DEL RIESGO GLOBAL A LA LÓGICA DE ENEMIGO: POLÍTICA CRIMINAL Y AMENAZA HÍBRIDA NUCLEAR EN ESPAÑA

FROM GLOBAL RISK TO ENEMY LOGIC: CRIMINAL POLICY AND HYBRID NUCLEAR THREAT IN SPAIN

Elena Avilés Hernández*
Universidad de Málaga, Málaga, España
elenaavileshernandez@uma.es
Orcid id: https://orcid.org/0000-0001-5002-4252

Recibido: septiembre de 2025
Aceptado: octubre de 2025

Palabras Clave: Amenaza híbrida, terrorismo nuclear, Derecho penal del enemigo, política criminal, ciberseguridad, España.
Keywords: Hybrid threat, nuclear terrorism, criminal law of the enemy, criminal policy, cybersecurity, Spain.

Resumen: El presente artículo analiza la evolución de la política criminal española como respuesta a la "amenaza híbrida nuclear", un desafío estratégico que desdibuja las fronteras entre la paz y la guerra mediante el uso de la "zona gris" y vectores como los ciberataques. La hipótesis central es que, para hacer frente a este riesgo de naturaleza existencial, el Estado español ha configurado un modelo de seguridad que se aproxima a la lógica del "Derecho penal del enemigo". A través del estudio de la arquitectura legislativa y la ejecución penitenciaria, se examina cómo esta política criminal se materializa en un marcado adelantamiento de la punibilidad y en un régimen de excepción que prioriza la neutralización del sujeto peligroso sobre el fin resocializador. El análisis demuestra que este paradigma, si bien busca una prevención eficaz, genera profundas tensiones con los principios de proporcionalidad y las garantías del Estado de Derecho. Como conclusión, se proponen una serie de reformas para reconducir la respuesta estatal hacia un modelo más racional e integral.

Abstract: This article analyzes the evolution of Spanish criminal policy in response to the "hybrid nuclear threat," a strategic challenge that blurs the

* El presente trabajo ha sido realizado en el seno del proyecto de investigación "Derecho y protección radiológica del medio ambiente (DEPRAMA)", financiado por el Consejo de Seguridad Nuclear - Ministerio para la Transición Ecológica y el reto demográfico. Además, se enmarca en el Grupo de Investigación "Derecho Penal (SEJ116)" del Plan Andaluz de Investigación, dirigido por el Dr. Octavio García Pérez.

lines between peace and war through the use of the "gray zone" and vectors such as cyberattacks. The central hypothesis is that, to address this existential risk, the Spanish state has developed a security model that aligns with the logic of the "criminal law of the enemy." Through the study of the legislative architecture and penitentiary execution, this paper examines how this criminal policy materializes in a significant *anticipatory penal logic* and an exceptional regime that prioritizes the *pre-emptive incapacitation of high-risk subjects* over resocialization. The analysis demonstrates that this paradigm, while seeking effective prevention, creates profound tensions with the principles of proportionality and the guarantees of a State under the rule of law. In conclusion, a series of reforms are proposed to steer the state's response towards a more rational and comprehensive model.

1. La amenaza híbrida nuclear como desafío político-criminal

El panorama de la seguridad internacional del siglo XXI se define por una creciente complejidad y una difuminación de las fronteras tradicionales entre la paz y la guerra. En este contexto, la amenaza nuclear, lejos de desvanecerse con el fin de la Guerra Fría, ha mutado, adoptando formas más ambiguas y elusivas que desafían los paradigmas convencionales de la disuasión y la defensa. La emergencia de la "amenaza híbrida nuclear" representa un desafío político-criminal de primer orden para los Estados democráticos, obligándolos a reevaluar sus marcos de seguridad y sus ordenamientos jurídicos. Este nuevo paradigma de amenaza, caracterizado por la convergencia de actores, métodos y dominios de conflicto, genera una tensión fundamental entre la necesidad de una prevención eficaz y la salvaguarda de las garantías fundamentales del Estado de Derecho.

El presente artículo analiza el modelo de respuesta penal y político criminal adoptado por España frente a este desafío. Se parte de la hipótesis de que tanto las últimas estrategias de seguridad como la legislación antiterrorista española, especialmente tras la reforma operada por la Ley Orgánica 2/2015, transita hacia un modelo de "Derecho penal del enemigo". Este modelo, en su afán por neutralizar riesgos futuros, anticipa las barreras de punición, focaliza el reproche en la peligrosidad del sujeto más que en la lesividad del hecho y, en última instancia, erosiona principios fundamentales como la proporcionalidad, la legalidad y la presunción de inocencia. A través de un análisis de la regulación internacional, de los tipos penales y de la política criminal penitenciaria, se pretende demostrar cómo dicha lógica se materializa en el ordenamiento jurídico español, para concluir con una serie de propuestas orientadas a la construcción de una política criminal más racional, equilibrada e integral.

