Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Artículo de Investigación

LAS INFRAESTRUCTURAS CRÍTICAS ESPAÑOLAS COMO OBJETIVO DE ELEMENTOS TERRORISTAS. ANÁLISIS DE VULNERABILIDADES, MARCO NORMATIVO Y ESTRATEGIAS DE PROTECCIÓN

Raúl Moreno Ruiz
Capitán de la Guardia Civil
Especialista en Seguridad Penitenciaria (Ministerio del Interior)
Máster en Dirección Operativa de la Seguridad - Grado en Derecho
raul.moreno@dgip.mir.es

Recibido 23/03/2026
Aceptado 04/06/2026
Publicado 30/06/2026

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8979

Cita recomendada: Moreno, R. (2026). Las infraestructuras críticas españolas como objetivo de elementos terroristas. Revista Logos Guardia Civil, 4(2), pp. 281–302. https://doi.org/10.64217/logosguardiacivil.v4i2.8979

Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8979

LAS INFRAESTRUCTURAS CRÍTICAS ESPAÑOLAS COMO OBJETIVO DE ELEMENTOS TERRORISTAS. ANÁLISIS DE VULNERABILIDADES, MARCO NORMATIVO Y ESTRATEGIAS DE PROTECCIÓN

Resumen: La vulnerabilidad de las infraestructuras críticas españolas ante la amenaza terrorista desde una perspectiva legal, institucional y operativa. El estudio considera el marco normativo existente —a través de la Ley 8/2011 y la Directiva (UE) 2022/2557 sobre la resiliencia de las entidades críticas (CER), se centra en los sectores clave más vulnerables al riesgo y evalúa la arquitectura institucional del sistema de protección español. A través de una metodología de análisis documental y la revisión de literatura especializada, se encuentra que a pesar de un sólido sistema de protección para infraestructuras críticas (PIC) en España, existen brechas significativas en la ciberseguridad industrial, la coordinación interadministrativa y la transposición de directivas europeas, que requieren atención urgente. Las principales amenazas para el horizonte 2025-2030 se identifican como el terrorismo yihadista, actores estatales hostiles y el ciberterrorismo.

Abstract: This article analyses the vulnerability of Spanish critical infrastructures to the terrorist threat from a legal, institutional and operational perspective. Its goals are to evaluate the current regulatory framework —led by Law 8/2011 and Directive (EU) 2022/2557 on the resilience of critical entities (CER)—, identify the strategic sectors most exposed to risk, and evaluate the institutional architecture of the Spanish protection system. Through documentary analysis and specialised literature review, it is concluded that Spain has a solid critical infrastructure protection (CIP) system. However, there are significant gaps in industrial cybersecurity, inter-administrative coordination and transposition of European directives that require urgent attention. The main threats identified for the 2025-2030 strategic horizon are jihadist terrorism, hostile state actors and cyberterrorism.

Palabras clave: infraestructuras críticas; terrorismo; seguridad nacional; ciberterrorismo; amenaza híbrida.

Keywords: critical infrastructure; terrorism; national security; cyberterrorism; hybrid threat.

ABREVIATURAS

CCN-CERT: Centro Criptológico Nacional – Computer Emergency Response Team

CITCO: Centro de Inteligencia contra el Terrorismo y el Crimen Organizado

CNI: Centro Nacional de Inteligencia

CNPIC: Centro Nacional de Protección de Infraestructuras Críticas

DSN: Departamento de Seguridad Nacional

ENISA: Agencia de la Unión Europea para la Ciberseguridad

ICS: Industrial Control Systems (Sistemas de Control Industrial)

ICE: Infraestructura Crítica Europea

ICN: Infraestructura Crítica Nacional

IoT: Internet of Things (Internet de las Cosas)

NAA: Nivel de Alerta Antiterrorista

NIS: Network and Information Security

PES: Plan Estratégico Sectorial

PIC: Protección de Infraestructuras Críticas

PNPIC: Plan Nacional de Protección de Infraestructuras Críticas

PSO: Plan de Seguridad del Operador

SCADA: Supervisory Control and Data Acquisition

TE-SAT: EU Terrorism Situation and Trend Report

ENCOT: Estrategia Nacional contra el Terrorismo

1. INTRODUCCIÓN

El terrorismo ha experimentado una transformación radical a lo largo de los años, tanto en su naturaleza como en los objetivos que elige perseguir. Los ataques terroristas en el siglo XX se centraban predominantemente en un pequeño porcentaje de personas: líderes políticos, profesionales militares o civiles en instalaciones públicas. Sin embargo, hoy en día, la tendencia actual es un aumento en el número de ataques a infraestructuras y sistemas vitales que permiten el desarrollo y la vida de un estado moderno. Esta progresión estratégica no es accidental; responde a una lógica de maximización del impacto que los grupos terroristas y militantes han venido perfeccionando con el tiempo: interrumpir los fundamentos materiales de la sociedad genera un impacto desestabilizador y psicológico mucho mayor que el de los ataques convencionales, de alta visibilidad pero de bajo impacto estructural. Esto no es una sorpresa para España.

El 11 de marzo de 2004, cuando varios trenes de cercanías que operaban a través de la red de Renfe en Madrid fueron destruidos y 193 personas murieron y más de 2,000 resultaron heridas, esto constituyó el ataque terrorista más devastador a la infraestructura de transporte de España. En ese momento, el sistema de protección de infraestructuras críticas estaba en su infancia, pero el evento catalizó un proceso legislativo y organizativo que resultó en la aprobación de la Ley 8/2011, de 28 de abril, el primer cuerpo regulador integral a nivel nacional. Hasta ahora, la experiencia acumulada ha permitido ensamblar un sistema de protección que ahora se enfrenta a desafíos cualitativos como resultado de los desafíos sobre los cuales se basó su creación.

En la primera mitad de la década de 2020, el contexto de amenaza en Europa había cambiado considerablemente. La agresión rusa en curso dirigida a Ucrania desde febrero de 2022 demostró la vulnerabilidad de la infraestructura energética europea a actores estatales hostiles a través del sabotaje de los gasoductos Nord Stream en septiembre de 2022. Y el terrorismo yihadista, particularmente vinculado a Daesh y Al Qaeda, sigue siendo una amenaza persistente en ese ámbito europeo, con células residuales activas y una preocupante capacidad de radicalización en línea para alimentar la figura del llamado "lobo solitario". Además, el radicalismo de derecha ha visto un resurgimiento preocupante dentro de muchas naciones de la Unión Europea, lo que hace que la aplicación más amplia de formas convencionales de amenaza terrorista sea más amplia, y no solo un llamado al yihadismo.

Este artículo pretende explorar desde un punto de vista multidisciplinario y académico la amenaza que los elementos terroristas representan para las infraestructuras críticas españolas. En busca de este objetivo, se examinará tanto en España la estructura reguladora de referencia nacional como también europea e internacional; se expondrán los sectores estratégicos más vulnerables; se escrutará el marco institucional de referencia del sistema CIP español; y se sugerirán mecanismos de mejora, destinados a aumentar la capacidad de resiliencia del sistema para las perspectivas de 2025 a 2030.

