campo de batalla

El 11-S permite comprender una cuestión hoy fundamental: **La protección de una sociedad depende de la protección de los sistemas que mantienen su funcionamiento que son sus infraestructuras críticas y esenciales que** adquieren especial importancia.

Una infraestructura puede ser objetivo directo, pero también puede ser utilizada como punto de entrada para afectar a otras.

Aquí aparece el concepto de: Dependencia crítica y, posteriormente: Interdependencia crítica. La caída de un sistema puede producir efectos en cascada sobre otros.

10 Propuesta de modelo de seguridad para el futuro

El nuevo paradigma debería estructurarse sobre ocho pilares:

1. **Anticipar antes que reaccionar.**
2. **Gestionar riesgos dinámicos y acumulativos.**
3. **Integrar seguridad física, electrónica, lógica y cibernética.**
4. **Garantizar continuidad de las funciones esenciales.**

5. **Tecnología. Utilizar IA, analítica, sensores, automatización y sistemas inteligentes bajo principios de gobernanza.**
6. **Coordinación. Integrar administraciones, operadores críticos, empresas y seguridad privada.**
7. **Garantizar que las medidas de seguridad sean legítimas, necesarias y proporcionales.**
8. **Convertir la seguridad en una responsabilidad colectiva.**

Conclusiones

Veinticinco años después, el 11-S continúa siendo una referencia fundamental para comprender la evolución de la seguridad contemporánea.

Su principal legado no es únicamente la transformación de la lucha contra el terrorismo. Es haber demostrado que: **una amenaza relativamente limitada en medios puede producir consecuencias sistémicas cuando encuentra una sociedad altamente interconectada y vulnerable.**

El 11-S cambió la arquitectura institucional de la seguridad, incrementó la cooperación entre inteligencia y fuerzas de seguridad, reforzó el control de fronteras y transportes y aceleró la creación de sistemas de intercambio de información.

Pero también generó un debate permanente sobre los límites del poder, la vigilancia, la privacidad y las libertades públicas.

La gran cuestión de los próximos años será todavía más compleja que la planteada en 2001.

Ya no se trata solamente de: **“¿cómo evitar otro 11-S?”**. La pregunta debe ser: **“¿Cómo proteger una sociedad democrática frente a un conjunto simultáneo de amenazas terroristas, híbridas, cibernéticas, geopolíticas, tecnológicas y contra sus infraestructuras críticas sin sacrificar los valores que precisamente pretende proteger?”**

La respuesta no puede ser la seguridad absoluta, porque ésta no existe. Tampoco puede ser la vigilancia permanente ni el miedo como principio político.

El nuevo paradigma debe construirse sobre:

**inteligencia + prevención + seguridad integral + proporcionalidad + resiliencia +
cooperación + continuidad + libertad**

En última instancia, la principal lección del 11-S puede expresarse mediante una paradoja: **Una sociedad verdaderamente segura no es aquella que elimina todos los riesgos, sino aquella que posee la capacidad de anticiparlos, resistirlos, recuperarse de ellos y hacerlo sin renunciar a sus principios fundamentales**

Manuel Sánchez Gómez-Merelo
Vocal de la Junta Directiva de AES