Para comprender la naturaleza del desafío político-criminal que plantea la amenaza híbrida nuclear, es imprescindible delimitar con precisión su marco conceptual. Dicha amenaza no se manifiesta como un acto singular y atribuible, sino como un fenómeno complejo que se desenvuelve en un espacio de ambigüedad estratégica conocido como la "zona gris". Baqués la define

como un escenario intermedio que no es ni la paz formal (zona "blanca", regida por la *bona fides* de las relaciones internacionales) ni la guerra abierta (zona "negra", ya sea convencional o híbrida). Se trata de un espacio de conflicto deliberadamente ambiguo donde los actores, tanto estatales como no estatales, persiguen objetivos geopolíticos disruptivos -equivalentes a los de una campaña militar- mediante instrumentos que operan al límite de la legalidad internacional, evitando cruzar el umbral que desencadenaría una respuesta militar convencional (2017: 26).

Este concepto se relaciona estrechamente con el de "guerra híbrida" (*Hybrid Warfare*), popularizado por Hoffman. Mientras que ésta última implica una "fusión de armas convencionales, tácticas irregulares, actos terroristas y desorden criminal" en un mismo campo de batalla, la zona gris opera en una fase previa o paralela, sin llegar necesariamente al empleo abierto de la fuerza armada (2007: 7-8). Ambos conceptos se engloban bajo el paraguas más amplio de la "amenaza híbrida" (*Hybrid Threat*), que la Unión Europea define como una "mezcla de actividades coercitivas y subversivas, y de métodos convencionales y no convencionales (es decir, diplomáticos, militares, económicos, tecnológicos, etc), que pueden ser utilizados de forma coordinada por agentes estatales o no estatales para lograr objetivos específicos" (High Representative of the Union for Foreign Affairs and Security Policy, EU, 2016: 2).

Mediante la operatividad en esta zona gris, se busca forzar los márgenes del sistema jurídico y político de las democracias liberales, utilizando sus propias reglas en su contra. Estos sistemas se fundamentan en una clara distinción binaria entre un estado de "paz", regido por el derecho civil y el pleno ejercicio de las libertades, y un estado de "guerra", que activa mecanismos legales de excepción y el Derecho Internacional Humanitario. Dicha zona se instala en la ambigüedad entre ambos, utilizando la desinformación, la presión económica, los ciberataques o el fomento de la agitación social para erosionar el *statu quo* sin ofrecer un motivo claro para una respuesta militar (Jordán Enamorado, 2022: 73). Esta ambigüedad no es un efecto secundario, sino el arma principal, diseñada para paralizar la toma de decisiones y forzar al Estado objetivo a un dilema irresoluble: o bien no responder y permitir la erosión de su soberanía y estabilidad, o bien reaccionar con medidas que podrían ser consideradas desproporcionadas o ilegítimas bajo su propio marco legal.

Un elemento crucial de esta nueva amenaza es la convergencia entre actores terroristas y redes de crimen organizado. La "guerrilla económica" propia de la zona gris puede ser potenciada por el uso de redes de delincuencia organizada afines para llevar a cabo sabotajes, manipular cadenas de suministro o intimidar a la población. A estas tácticas se suman los cortes de suministros de productos tan relevantes como las fuentes de energía (o la mera amenaza de llevarlos a cabo), así como la manipulación de sus precios. Esta simbiosis dota a los grupos terroristas de capacidades logísticas, financieras y operativas que de otro modo no poseerían, al tiempo que difumina aún más las líneas de atribución (Baqués, 2017: 22).

El verdadero peligro de esta simbiosis se magnifica cuando su lógica híbrida se aplica al dominio nuclear, dando lugar a la llamada "amenaza híbrida nuclear", la cual podría definirse como la convergencia de tres vectores interrelacionados:

1. El despliegue en la denominada zona gris, entendida como un espacio estratégico de ambigüedad entre paz y guerra.
2. La convergencia de agentes estatales y no estatales (incluyendo terroristas y redes criminales) que emplean de forma coordinada tanto métodos convencionales como irregulares.
3. La dimensión nuclear o radiológica, que introduce un potencial de riesgo catastrófico con capacidad disruptiva global.