El estudio actual emplea una perspectiva integradora que yuxtapone el análisis legal con el lente de las ciencias de la seguridad y la criminología, creyendo que las complejidades del fenómeno demandan un enfoque plural y complementario. La hipótesis guía que dirige la investigación es la expresada de la siguiente manera: España tiene un sistema regulador robusto y un marco institucional que cubre infraestructuras críticas según los estándares europeos, pero también vulnerabilidades estructurales,

especialmente con respecto a la ciberseguridad industrial y la colaboración público-privada, que los actores terroristas podrían explotar en un contexto de amenaza creciente y diversificada.

Siguiendo esta hipótesis, el documento mostrará que la respuesta a esta amenaza necesita un nuevo enfoque, que implique no solo reformar el marco regulador actual para infraestructuras críticas, sino también replantear los modelos de gobernanza y la asociación entre el sector público y los operadores privados de infraestructuras críticas. Esta metodología particular se deriva del análisis documental de fuentes primarias — legislación, informes oficiales, documentos estratégicos — y fuentes secundarias — literatura académica especializada, informes de organizaciones internacionales — durante un período de referencia desde la aprobación de la Ley 8/2011 hasta 2025.

2. METODOLOGÍA

La investigación adopta un diseño cualitativo basado en el análisis documental sistemático, enfoque apropiado para el estudio de fenómenos jurídico-institucionales en los que la comprensión del marco normativo y conceptual resulta previa y necesaria respecto de cualquier valoración empírica. La brecha que el trabajo pretende cubrir reside en la ausencia de estudios que integren de forma articulada las tres dimensiones —legal, institucional y operativa— del sistema español de PIC frente a la amenaza terrorista, incorporando los desarrollos normativos europeos más recientes (Directiva CER y NIS2, ambas de 2022) y la nueva Estrategia Nacional contra el Terrorismo de 2023.

Las fuentes primarias comprenden: legislación nacional (Ley 8/2011, Real Decreto 704/2011, Ley Orgánica 4/2015, Real Decreto 311/2022 y Real Decreto 1150/2021); normativa europea (Directiva CER 2022/2557, Directiva NIS2 2022/2555 y Directiva 2008/114/CE); instrumentos internacionales (Resoluciones del Consejo de Seguridad de la ONU 1373/2001 y 2341/2017; CETS n.º 196); y documentos estratégicos oficiales (Estrategia de Seguridad Nacional 2021, ENCOT 2023, informes anuales del CNPIC). Las fuentes secundarias incluyen literatura académica especializada en seguridad nacional, protección de infraestructuras críticas y terrorismo, recuperada mediante búsqueda sistemática en las bases de datos Scopus, Web of Science y Google Scholar, con las palabras clave: “critical infrastructure protection”, “terrorism”, “hybrid threats”, “CIP Spain”, “infraestructuras críticas”, “terrorismo” y “resiliencia”; así como informes de organismos internacionales (Europol TE-SAT, ENISA Threat Landscape). Se aplicaron como criterios de inclusión: publicaciones en español o inglés, periodo 2001-2025, y pertinencia directa con el objeto de estudio. Quedaron excluidos los trabajos de carácter exclusivamente descriptivo sin aportación analítica o propositiva, así como fuentes no verificables o de difusión restringida.

3. MARCO CONCEPTUAL: ¿QUÉ SON LAS INFRAESTRUCTURAS CRÍTICAS?

La noción de "infraestructura crítica" no es inequívoca en la academia o en la regulación. A medida que las sociedades modernas han dependido más de ciertos sistemas o servicios críticos, su definición ha cambiado. Para los propósitos de este trabajo, bajo el alcance y los parámetros de la Ley 8/2011, la infraestructura crítica se refiere a instalaciones, redes, servicios y equipos de tecnología de la información y comunicación cuya interrupción o destrucción tendría un impacto significativo en la salud, seguridad o bienestar económico

de los ciudadanos, o en el funcionamiento efectivo de las instituciones del Estado y las Administraciones Públicas. Esta definición indica una visión del impacto potencial que se centra no tanto en la naturaleza de la infraestructura, sino más bien en las consecuencias de su fallo o destrucción para la sociedad en su conjunto.

3.1. CLASIFICACIÓN SECTORIAL

El Artículo 2 del Real Decreto 704/2011 identifica doce sectores estratégicos sujetos a protección bajo el sistema PIC español: administración, agua, alimentación, energía, espacio, industria nuclear, industria química, instalaciones de investigación, salud, sistema financiero y tributario, tecnologías de la información y la comunicación (TIC), y transporte. Esta categorización es consistente con la descripción dada en la Directiva (UE) 2022/2557 (Directiva CER), que amplía el conjunto de sectores a once, y que define explícitamente la infraestructura digital, el espacio y la administración pública como categorías específicas.

La ponderación relativa en términos de seguridad de los sectores es diferente para distintos tipos de amenazas y las posibles consecuencias de una interrupción, pero en esencia, los sectores de energía, transporte y TIC están en el contexto español relativamente concentrados en cuanto a sus activos clave. Basado en datos proporcionados por el CNPIC, España cuenta con más de 3,700 operadores críticos designados que se dividen entre los doce sectores estratégicos, siendo los sectores de TIC y energía los que concentran el mayor número de operadores en términos absolutos.

3.2. INFRAESTRUCTURA CRÍTICA NACIONAL E INFRAESTRUCTURA CRÍTICA EUROPEA

La diferencia entre la infraestructura crítica nacional (ICN) y la infraestructura crítica europea (ICE) es especialmente relevante a la luz de la legislación de la UE. Una infraestructura se denomina ICE si su interrupción o destrucción afectaría gravemente a dos o más estados miembros, o a la UE en su conjunto. La Directiva 2008/114/CE fue la primera en establecer este concepto; inicialmente restringió su alcance a los sectores de energía y transporte. La Directiva CER de 2022 amplía el alcance del concepto y refuerza los medios para identificar y proteger estas infraestructuras. España ha establecido varias de estas instalaciones como ICE, principalmente en los sectores de energía y transporte, dado el papel estratégico del país como corredor de energía y comunicaciones entre Europa y el norte de África, una posición geopolítica que, si bien otorga a España un papel central en la arquitectura de seguridad europea, aumenta su exposición a ciertas amenazas transnacionales.

3.3. EL CONCEPTO DE INTERDEPENDENCIA

Un tema central del análisis de infraestructuras críticas es el problema de la interdependencia. Los sistemas críticos de hoy en día no funcionan solos; dependen mucho de otros sistemas de los cuales dependen para su operación. La industria eléctrica depende de las infraestructuras de telecomunicaciones para su gestión automatizada; el transporte ferroviario se alimenta de energía eléctrica; y el sector financiero depende de las TIC para prácticamente todas sus operaciones. Tal interdependencia crea lo que la literatura especializada denomina "efectos en cascada": el fallo de una infraestructura

puede causar el fallo sucesivo de otras con un eventual resultado devastador para todo el sistema (Rinaldi et al., 2001).