Como se desprende de lo anterior, la amenaza no consiste tanto en la detonación de un arma atómica estatal, sino en el riesgo mucho más plausible de que los mencionados actores no estatales -como los mismos grupos terroristas, apoyados por sus redes criminales o por un Estado- adquieran y utilicen materiales nucleares o radiológicos.

En este sentido, la Resolución 1540 (2004) del Consejo de Seguridad de la ONU, adoptada bajo el Capítulo VII de la Carta, reconoce explícitamente esta amenaza al imponer a todos los Estados la obligación vinculante de adoptar medidas para "prohibir a los agentes no estatales la fabricación, la adquisición, la posesión, el desarrollo, el transporte, la transferencia o el empleo de armas nucleares, químicas o biológicas y sus sistemas vectores" (Resolución 1540(2004), aprobada por el Consejo de Seguridad en su 4956ª sesión, celebrada el 28 de abril de 2004. Doc. S/RES/1540(2004), 2004: 3). Este instrumento constata a nivel internacional la existencia de un nuevo desafío que fusiona el terrorismo, la proliferación y las tácticas de la zona gris.

Resulta crucial, por tanto, diferenciar las amenazas híbridas de las nucleares tradicionales. Mientras que estas últimas responden a la lógica interestatal clásica del equilibrio del terror y el control de arsenales, las primeras se caracterizan por la participación de actores no estatales y la opacidad en la atribución y el uso de métodos indirectos que desbordan los marcos convencionales. Es precisamente esta distinción la que define la relevancia del análisis, cuyo objeto no es tanto la estrategia nuclear convencional, sino el fenómeno emergente que articula factores geopolíticos, criminológicos y político-criminales.

1.1 El dilema político-criminal: prevención vs. garantías

La naturaleza de la amenaza híbrida nuclear ejerce una notable presión sobre el Estado para que adopte un paradigma de seguridad eminentemente preventivo. La lógica reactiva del Derecho penal clásico, que interviene tras la comisión de un daño, se percibe como insuficiente ante un riesgo cuya materialización podría tener consecuencias irreversibles. Esta percepción impulsa una tendencia político-criminal que Silva Sánchez denomina "la expansión del Derecho penal". En este modelo, el *ius puniendi* se desplaza desde su función tradicional de castigo de hechos lesivos hacia una nueva función de gestión de riesgos futuros, adelantando las barreras de protección penal a estadios cada vez más tempranos del *iter criminis* (Silva Sánchez & Kretschmer, 2011: 149). Esta tendencia, lejos de atenuarse, se ha ido intensificando desde su formulación original. Como el propio Silva Sánchez reconoce en una investigación posterior, la persistencia de la crisis y la

aparición de nuevos riesgos globales -el terrorismo tras el 11S, la crisis financiera de 2008, las amenazas climáticas y tecnológicas- han provocado que el recurso al Derecho penal como herramienta de gestión de problemas sea una constante. Así, el paradigma preventivo no solo se consolida, sino que se expande ante un escenario de inseguridad estructural creciente (2025: 1-4).

Esta aceleración se ha visto catalizada por la pandemia de la COVID-19, que forzó una transformación digital apresurada y, a menudo, insegura. Como señala Candau Romero, el despliegue masivo del teletrabajo y el uso de nuevas tecnologías de acceso remoto "provocó que no se evaluaran los riesgos asociados, ni las soluciones, ni los protocolos de actuación, incorporando numerosas deficiencias de seguridad que los ciberatacantes han sabido aprovechar" (2021: 24). Este nuevo escenario de vulnerabilidad sistémica ha justificado, a ojos del legislador, una mayor anticipación punitiva para neutralizar amenazas antes de que puedan explotar estas nuevas debilidades.

Dicha estrategia de anticipación punitiva, si bien puede parecer una respuesta lógica a la magnitud de la amenaza, colisiona frontalmente con los principios y garantías fundamentales que estructuran el Estado de Derecho. El problema político-criminal central reside en la difícil ponderación entre la eficacia preventiva y el respeto a las libertades individuales. Como advierte Terradillos Basoco, la lucha contra el terrorismo a menudo conduce a la creación de un "Derecho penal de excepción" que, en nombre de la seguridad, normaliza medidas que en otros contextos serían inaceptables, pervirtiendo las reglas de la teoría del delito y las garantías procesales (2016: 29).

Frente a esta deriva hacia un Derecho penal de excepción, el debate se articula en torno a la "racionalidad de las leyes penales" (Díez Ripollés, 2003: 23), un concepto que somete la legislación a un test de legitimidad basado en los principios de idoneidad, necesidad y proporcionalidad en sentido estricto. Desde esta perspectiva, una política criminal expansiva debe justificar no sólo que sus medidas son idóneas para prevenir el riesgo, sino también que son necesarias -al no existir alternativas menos lesivas para los derechos fundamentales- y proporcionales, asegurando que el sacrificio de libertades se equilibre con el beneficio en seguridad que se obtiene. La amenaza híbrida nuclear, por su carácter extremo, pone a prueba estos principios hasta el límite, tentando al legislador a priorizar la seguridad de forma casi absoluta, en detrimento de un sistema de garantías que puede ser percibido como un obstáculo para una prevención eficaz.

1.2 Del dilema a la excepción: el modelo penal español y la lógica de enemigo

Esta tensión entre la tendencia preventiva y el límite de las garantías encuentra en el modelo penal español una resolución concreta: la adopción progresiva de lo que la doctrina denomina "lógica de enemigo". Este concepto, acuñado por Jakobs y desarrollado en el contexto español por Cancio Meliá, describe un subsistema dentro del ordenamiento que deja de tratar al infractor como un "ciudadano" que ha delinquido para considerarlo un "enemigo" del Estado. Este cambio de

estatus justifica un tratamiento jurídico diferenciado, caracterizado por tres rasgos principales: una amplia anticipación de la punibilidad, la imposición de penas desproporcionadas y la flexibilización o supresión de garantías procesales (2003: 41). El objetivo ya no es la retribución o la resocialización, sino la inocuización: la neutralización de una fuente de peligro para el mantenimiento del sistema.

Esta deriva hacia un nuevo modelo punitivo encuentra su principal exponente en la reforma del Código Penal en materia de terrorismo, materializada en la Ley Orgánica 2/2015. Si bien su alcance es amplio, su aplicación al ámbito nuclear es paradigmática. El ejemplo más destacado es la posesión ilícita de materiales nucleares con finalidad terrorista del art. 574.3 CP, la cual se castiga con penas de diez a veinte años de prisión, un "salto punitivo" significativo frente al tipo básico (de uno a cinco años). Este incremento desproporcionado evidencia que el foco se desplaza del hecho en sí -la mera posesión- a la peligrosidad extrema del autor, a quien se le atribuye la condición de "enemigo" por la naturaleza de sus intenciones. Esta misma lógica de anticipación máxima se extiende a otras figuras de la reforma, como el delito de autoadoctrinamiento (art. 575.2 CP), que, aunque no se refiere directamente al ámbito nuclear, se utiliza para criminalizar procesos cognitivos en una fase muy anterior a cualquier acto preparatorio tangible, legitimando la intervención penal por lo que el sujeto podría llegar a hacer con esa formación. Como señalan algunos autores, esta tipología penal castiga conductas que se sitúan en una difusa frontera entre la ideología y la punibilidad, sancionando actos de autoformación muy alejados de la preparación de un atentado concreto (Cruz-Palmera, 2023: 3 y ss.; Muñoz Conde, 2003: 825).

Frente a esta expansión legislativa, la jurisprudencia del Tribunal Supremo ha intentado ejercer una función de contención, estableciendo criterios interpretativos restrictivos para salvaguardar los derechos fundamentales. Sentencias como la STS nº 661/2017, de 10 de octubre, refleja la tensión entre la literalidad de los nuevos preceptos y su compatibilidad con los principios constitucionales. Al hacerlo, el tribunal se ve obligado a realizar una compleja labor de ponderación para evitar que la lucha contra la amenaza terrorista, especialmente en sus formas más graves como la nuclear, suponga un menoscabo de las garantías esenciales que definen al propio Estado de Derecho que se pretende proteger.

2. El nuevo paradigma de la amenaza: riesgo nuclear en la "zona gris"

La amenaza híbrida nuclear es producto y, a su vez, catalizador de una crisis en el orden de seguridad internacional. La erosión de los regímenes de control de armamentos, la proliferación de nuevas tecnologías disruptivas y la intensificación de la competencia geopolítica han creado un entorno propicio para amenazas más complejas y ambiguas, donde el riesgo nuclear adquiere una nueva dimensión criminológica. En este escenario, la respuesta penal del Estado español no puede entenderse como un ejercicio de soberanía autónoma, sino como el resultado de un complejo proceso de transposición condicionado por un denso marco jurídico supranacional. Por

tanto, para comprender la legislación nacional es imprescindible analizar primero la arquitectura global de la que emana, la cual se enfrenta a una doble amenaza: la erosión del régimen de no proliferación estatal y la emergencia del terrorismo no estatal que busca explotar, precisamente, sus fisuras.