La profundización de la digitalización de los sistemas críticos —vinculada a las tecnologías IoT, plataformas de datos en la nube y sistemas de control industrial SCADA— ha amplificado estas interdependencias, dando lugar a nuevos vectores de vulnerabilidad que grupos terroristas más sofisticados están comenzando a explotar sistemáticamente. Esta interdependencia no es únicamente una cuestión de naturaleza técnica o cibernética; involucra aspectos geográficos —infraestructuras transfronterizas como redes eléctricas o gasoductos—, cibernéticos —sistemas de control compartidos o interconectados— y organizacionales —operadores que gestionan activos en numerosos sectores.

La naturaleza multifacética de tal interdependencia hace que el análisis del riesgo de infraestructuras críticas sea un proceso de inmensa complejidad que no puede reducirse a examinar cada infraestructura de manera independiente.

4. MARCO NORMATIVO DE REFERENCIA

La protección de las infraestructuras críticas contra amenazas terroristas y otras amenazas intencionales se estructura a través de un complejo marco regulatorio multinivel, que incluye disposiciones nacionales, europeas e internacionales. Esta arquitectura regulatoria también representa la comprensión creciente de que la amenaza a las infraestructuras críticas trasciende las fronteras nacionales y requiere respuestas coordinadas en diferentes niveles de gobernanza. Cada uno de estos niveles se discute en secciones posteriores con un enfoque en los últimos desarrollos regulatorios y los desafíos que plantea su implementación.

4.1. NORMATIVA ESPAÑOLA

La Ley 8/2011, de 28 de abril, forma la base de la legislación nacional española sobre la protección de infraestructuras críticas. Esta ley transpone la Directiva 2008/114/CE al derecho español y establece el Sistema de Protección de Infraestructuras Críticas, una herramienta que se basa en tres principios fundamentales: el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), el Catálogo Nacional de Infraestructuras Estratégicas y la planificación de la protección. Distingue entre el Plan Nacional de Protección de Infraestructuras Críticas (PNPIC), los Planes Estratégicos Sectoriales (PES) y los Planes de Seguridad del Operador (PSO) en el marco legal de España y proporciona un plan "escalonado y de alto nivel" que se desarrolla desde el nivel general hasta el específico. El desarrollo normativo de la Ley PIC se lleva a cabo mediante el Real Decreto 704/2011, de 20 de mayo, que afirma la aplicación para la protección de infraestructuras críticas.

Esta regulación establece los criterios para la designación de operadores críticos, el contenido mínimo de los Planes de Seguridad del Operador y los Planes de Protección Específicos, y las responsabilidades de comunicación respecto a incidentes. Especialmente relevante es el Artículo 24 que establece el régimen de inspección/supervisión para los operadores críticos, lo que a su vez permite al CNPIC verificar el cumplimiento de las obligaciones de seguridad. Varios autores han destacado cómo esta supervisión del cumplimiento en la práctica ha sido señalada como una

debilidad del sistema con un gran número de operadores y recursos limitados para la administración operativa. La Estrategia de Seguridad Nacional de 2021, según la autorización del Real Decreto 1150/2021, identifica el terrorismo como uno de los riesgos centrales de preocupación y amenazas para España, y considera la protección de infraestructuras críticas como un enfoque de objetivos ambiciosos del sistema de seguridad nacional bajo el enfoque holístico de seguridad que caracteriza al sistema español.

En consonancia con esto, la Estrategia Nacional contra el Terrorismo (ENCOT) de 2023 —que actualiza y sustituye a la versión de 2019— estructura la respuesta antiterrorista del Estado en torno a cuatro pilares de acción (prevenir, proteger, perseguir y responder) y sitúa la protección de infraestructuras críticas en el núcleo del pilar de "proteger". La ENCOT 2023 introduce una novedad conceptual de primer orden al asumir institucionalmente que la invulnerabilidad absoluta es inalcanzable, desplazando el foco estratégico desde la mera protección estática hacia la resiliencia integral, entendida como la capacidad de absorber el impacto de un incidente, garantizar la continuidad de los servicios esenciales y restaurar la normalidad con celeridad. Esta visión se alinea plenamente con el enfoque de la Directiva CER de 2022, lo que convierte a la ENCOT 2023 en un puente doctrinal entre la estrategia antiterrorista nacional y el marco europeo de entidades críticas. Además, la ENCOT 2023 advierte sobre el desplazamiento de la amenaza hacia denominados "objetivos blandos" —lugares de culto, celebraciones multitudinarias y espacios públicos— que, sin constituir infraestructuras críticas en sentido técnico, resultan determinantes para la seguridad ciudadana; una realidad que interpela directamente al ámbito de aplicación de la futura legislación de transposición. En términos de ciberseguridad, el Esquema Nacional de Seguridad, aprobado mediante el Real Decreto 311/2022, prescribe requisitos mínimos en los sistemas de información de las Administraciones Públicas y sus operadores de servicios esenciales, completando así el régimen PIC en lo relativo a los activos de información de los operadores críticos.

La Ley Orgánica 4/2015, de 30 de marzo, sobre la Protección de la Seguridad Ciudadana, introduce medidas relevantes de control de acceso a instalaciones sensibles y vigilancia de entornos de riesgo, complementando el sistema de protección física proporcionado por las regulaciones PIC.

4.2. NORMATIVA EUROPEA

El marco regulatorio de la Unión Europea ha sido revisado a fondo tras la aprobación de la Directiva (UE) 2022/2557 (14 de diciembre de 2022) sobre la resiliencia de las entidades críticas (Directiva CER). Esta regulación reemplaza a la Directiva 2008/114/CE y crea un marco reconceptualizado que se centra más bien en la resiliencia integral de las entidades que operan infraestructuras, en lugar de solo en la provisión física y protección de los sistemas, definida como su capacidad para evitar incidentes, soportar su impacto, responder a las consecuencias y recuperarse rápidamente. Los desarrollos clave en la Directiva CER incluyen la ampliación del ámbito sectorial de dos sectores a once, la necesidad de requisitos fortalecidos sobre análisis de riesgos e informes de incidentes, y el establecimiento de un mecanismo de la UE para apoyar a los Estados miembros en la identificación de entidades críticas, aquellas con particular relevancia europea.

La fecha límite para la transposición de la Directiva CER fue el 17 de octubre de 2024. España no había completado este procedimiento hasta ese momento, dejándola en

una situación de incumplimiento que podría llevar a un proceso de infracción por parte de la Comisión Europea si se prolonga. Este retraso es resultado de la complejidad técnica y política que implica una transposición que conlleva enmendar o derogar la Ley 8/2011 y su reglamento de aplicación, así como una revisión del Catálogo Nacional de Infraestructuras Estratégicas para adaptarlo a los nuevos sectores cubiertos y reformar los mecanismos de cooperación interministerial e intersectorial.

La Directiva NIS2 (Directiva (UE) 2022/2555), que fue aprobada el mismo día que la Directiva CER, revisa y deroga la Directiva NIS de 2016 y establece medidas para mantener un alto nivel común de ciberseguridad en toda la UE. Amplía enormemente el rango de regulaciones de ciberseguridad, pasando de "operadores de servicios esenciales" a "entidades esenciales e importantes", e implica responsabilidades fortalecidas basadas en la gestión de riesgos, informes de incidentes y cooperación transfronteriza.

La interacción entre la Directiva CER y la NIS2 es uno de los aspectos más complicados de este nuevo marco europeo: ambas directivas se aplican a muchas de las mismas entidades, sin embargo, desde diferentes perspectivas, con (1) resiliencia física integral y (2) ciberseguridad, y por lo tanto, un enfoque hacia ellas que requeriría coordinación durante la transposición para evitar superposiciones y contradicciones.

4.3. MARCO INTERNACIONAL

En la escena internacional, la Resolución 1373 (2001) del Consejo de Seguridad de las Naciones Unidas establece las obligaciones de todos los Estados en la lucha contra el terrorismo, que incluyen requisitos para implementar medidas que prevengan el uso de su territorio para actividades terroristas y el intercambio de información con otros Estados.

La Resolución 2341 (2017) del Consejo de Seguridad es el primer instrumento de este organismo específicamente dedicado a la protección de infraestructuras críticas contra el terrorismo, instando a los Estados a desarrollar medidas de protección proporcionales al riesgo identificado, promoviendo la cooperación internacional en relación con la dimensión cibernética de la amenaza. La Convención para la Prevención del Terrorismo (CETS No. 196), en vigor desde 2007, y su Protocolo Adicional de 2015 crean obligaciones sobre la criminalización y la cooperación judicial que complementan el marco de la ONU.

5. EL TERRORISMO COMO AMENAZA ESPECÍFICA CONTRA INFRAESTRUCTURAS CRÍTICAS

5.1. TIPOLOGÍA DE GRUPOS TERRORISTAS CON INTERÉS EN INFRAESTRUCTURAS CRÍTICAS

El fenómeno terrorista se erige, por tanto, como una de las amenazas más complejas y multifacéticas para las infraestructuras esenciales de la sociedad contemporánea. A diferencia de otras amenazas como los desastres naturales o los fallos tecnológicos accidentales, el terrorismo presenta una intención maliciosa y una racionalidad estratégica, lo que significa que los terroristas adaptan y renuevan sus tácticas, técnicas y procedimientos en función de las medidas de protección desplegadas. Una respuesta protectora eficaz exige, por ello, una reacción igualmente dinámica y proactiva ante la

naturaleza adaptativa de la amenaza, que no puede limitarse a medidas de seguridad físicas y lógicas de carácter estático.

5.1.1. Terrorismo yihadista

El terrorismo inspirado por yihadistas, particularmente asociado con grupos como Daesh y Al Qaeda, ha expresado repetidamente su interés estratégico en atacar infraestructuras clave en países occidentales. Los folletos, publicados por ejemplo en Dabiq o Inspire, ambos grupos han incluido orientación explícita para atacar plantas de energía, fuentes de agua potable e instalaciones de transporte en Europa y América del Norte, prestando especial atención a los efectos en cadena de interrumpir infraestructuras interconectadas.

En España, más específicamente, el ataque (en agosto de 2017) de La Rambla en Barcelona y Cambrils por una célula de Daesh reflejó cómo la amenaza yihadista seguía presente a nivel nacional, aunque, esta vez, su propósito era infligir bajas en el espacio público en lugar de atacar una infraestructura específica. Según el informe TE-SAT 2024 de Europol, el terrorismo yihadista sigue siendo la amenaza más grave para la Unión Europea en términos de número de operaciones, arrestos y ataques cometidos o bloqueados.

En este contexto, España opera en una posición especialmente vulnerable: su estatus como país de tránsito entre el norte de África y Europa, los flujos migratorios que atraviesan sus fronteras del sur, y la presencia de comunidades con grados documentados de radicalización. El modelo de “lobo solitario”, que actúa de manera autónoma una vez radicalizado a través de vías digitales, enfrenta desafíos únicos de detección temprana, y actualmente es el perfil más probable de ataques terroristas inspirados por yihadistas en suelo español.

5.1.2. Actores estatales hostiles y amenazas híbridas

Esta clase de actores estatales hostiles merece una consideración especial dentro del ámbito de las amenazas a la infraestructura crítica. El cuerpo de evidencia recopilado desde 2014 sugiere que Rusia ha desarrollado y desplegado capacidades avanzadas para sabotear la infraestructura crítica en Europa, a través de medios cibernéticos directos (incluidos ataques por parte del grupo Sandworm contra la red eléctrica ucraniana en 2015 y 2016) y mediante actividades encubiertas de sabotaje físico.

El más espectacular es el sabotaje de los gasoductos Nord Stream en septiembre de 2022, que cortó el suministro de gas natural a Europa desde Rusia y demuestra la disposición de los actores estatales para atacar la infraestructura de Europa con la intención de utilizarlo como una palanca geopolítica.

El concepto de "amenaza híbrida" se refiere a la combinación de una serie de herramientas tradicionales y fuera de lo común, incluyendo desinformación, ciberataques, sabotaje físico y presión económica, para crear una "estrategia de amenaza híbrida" integrada diseñada para debilitar a un estado sin cruzar a la categoría de confrontación armada convencional. Este tipo de amenaza, en la que Rusia ha utilizado su perfil de amenaza como la fuerza más activa en Europa en los últimos años, presenta una dificultad particular para los sistemas cuyo objetivo principal es proteger la infraestructura crítica donde la amenaza subyacente se aborda como amenazas tradicionales individuales. Irán

y Corea del Norte, que también son vistos por expertos como atacantes cibernéticos de infraestructura crítica, han demostrado tener capacidades de ciberataque contra infraestructura crítica, aunque su peligro real para el suelo español ahora se considera menos sustancial que la amenaza rusa.

5.1.3. Terrorismo de extrema derecha

Aunque el terrorismo de extrema derecha generalmente no se centra en atacar infraestructuras como el terrorismo yihadista, se ha vinculado a varios incidentes graves en Europa en los últimos años. Los ataques en Utøya (Noruega, 2011), Hanau (Alemania, 2020) y Christchurch (Nueva Zelanda, 2019) han destacado la capacidad letal de estos tipos de actores.

En el ámbito de la infraestructura crítica, algunas células extremistas de derecha han mostrado interés en atacar infraestructuras de comunicación, energía o transporte como una forma de desestabilizar la sociedad y provocar un colapso del orden establecido, lo que estos grupos denominan "aceleración". Este fenómeno es reconocido como una amenaza emergente por la Estrategia de la UE para la Unión de la Seguridad 2020-2025, que sostiene que en el área de inteligencia, así como en las herramientas regulatorias, debe ser tratado y abordado con la misma seriedad que el terrorismo yihadista.