2.1 El régimen de no proliferación: una arquitectura en crisis

El régimen de no proliferación, cuya "clave de bóveda" es desde 1968 el Tratado sobre la no Proliferación de las Armas Nucleares (Garrido Rebolledo, 2025a: 14), atraviesa una profunda crisis de credibilidad. Este instrumento, de adhesión casi universal, se articula sobre un delicado equilibrio entre tres pilares interdependientes (Tratado sobre la No Proliferación de Armas Nucleares (Doc. INFCIRC/140), 1970):

1. No proliferación: se establece una obligación dual por la que los Estados no poseedores de armas nucleares (ENPAN) se comprometen a no adquirirlas, mientras que los cinco Estados poseedores reconocidos por el tratado (EPAN: China, Estados Unidos, Francia, Reino Unido y Rusia) se comprometen a no transferirlas.
2. Desarme: el artículo VI impone a los EPAN la obligación de negociar "de buena fe medidas eficaces" para el cese de la carrera armamentística y el desarme nuclear.
3. Uso pacífico: se reconoce el "derecho inalienable" de todos los Estados a desarrollar la energía nuclear con fines pacíficos, bajo el sistema de verificación del Organismo Internacional de Energía Atómica (OIEA).

Con todo, la arquitectura de este régimen adolece de una creciente crisis de legitimidad y eficacia, como resultado de una convergencia de factores desestabilizadores. El sistema sufre una contradicción interna fundamental: el incumplimiento del pilar de desarme. El pacto original del TNP implicaba que los Estados no poseedores de armas nucleares renunciaban a ellas a cambio de que los Estados poseedores avanzaran hacia el desarme. Sin embargo, la eficacia del tratado se ha visto gravemente mermada por la falta de avances significativos en este pilar. Dicha parálisis ha quedado de manifiesto en las sucesivas Conferencias de Revisión del TNP, en las que la creciente polarización entre los Estados nucleares y los no nucleares ha culminado en una reiterada falta de consenso, evidenciando la inoperancia del foro (Garrido Rebolledo, 2025b: 52 y ss.). Lejos de avanzar hacia el desarme, los EPAN están inmersos en extensos y costosos programas de modernización de sus arsenales, lo que contradice el espíritu del Artículo VI y debilita la legitimidad del tratado en su conjunto. A esta debilidad interna se suman desafíos estructurales a su universalidad y cumplimiento, como la existencia de Estados con capacidad nuclear no firmantes (India, Pakistán, Israel), la retirada de Corea del Norte y la crisis continua que ha representado el programa nuclear de Irán para el sistema de verificación.

Esta fragilidad estructural, a su vez, se ha visto exacerbada de forma dramática por la invasión rusa de Ucrania en 2022. La retórica nuclear explícita por parte de Moscú y los ataques a infraestructuras nucleares civiles, como la central de

Zaporiyia, han reintroducido el arma atómica como un instrumento de coerción en la política de las grandes potencias, erosionando el tabú nuclear que había prevalecido durante décadas (Pérez Gil, 2025: 71-106). A esto se suma la suspensión por parte de Rusia de su participación en el tratado New START, el último gran acuerdo de control de armas estratégicas con Estados Unidos, lo que abre la puerta a una nueva carrera armamentística sin restricciones (Beckmann, 2015: 26). Como reacción a esta parálisis, la frustración de los Estados no nucleares impulsó la adopción del Tratado sobre la Prohibición de las Armas Nucleares (TPAN) en 2017, un instrumento simbólicamente poderoso pero boicoteado por las potencias nucleares, evidenciando la profunda fractura del régimen. En este contexto de desconfianza creciente, el riesgo de proliferación se intensifica, pues la percepción de que las armas nucleares son garantes de la seguridad puede incentivar a otros Estados a desarrollar sus propios programas. Simultáneamente, la degradación del control estatal aumenta el riesgo de que materiales nucleares o radiológicos caigan en manos de actores no estatales.