5.2. CASOS HISTÓRICOS RELEVANTES

El ataque del 11 de marzo de 2004 en Madrid sigue siendo sin duda el caso de referencia en España. Durante las horas punta de la mañana, la detonación coordinada de diez explosivos en trenes de cercanías fue una explotación de las vulnerabilidades inherentes de los sistemas de transporte masivo; son abiertos, los usuarios están concentrados y es difícil implementar una infraestructura de seguridad integral sin sacrificar la eficiencia del servicio. El ataque resultó en 193 muertes y más de 2,000 heridos y tuvo un gran impacto económico y social (Reinares, 2014). No solo fue inmediatamente efectivo: el 11 de marzo expuso la infraestructura de transporte ferroviario como poseedora de vulnerabilidades estructurales que no habían sido suficientemente consideradas en los planes de seguridad de la época. En términos europeos, el ataque de 2016 en Bruselas, que involucró la explosión de dispositivos en el Aeropuerto Internacional de Zaventem y dentro del metro de la ciudad, demuestra cómo los terroristas son capaces de atacar dos o más nodos de infraestructuras de transporte de una sola vez, dándoles el máximo efecto psicológico y mediático.

Un aeropuerto internacional se considera un objetivo deliberado: este tipo de aeropuerto concentra grandes volúmenes de individuos de diferentes nacionalidades en lugares únicos, que tienen una alta atención mediática internacional, tanto que su interrupción crea efectos económicos y de imagen desproporcionados al costo material del ataque. En el contexto español, una serie de sabotajes a infraestructuras de fibra óptica reportados en varias comunidades autónomas en 2024 subrayaron la susceptibilidad de las redes de telecomunicaciones hacia actos intencionados de destrucción; demostrando que la desactivación de infraestructuras vitales se puede llevar a cabo con técnicas técnicas relativamente sencillas donde los activos tienen una protección física inadecuada.

5.3. EL CIBERTERRORISMO Y LOS ATAQUES HÍBRIDOS COMO NUEVA FRONTERA

El ciberterrorismo, definido como el uso intencional de capacidades informáticas (para intimidación o presión política) para causar estragos en infraestructuras críticas, es el aspecto más nuevo, y posiblemente más disruptivo, del ataque terrorista contra infraestructuras de alto valor. Y a diferencia del terrorismo tradicional, los ciberataques pueden llevarse a cabo desde la distancia, en algunos casos sin ser identificables, y desde diferentes áreas, lo que hace que la atribución y el control sean un desafío mucho más complicado para las autoridades.

La interconexión y fusión del ciberespacio y el control industrial ha llevado a lo que algunos llaman el "quinto dominio de la guerra" (Clarke y Knake, 2010), donde los terroristas son capaces de infligir daños físicos reales a estructuras críticas sin tener que estar cerca de ellas. El ataque de Estados Unidos al Colonial Pipeline (mayo de 2021) utilizando ransomware subrayó cuán indefensas son las infraestructuras energéticas críticas ante tales ciberataques y la rapidez con la que tales ataques pueden llevar a escasez de suministros y alarma social.

En Europa, los ciberataques a la compañía eléctrica ucraniana Ukrenergo en 2015 y 2016, ejecutados por individuos asociados con el estado ruso, dejaron grandes áreas de Ucrania sin electricidad durante varias horas, un presagio de que los ataques a la infraestructura energética en Europa podrían surgir en un momento de creciente conflicto geopolítico.

Según la encuesta ENISA Threat Landscape 2024, la ciberamenaza a las infraestructuras industriales en sectores esenciales ha aumentado en Europa un 78% de 2022 a 2023, demostrando las tendencias crecientes en este tipo de ataques.

6. VULNERABILIDADES DE LAS INFRAESTRUCTURAS CRÍTICAS ESPAÑOLAS

En un esfuerzo por analizar las vulnerabilidades en el sistema de infraestructura crítica española frente a la amenaza terrorista, el enfoque debe ser sectorial —teniendo en cuenta las características específicas de cada sector estratégico— y un enfoque transversal, que identifique las debilidades estructurales comunes a todo el sistema. Las secciones a continuación abordan primero las vulnerabilidades específicas de los sectores de mayor riesgo, seguidas de un examen de los factores transversales de vulnerabilidad.

6.1. ANÁLISIS SECTORIAL DE VULNERABILIDADES

6.1.1. Sector Energético

El sector energético representa uno de los objetivos prioritarios para los grupos terroristas sofisticados debido a la magnitud del impacto potencial de un ataque exitoso. España opera una red eléctrica de alta tensión, que conecta el sistema peninsular con las Islas Canarias y Baleares y con Francia y Portugal a través de los interconectores pirenaicos, y es operada por Red Eléctrica de España (REE). La concentración de activos cruciales en algunos nodos de la red — plantas de generación, centros de despacho de carga o transformadores de alta tensión — y su reemplazo tras daños severos que lleva meses,

crea vulnerabilidades particulares a ataques físicos o cibernéticos coordinados. Además, las plantas nucleares existentes y operativas en España — Almaraz, Ascó, Cofrentes, entre otras — necesitan protección a diferentes niveles debido a los efectos potencialmente catastróficos de incidentes en los sitios, pero su seguridad física así como radiológica es monitoreada en todo momento por el Consejo de Seguridad Nuclear (CSN).

6.1.2. Sector del Transporte

España cuenta con una de las redes de trenes de alta velocidad más extensas del mundo, con más de 3,900 kilómetros de líneas de alta velocidad operativas. Esta infraestructura, con la concentración de pasajeros en grandes estaciones — Atocha, Sants, Santa Justa — más ciertos elementos que la hacen susceptible como túneles, viaductos, sistemas de señalización, representa objetivos principales para que los terroristas se aprovechen. El Aeropuerto Adolfo Suárez Madrid-Barajas, el cuarto aeropuerto más concurrido de Europa con más de 62 millones de pasajeros anuales, y el Puerto de Algeciras, el principal puerto de contenedores de España y una puerta de entrada para mercancías de África del Norte, tienen características de alto riesgo que exigen medidas de seguridad particularmente rigurosas.

6.1.3. Sector TIC

La infraestructura digital de España ha crecido rápidamente en los últimos años debido a la digitalización de la economía, así como al 5G y la aplicación de infraestructuras de computación en la nube. Los cables de comunicaciones submarinos que conectan a España con el resto del mundo — incluidos aquellos que enlazan la Península Ibérica con las Islas Canarias y el continente americano — también se han erigido en un vector de vulnerabilidad de primer orden, tal como constatan los incidentes registrados en el mar Rojo y el Báltico entre 2023 y 2025. Estos cables concentran la mayor parte del tráfico internacional de datos y voz, y su daño intencionado podría llevar a una pérdida de capacidad de comunicación a escala continental. Dada la dispersión geográfica de los activos TIC y la rápida evolución tanto de las tecnologías como de los vectores de ataque, el CNPIC señaló que el sector TIC plantea algunos de los desafíos más urgentes en cuanto a protección.

6.2. RIESGOS DERIVADOS DE LA DIGITALIZACIÓN Y LA CONECTIVIDAD

La adopción de tecnologías de la información (TI) y tecnologías operativas (OT) en contextos industriales es una de las tendencias más importantes—y más preocupantes desde una perspectiva de seguridad—de los últimos diez años. La llamada "brecha de aire" entre los sistemas de control industrial (ICS/SCADA) y las redes corporativas e internet ha provocado una integración gradual de los sistemas TI dentro de entornos digitales para mejorar la eficacia operativa y la gestión de reparaciones remotas.

Esta conectividad crea nuevas superficies de ataque que pueden ser explotadas por grupos terroristas con capacidades cibernéticas avanzadas. El número de dispositivos IoT instalados como clave para sistemas críticos—como: sensores de temperatura, cámaras de seguridad y sistemas de control de acceso—exacerba la amenaza al incluir componentes que no son inherentemente seguros cuando se integran en sistemas operativos críticos para la seguridad. La ausencia de actualizaciones de seguridad de

dispositivos integrados, la existencia de protocolos de comunicación industrial antiguos sin capacidades criptográficas y la falta de expertos profesionales en ciberseguridad dentro del sector industrial aumentan severamente este nivel de vulnerabilidad.

6.3. COORDINACIÓN PÚBLICO-PRIVADA: EL RETO PENDIENTE

Una característica sistémica del sistema de infraestructura crítica de España que ha creado vulnerabilidades específicas es que la mayoría de los operadores críticos son de propiedad privada. De los aproximadamente 3,700 operadores designados en España, la mayoría son entidades privadas o mixtas, lo que representa un desafío continuo para los intereses privados que enfatizan las ganancias y la eficiencia sobre la seguridad nacional.

En este sentido, y en el contexto de estas obligaciones, en combinación con la provisión de la Ley PIC, los operadores críticos deben elaborar Planes de Seguridad del Operador y Planes de Protección Específicos para su operación, pero la inversión realizada hacia estos esquemas a menudo supera los requisitos mínimos de cumplimiento de la Ley PIC, al menos donde hay muy pocas razones económicas para aceptar tal suma de capital. El intercambio de información y la confianza mutua entre los sectores público y privado son destacados por la literatura especializada como componentes críticos para la efectividad del sistema PIC (Moteff, 2014).

Con respecto a esto, España ha establecido mecanismos para el intercambio de información y sistemas de alerta temprana a través del CNPIC, sin embargo, la integración completa de los operadores privados en el sistema de inteligencia de amenazas sigue siendo un área crítica donde el progreso no puede ser limitado. La asimetría de información entre las autoridades competentes, que pueden recurrir a inteligencia clasificada sobre amenazas, y los operadores privados, que requieren el conocimiento para calibrar sus inversiones en seguridad, es una de las barreras más duraderas para forjar una cooperación público-privada efectiva en el PIC.

7. EL SISTEMA ESPAÑOL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

7.1. ARQUITECTURA INSTITUCIONAL

El Sistema de Protección de Infraestructuras Críticas de España se basa en una estructura institucional complicada que vincula instituciones de diversos tamaños y especialidades. El CNPIC, dentro de la Secretaría de Estado de Seguridad del Ministerio del Interior, asume la posición de desarrollar, coordinar y supervisar el sistema. Es responsable de la regulación del Catálogo Nacional de Infraestructuras Estratégicas, el inventario clasificado del país sobre infraestructuras críticas, la planificación de esquemas de protección coordinados y el monitoreo del cumplimiento para los operadores críticos.

El CNPIC cuenta con la cooperación permanente del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), la institución encargada de proporcionar inteligencia antiterrorista e información sobre España, para proporcionar medidas de protección basadas en el riesgo que puedan contrarrestar. El Centro Nacional de Inteligencia (CNI), a través del Centro Criptológico Nacional (CCN) y su fuerza de respuesta a incidentes CCN-CERT, es el organismo competente en relación con la

ciberseguridad para las Administraciones Públicas y los sistemas de información de los operadores de servicios esenciales.

La complementariedad inherente en ambas funciones del CNPIC (enfocadas en la protección física y la planificación de la seguridad) y el CCN-CERT (enfocado en la ciberseguridad) es clave para la protección efectiva de las infraestructuras críticas frente a una amenaza que puede conceptualizarse tanto física como cibernética. La reciente coordinación operativa en ambas organizaciones ha evolucionado mucho y las ha visto unir fuerzas para desarrollar grupos de trabajo y protocolos para compartir información sobre incidentes de carácter mixto.

El Departamento de Seguridad Nacional (DSN) es responsable de la coordinación estratégica de todo el sistema de seguridad nacional, incluida la protección de infraestructuras críticas y está adscrito a la Presidencia del Gobierno. En materia de seguridad nacional, el DSN lleva a cabo el desarrollo y monitoreo de Estrategias de Seguridad Nacional y actúa como enlace con las herramientas de coordinación estratégica de la OTAN y la UE.

Las Fuerzas y Cuerpos de Seguridad del Estado —Cuerpo Nacional de Policía y Guardia Civil— y las Fuerzas Armadas, a través de sus unidades especializadas, completan el marco institucional con especialización nacional en protección física, intervención en incidentes graves y apoyo a las autoridades civiles. Merece especial atención el papel operativo de la Guardia Civil en este sistema. A través de sus unidades especializadas —en particular la Unidad Central Operativa (UCO), la Unidad de Cibercrímenes (UCC) y los Equipos de Activación de NBQR—, la Guardia Civil despliega capacidades específicas de respuesta ante incidentes físico-cibernéticos en infraestructuras críticas de naturaleza rural, industrial y de transporte, que son precisamente los entornos más expuestos a amenazas híbridas. La estrecha coordinación técnico-policial entre la Guardia Civil y el CNPIC se articula mediante protocolos de actuación conjunta que permiten activar, en función del nivel de alerta antiterrorista vigente, dispositivos específicos de protección de infraestructuras en los sectores de energía, transporte y agua. Esta complementariedad entre la capacidad de inteligencia táctica de las Fuerzas y Cuerpos de Seguridad y la función de coordinación estratégica del CNPIC constituye uno de los activos diferenciadores del modelo español de PIC en el contexto europeo comparado.

7.2. EL SISTEMA DE NIVELES DE ALERTA ANTITERRORISTA (NAA)

El Nivel de Alerta Antiterrorista (NAA) se refiere al mecanismo establecido para implementar medidas de protección que corresponden a la amenaza terrorista en ese momento. El NAA de cinco niveles que ha sido actualizado por la Resolución del Secretario de Estado de Seguridad en 2019 —que va desde 1 (bajo) hasta 5 (muy alto)— se complementa con un catálogo de medidas de seguridad aplicadas progresivamente para varios sectores estratégicos.

Desde junio de 2015, se ha aplicado en España el nivel 4 (alto), que comprende la implementación de estructuras de seguridad mejoradas para todos los sectores estratégicos, como controles en torno a infraestructuras de transporte, aumento de la vigilancia perimetral de instituciones clave y el despliegue de protocolos de comunicación prioritarios para incidentes.