Para hacer frente a esta creciente preocupación, la comunidad internacional ha erigido una arquitectura jurídica multinivel, destacando la Resolución 1373 (2001) adoptada tras los atentados del 11 de septiembre para reprimir la financiación del terrorismo (Resolución 1373 (2001), aprobada por el Consejo de Seguridad en su 4385ª sesión, celebrada el 28 de septiembre de 2001, Doc. S/RES/1373, 2001: 2); la Convención internacional para la represión de actos de terrorismo nuclear (2005), configurada como herramienta penal específica, imponiendo a los Estados la obligación de tipificar un catálogo preciso de delitos -como la posesión ilícita de material radiactivo con fines terroristas- y consagrando el principio *aut dedere aut judicare* (extraditar o juzgar) para eliminar refugios seguros (Convenio internacional para la represión de los actos de terrorismo nuclear, hecho en Nueva York el 13 de abril de 2005 y ratificado por España el 29 de enero de 2007 (BOE núm. 146, de 19 de junio de 2007): 2); o la Resolución 2341 (2017), de 13 de febrero, la cual complementa las anteriores al centrarse específicamente en la protección de infraestructuras críticas, incluidas las nucleares, instando a los Estados a desarrollar estrategias para reducir los riesgos y prevenir que se conviertan en objetivos de ataques terroristas (Resolución 2341 (2017), aprobada por el Consejo de Seguridad en su 7882.ª sesión, celebrada el 13 de febrero de 2017. Doc. S/RES/2341, 2017). Es en esta fisura del régimen de control estatal donde la amenaza híbrida nuclear encuentra su caldo de cultivo.

2.2 Modalidades criminológicas en la Zona Gris

La amenaza híbrida nuclear se materializa a través de modalidades criminológicas específicas que combinan la clandestinidad, el uso de tecnologías avanzadas y la explotación de las vulnerabilidades de las sociedades abiertas. Dos de las más significativas son el tráfico ilícito de materiales y los ciberataques a infraestructuras críticas.

2.2.1 El tráfico ilícito como amenaza latente

La posibilidad de que un grupo terrorista adquiera materiales nucleares o radiológicos para fabricar un arma nuclear improvisada o un "dispositivo de dispersión radiológica" (RDD, comúnmente conocido como "bomba sucia") no es una hipótesis teórica, sino un riesgo tangible documentado por organismos internacionales. La Base de Datos sobre Tráfico Ilícito (ITDB) del Organismo Internacional de Energía Atómica (OIEA) ha registrado, desde 1993 hasta el 31 de diciembre de 2024, un total de 4.390 incidentes confirmados de materiales nucleares y otros materiales radiactivos fuera del control reglamentario. En el último año, se han reportado 147 nuevos incidentes, manteniendo la media histórica y subrayando que el problema no remite. Desde 1993, los incidentes se han clasificado en tres grupos según su intencionalidad. El grupo I engloba 353 casos confirmados de tráfico o uso ilícito, donde casi la mitad de los cuales (47 %) involucraron material nuclear. El grupo II, con 1065 incidentes se centra principalmente en robos o pérdidas, siendo el 83% de ellos fuentes radiactivas. Finalmente, el grupo III, el más numeroso con 2972 casos, no está relacionado con el tráfico o uso ilícito, pero sí con recuperaciones o descubrimientos. En este caso, más de la mitad (53%) estaba vinculado a fuentes de carácter radiactivo. Un hallazgo clave es la vulnerabilidad del transporte, ya que el 53% de todos los robos reportados ocurrieron durante el traslado autorizado de materiales, una cifra que se eleva al 65% en la última década. En términos generales, del total de incidentes, el 14% ha involucrado material nuclear, el 59% otros materiales radiactivos y el 27% restante materiales contaminados (Organismo Internacional de Energía Atómica, 2025: 2). Aunque la mayoría de estos incidentes no están directamente relacionados con actividades terroristas, demuestran la existencia de vulnerabilidades persistentes en la seguridad y el control de estos materiales a nivel global.

El marco jurídico y regulatorio, tanto internacional como nacional, busca mitigar este riesgo. A nivel internacional, las recomendaciones del OIEA, en particular el documento de Recomendaciones de Seguridad Física Nuclear sobre la Protección Física de los Materiales y las Instalaciones Nucleares, establecen el estándar de referencia (OIEA, 2011: 20-22). España ha transpuesto las directrices internacionales sobre protección física a su ordenamiento interno a través de un marco normativo que ha evolucionado para adaptarse a las nuevas realidades de la amenaza. La arquitectura regulatoria se sostiene sobre dos pilares fundamentales: una ley histórica que sentó las bases y una reglamentación reciente que moderniza y detalla las exigencias.

La Ley 25/1964, de 29 de abril, sobre energía nuclear, aunque preconstitucional, sigue siendo la norma marco que establece el régimen de autorizaciones y el control administrativo fundamental sobre las instalaciones y los materiales nucleares en España. (Ley 25/1964, de 29 de abril, sobre energía nuclear, BOE núm. 107, de 04/05/1964). Sin embargo, su redacción original no podía prever los desafíos actuales, como el terrorismo no estatal o las ciberamenazas. Por ello, su función hoy es la de proporcionar el esqueleto legal sobre el que se articulan normativas más específicas y actualizadas.