La conexión entre el NAA y el sistema PIC se cumple a través de Planes de Respuesta, que determinan las acciones específicas que los operadores críticos deben tomar según el nivel de alerta actual. Esto permite una respuesta escalonada y coordinada a medida que varía el nivel de amenaza. Pero mantener el nivel de alerta 4 durante más de diez años podría llevar a una cierta "fatiga de alerta" por parte de los operadores críticos, cuyas medidas de protección asociadas con el nivel pueden convertirse en una rutina y parte insuficientemente vigilante de su trabajo.

La implicación es que se necesita revisar periódicamente el sistema de alerta y establecer mecanismos para evaluar la verdadera efectividad de todas las medidas tomadas.

7.3. COOPERACIÓN INTERNACIONAL

La dimensión internacional de la protección de infraestructuras críticas es cada vez más relevante en un contexto donde las amenazas son de naturaleza transnacional. España participa activamente en diversas iniciativas de cooperación multilateral en este ámbito. Dentro de Europol, la Red Atlas de Unidades de Intervención Especial facilita la cooperación operativa entre las fuerzas policiales de los estados miembros en situaciones de crisis terrorista que puedan afectar a infraestructuras críticas.

El Consejo Asesor de la Asociación para la Infraestructura Crítica de la UE (CP-ISAC) promueve el intercambio de información y mejores prácticas entre las autoridades nacionales y los operadores críticos europeos. En el marco de la OTAN, España participa en los mecanismos de protección de infraestructuras críticas de la Alianza, que se fortalecieron significativamente después de la cumbre de Madrid de 2022, reconociendo la resiliencia de las infraestructuras críticas como un elemento central de la defensa colectiva.

8. RETOS Y PROPUESTAS DE MEJORA

El análisis previo permite identificar los desafíos y brechas en el sistema español para la protección de infraestructuras críticas que requieren consideración urgente. Las propuestas elaboradas aquí están lejos de ser exhaustivas, pero sí delinean las líneas de acción más urgentes con el mayor potencial de cambio positivo para mejorar la resiliencia del sistema frente a la amenaza terrorista.

8.1. TRANSPOSICIÓN URGENTE DE LA DIRECTIVA CER

Por lo tanto, es necesario modificar el marco regulatorio de acuerdo con los términos de la Directiva CER al estándar necesario para mantener la coherencia del sistema español con el marco europeo y aprovechar al máximo los mecanismos de apoyo integrados en la Directiva.

Se recomienda encarecidamente la aprobación de esta legislación, con una ley de re-promulgación que cubra la protección de infraestructuras y entidades críticas que derogue la Ley 8/2011 y que fusione los elementos de la Directiva CER con las disposiciones de NIS2 en un único régimen regulatorio con mejoras significativas en los mecanismos para monitorear el cumplimiento por parte de los operadores. Esta nueva regulación debería implementar un sistema de incentivos —deducciones fiscales o acceso

preferencial a financiamiento público— para que los operadores privados inviertan voluntariamente en medidas para aumentar la resiliencia por encima de los mínimos legales. Por lo tanto, se hace necesario que la nueva ley requiera la participación activa de los operadores críticos en el proceso, de modo que se alinee formalmente con la realidad operativa de cada sector.

8.2. FORTALECIMIENTO DE LA CIBERSEGURIDAD INDUSTRIAL

La convergencia IT-OT en entornos críticos requiere una inversión continua en ciberseguridad industrial que supere el cumplimiento mínimo regulatorio. Se recomienda implementar un Plan Nacional de Ciberseguridad Industrial para estipular estándares específicos para los sistemas SCADA/ICS de operadores críticos, promover la certificación de componentes industriales con referencia al Reglamento (UE) 2019/881, y apoyar la actualización de sistemas heredados con vulnerabilidades conocidas. El CCN-CERT debería mejorar aún más su capacidad para apoyar a los operadores del sector privado crítico en ciberseguridad industrial creando equipos sectoriales especializados (energía, transporte y agua, como prioridad) que puedan proporcionar soporte técnico específico en caso de incidentes físicos-cibernéticos mixtos.

8.3. MEJORA DE LA COORDINACIÓN PÚBLICO-PRIVADA

La creación de plataformas sectoriales para el intercambio de información sobre amenazas, en línea con el modelo de los Centros de Intercambio y Análisis de Información de Estados Unidos (ISAC), representa una prioridad para mejorar la cooperación entre el sector público y los operadores privados. Estas plataformas, que deberían operar bajo el paraguas del CNPIC y con la participación del CCN-CERT y CITCO, permitirían un flujo bidireccional de información sobre amenazas, vulnerabilidades e incidentes que fortalecería la capacidad de respuesta de todo el sistema.

Una condición esencial para su efectividad es la adopción de un marco legal que garantice la confidencialidad de la información compartida por los operadores privados, eliminando el riesgo de que su divulgación genere responsabilidades legales o ventajas competitivas para sus competidores.

8.4. FORMACIÓN Y EJERCICIOS DE SIMULACIÓN

La resiliencia de las infraestructuras críticas frente a ataques terroristas depende en gran medida de la preparación del personal que las gestiona y protege. Se recomienda institucionalizar un programa nacional de formación en protección de infraestructuras críticas, con módulos específicos para operadores en diferentes sectores, y la ejecución anual de ejercicios de simulación de crisis que contemplen escenarios de ataques físicos-cibernéticos combinados. Estos ejercicios, que deberían involucrar simultáneamente a las autoridades competentes, fuerzas de seguridad y operadores críticos, permiten identificar brechas en los planes de respuesta, reforzar la coordinación entre los actores y mantener actualizada la cultura de seguridad de las organizaciones. El Centro Europeo de Excelencia para Contrarrestar Amenazas Híbridas (Hybrid CoE) en Helsinki es un socio relevante para el diseño e implementación de estos ejercicios en la dimensión transnacional.

8.5. INTELIGENCIA ANTICIPATORIA

Anticipar las amenazas terroristas contra infraestructuras críticas requiere fortalecer las capacidades de inteligencia estratégica del CITCO y el CNI, con especial atención al análisis de tendencias en las aspiraciones operativas de grupos terroristas y actores estatales hostiles contra objetivos de infraestructura. La integración de datos de fuentes abiertas, incluyendo el monitoreo sistemático de foros extremistas en la dark web y el análisis de publicaciones de organizaciones terroristas, debería sistematizarse como parte de la evaluación específica de amenazas contra cada sector estratégico.

El desarrollo de capacidades de inteligencia artificial aplicadas al análisis de amenazas contra infraestructuras críticas representa una línea de inversión prometedora, aunque su implementación debe ir acompañada de garantías legales adecuadas que salvaguarden los derechos fundamentales.

9. CONCLUSIONES

El análisis desarrollado en este documento nos permite extraer las siguientes conclusiones sobre la amenaza terrorista que se cierne sobre las infraestructuras críticas españolas y el estado actual del sistema de protección.