La modernización clave llega con el Real Decreto 1029/2022, de 20 de diciembre, sobre protección física de las instalaciones y los materiales nucleares. Esta norma deroga la reglamentación anterior y actualiza de forma exhaustiva las exigencias de seguridad para alinearlas con los estándares internacionales más recientes, en particular la Convención sobre la Protección Física de los Materiales Nucleares y su Enmienda, y las recomendaciones del OIEA (Real Decreto 1029/2022, de 20 de diciembre, por el que se aprueba el Reglamento sobre protección de la salud contra los riesgos derivados de la exposición a las radiaciones ionizantes, BOE núm. 305, de 21/12/2022). En tal contexto, la lucha por la persecución de estos delitos presenta desafíos únicos, haciendo de la "investigación forense nuclear" una herramienta indispensable para la atribución de origen de los materiales incautados y la identificación de las redes de tráfico, como subraya Llorente Aguilera (2021: 3 y ss.).

2.2.2 El ciberataque como vector estratégico

La creciente digitalización de los sistemas de control industrial ha abierto una nueva y peligrosa vía de ataque. El gusano informático Stuxnet, descubierto en 2010, fue un punto de inflexión, al demostrar que un ciberataque podía causar un daño físico directo a una infraestructura nuclear, en este caso, a las centrifugadoras de enriquecimiento de uranio en Irán. Stuxnet fue una pieza de *malware* de una complejidad sin precedentes, diseñada para reprogramar los controladores lógicos programables y sabotear el proceso industrial mientras ocultaba su actividad a los operadores (Falliere *et al*., 2011: 2).

Informes posteriores, como el influyente estudio de Chatham House, han puesto de manifiesto que la creencia de que las instalaciones nucleares están completamente aisladas de internet (*air-gapped*) es un mito. La conectividad, a menudo no documentada, las vulnerabilidades en la cadena de suministro y la falta de una cultura de ciberseguridad robusta entre el personal convierten a estas instalaciones en objetivos atractivos y vulnerables (Baylon *et al*., 2025: 8 y ss.). Un ataque exitoso podría no solo provocar un incidente radiológico, sino también servir como una táctica de distracción o habilitación para una operación física, como el robo de materiales.

Aunque no se ha producido un ciberataque de esta magnitud sobre una instalación nuclear, el reciente auge de los ataques de *ransomware* a infraestructuras críticas demuestra la plausibilidad del escenario. El caso del ataque al oleoducto Colonial en Estados Unidos en mayo de 2021 es paradigmático: un grupo de cibercrimen, utilizando *ransomware*, logró interrumpir la operación de un oleoducto de 8.000 km, responsable del 45% del suministro de combustible de la Costa Este, generando temor a un desabastecimiento en 50 millones de personas y forzando el pago de un rescate millonario (Candau Romero, 2021: 24-25). Este incidente evidencia cómo un ataque a las redes corporativas (redes IT) puede tener un impacto directo y paralizante sobre las redes operacionales (redes OT), una lección directamente aplicable al sector nuclear.

Esta amenaza sinérgica, donde un ciberataque facilita el tráfico ilícito, representa un

ejemplo perfecto de una amenaza híbrida. En este escenario, un actor sofisticado podría lanzar un ciberataque no con el objetivo de provocar una fusión del núcleo -un acto de consecuencias masivas y alta atribución-, sino para desactivar temporalmente los sistemas de vigilancia, control de acceso y monitorización de materiales. Esta ventana de vulnerabilidad, creada digitalmente, podría ser explotada por un grupo para llevar a cabo una filtración física de material nuclear o radiológico. Como resultado, esta operación combinada maximizaría la ambigüedad, dificultaría la atribución de responsabilidades y paralizaría la capacidad de respuesta del Estado víctima, encajando perfectamente en el paradigma de la "zona gris".

Lejos de ser una mera hipótesis, la viabilidad de este tipo de ataques se fundamenta en debilidades técnicas bien documentadas. Como ya advertía Candau Romero, el riesgo principal en los sistemas SCADA que controlan procesos críticos -desde redes eléctricas hasta centrales nucleares- reside en "el desconocimiento por parte del propietario de las interconexiones reales", la "ausencia de buenas prácticas de seguridad como la realización de actualizaciones periódicas o una adecuada gestión de las contraseñas" y "las deficiencias en la configuración de los diferentes dispositivos" (2013: 219). Esta confluencia de factores, unida a la creciente conexión de estos sistemas a redes públicas para maximizar la rentabilidad, crea una superficie de ataque que los actores híbridos están especialmente preparados para explotar.