En primer lugar, España cuenta con un marco normativo e institucional para la protección de infraestructuras críticas, que en conjunto proporcionan un nivel de protección adecuado según los términos comparativos europeos. La Ley 8/2011 y su desarrollo normativo son la piedra angular de un sistema coherente que ha demostrado, durante más de diez años, su eficacia en la coordinación interinstitucional y la gestión de incidentes. Sin embargo, el retraso en la transposición de la Directiva CER de 2022 deja un vacío de incertidumbre normativa que deteriora la posición de España en el sistema europeo de protección de infraestructuras críticas y debe resolverse urgentemente mediante una nueva legislación que incorpore el enfoque de resiliencia integral que caracteriza al nuevo marco europeo.

En segundo lugar, el terrorismo yihadista sigue siendo la principal amenaza terrorista para las infraestructuras críticas españolas en cuanto a probabilidad de ocurrencia, tal como constatan la persistencia de células activas en el entorno español y la continua difusión de propaganda que promueve ataques contra objetivos de infraestructura en toda Europa. La ENCOT 2023 coincide en esta valoración, destacando el incremento de los actores solitarios que, tras procesos de autorradicalización en entornos digitales, ejecutan acciones con medios rudimentarios pero de alta letalidad —patrón que ilustran los atentados de Las Ramblas y Cambrils—, lo que supone un desafío mayorúsculo para los sistemas de detección temprana. Sin embargo, el peligro que representan los actores estatales hostiles —especialmente Rusia— y los ataques inspirados por extremistas de diversas orientaciones ideológicas debe abordarse con esfuerzos estratégicos comparables, habida cuenta de su potencial para causar daños catastróficos a las infraestructuras esenciales.

En tercer lugar, la digitalización y la convergencia IT-OT han transformado el panorama de vulnerabilidades para las infraestructuras críticas españolas y han creado nuevos vectores de ataque que los sistemas de protección existentes no siempre pueden neutralizar eficazmente. El fortalecimiento de la ciberseguridad industrial debe

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8979

considerarse una prioridad nacional de primer orden, que solo puede lograrse mediante inversiones sostenidas en tecnología, formación especializada y actualización de marcos normativos y estándares técnicos.

En cuarto lugar, la coordinación público-privada, aunque ha evolucionado considerablemente desde la adopción de la Ley 8/2011, sigue siendo un área crítica para mejorar en el sistema español. Los activos de infraestructuras críticas de propiedad privada requieren mecanismos más sofisticados para alinear incentivos e intercambiar información clasificada entre el sector público y los operadores, que solo pueden desarrollarse sobre la base de un marco legal que garantice la confianza y confidencialidad de todas las partes.

En quinto lugar, la cooperación internacional, no solo dentro del marco de la UE, sino también dentro de la OTAN y otros foros multilaterales, es un factor determinante en la efectividad del sistema de protección de infraestructuras críticas españolas. La ubicación de España como puerta de entrada entre Europa y el norte de África debería traducirse en un papel único en la arquitectura de seguridad europea, y por lo tanto, un compromiso específico con los mecanismos de cooperación multilateral existentes y el desarrollo de sus propias capacidades para proporcionar un valor diferencial a todo el sistema.

Debería haber futuras investigaciones en esta área para centrarse en el análisis sectorial de vulnerabilidades que emplee metodologías de evaluación de riesgos cuantitativos, el estudio comparativo de los modelos de transposición de la Directiva CER adoptados por los principales estados miembros de la Unión Europea, y la evaluación empírica de la efectividad de los mecanismos de coordinación público-privada existentes mediante metodologías de investigación primaria con operadores críticos.

10. REFERENCIAS BIBLIOGRÁFICAS

Arteaga, F. (2023). Infraestructuras críticas y seguridad nacional en España. *Real Instituto Elcano.* https://www.realinstitutoelcano.org

Boin, A. y McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management, 15*(1), 50-59. https://doi.org/10.1111/j.1468-5973.2007.00504.x

Clarke, R. A. y Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* HarperCollins.

Departamento de Seguridad Nacional. (2021). *Estrategia Nacional de Seguridad.* Presidencia del Gobierno de España.

ENISA. (2024). *ENISA Threat Landscape 2024.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Europol. (2023). *European Union Terrorism Situation and Trend Report (TE-SAT) 2023.* Publications Office of the European Union.

Europol. (2024). *European Union Terrorism Situation and Trend Report (TE-SAT) 2024.* Publications Office of the European Union. https://www.europol.europa.eu

Luiijf, E., Besseling, K. y De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures, 9*(1-2), 3-31. https://doi.org/10.1504/IJCIS.2013.052819

Masse, T. (2020). *Terrorism and Critical Infrastructure: Assessing the Threat.* Congressional Research Service.

Ministerio del Interior. (2023). *Estrategia Nacional contra el Terrorismo (ENCOT) 2023.* Secretaría de Estado de Seguridad. https://www.dsn.gob.es/es/publicaciones/estrategias-sectoriales/ENCOT2023

Moteff, J. D. (2014). *Critical Infrastructures: Background, Policy, and Implementation.* Congressional Research Service.

Reinares, F. (2014). Al-Qaeda y el 11-M en España. *Revista de Occidente, 400,* 75-95.

Reinares, F. y García-Calvo, C. (2022). *Terrorismo yihadista en España: Características y tendencias.* Real Instituto Elcano. https://www.realinstitutoelcano.org

Rinaldi, S. M., Peerenboom, J. P. y Kelly, T. K. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine, 21*(6), 11-25. https://doi.org/10.1109/37.969131

Weimann, G. (2015). *Terrorism in Cyberspace: The Next Generation.* Columbia University Press. https://doi.org/10.7312/weim16650

11. NORMATIVA

Naciones Unidas. Resolución 1373 (2001), de 28 de septiembre. Consejo de Seguridad de las Naciones Unidas. S/RES/1373 (2001).

Consejo de Europa. Convenio sobre Prevención del Terrorismo (CETS n.º 196). Varsovia, 16 de mayo de 2005. En vigor desde el 1 de junio de 2007.

Unión Europea. Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas. *Diario Oficial de la Unión Europea*, L 345, de 23 de diciembre de 2008.

España. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. *Boletín Oficial del Estado*, núm. 102, de 29 de abril de 2011.

España. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. *Boletín Oficial del Estado*, núm. 121, de 21 de mayo de 2011.

España. Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana. *Boletín Oficial del Estado*, núm. 77, de 31 de marzo de 2015.

Naciones Unidas. Resolución 2341 (2017), de 13 de febrero. Consejo de Seguridad de las Naciones Unidas. S/RES/2341 (2017).

España. Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia Nacional de Seguridad. *Boletín Oficial del Estado*, núm. 311, de 29 de diciembre de 2021.

España. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*, núm. 105, de 4 de mayo de 2022.

Unión Europea. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2). *Diario Oficial de la Unión Europea*, L 333, de 27 de diciembre de 2022.

Unión Europea. Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas (Directiva CER). *Diario Oficial de la Unión Europea*, L 333, de 27 de diciembre de 2022.