Precisamente para hacer frente a este panorama de riesgo, la respuesta regulatoria frente a las ciberamenazas a infraestructuras críticas, como las nucleares, se ha articulado en un marco multinivel que combina la armonización europea con la estrategia nacional. Este andamiaje jurídico busca superar las deficiencias de la normativa anterior y crear un ecosistema de seguridad y resiliencia mucho más exigente. A nivel europeo, este andamiaje se basa en un doble enfoque legislativo. Por un lado, la Directiva (UE) 2022/2555 (NIS2) actualiza y endurece significativamente la legislación en ciberseguridad, ampliando su alcance para incluir explícitamente la energía nuclear e imponiendo a los operadores obligaciones más estrictas en la gestión de riesgos de la cadena de suministro y la notificación de incidentes (Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, DOUE núm. 333, de 27 de diciembre de 2022, Art. 7). Por otro lado, y de manera complementaria, la Directiva (UE) 2022/2557 sobre la Resiliencia de las Entidades Críticas aborda la resiliencia física frente a amenazas como el sabotaje o el terrorismo, obligando a los Estados a identificar sus "entidades críticas" y a exigirles la realización de evaluaciones de riesgos periódicas(Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas, DOUE núm. 333, de 27 de diciembre de 2022, Art. 4). En conjunto, ambas directivas funcionan de manera coordinada para asegurar que la protección de infraestructuras como las centrales nucleares sea integral, cubriendo tanto las amenazas digitales como las físicas.

3. La respuesta española: un modelo de seguridad multinivel

3.1. Gobernanza y prevención: la Estrategia Nacional de Ciberseguridad

A nivel nacional, España ha integrado las directrices europeas de las directivas NIS2 y CER en un sofisticado y multinivel marco de gobernanza cuya pieza central es el Consejo Nacional de Ciberseguridad (CNC). Este órgano, creado en 2013 como apoyo al Consejo de Seguridad Nacional, coordina y supervisa las políticas estratégicas a través de un modelo de cuatro niveles: político, estratégico, operacional y técnico (Sánchez Goicochea *et al*., 2024: 10). Es precisamente en este marco donde se inserta la Estrategia Nacional de Ciberseguridad, que funciona como la hoja de ruta operativa del país. Lejos de ser una mera declaración de intenciones, establece un plan de acción concreto, articulado en torno a cinco objetivos estratégicos, destacando la protección de sectores como el nuclear como una prioridad absoluta para la seguridad nacional (Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, BOE núm. 103, de 30 de abril de 2019: 43444 y ss.)

Para materializar esta protección, la estrategia se apoya en una arquitectura institucional especializada con roles bien definidos, dando continuidad a las líneas de acción que ya se esbozaban en documentos estratégicos previos (Candau Romero, 2011b: 339-344). Por un lado, el Centro Criptológico Nacional (CCN-CERT), adscrito al CNI, se erige como el CERT Gubernamental Nacional, responsable de coordinar la respuesta a incidentes en el sector público y en los operadores de infraestructuras críticas (Candau Romero, 2011a: 302). Su labor es fundamental en la prevención, proporcionando guías técnicas, alertas tempranas y capacidad de análisis forense, y en el desarrollo y supervisión del Esquema Nacional de Seguridad (ENS). De forma complementaria, el Instituto Nacional de Ciberseguridad (INCIBE) se centra en la ciberseguridad de ciudadanos y del sector privado, impulsando una cultura de seguridad que reduce el riesgo derivado del factor humano (Baylon et al., 2025: 12) y fortaleciendo el ecosistema industrial a través de programas como INCIBE Emprende y Cyberinnova (Sánchez Goicochea *et al*., 2024: 12). Este andamiaje se completa con el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), dependiente del Ministerio del Interior, que coordina la crucial colaboración público-privada mediante el intercambio de inteligencia y la realización de ejercicios conjuntos (Candau Romero, 2011a: 271).

De este modo, la estrategia española no solo se alinea formalmente con las obligaciones impuestas por la NIS2 y la Directiva CER, sino que las dota de un marco de implementación detallado, con actores definidos y mecanismos de cooperación concretos para asegurar su aplicación efectiva en el contexto español.

Si bien esta arquitectura estratégica e institucional conforma la primera línea de defensa, basada en la prevención y la coordinación, el Estado también se ha dotado de un contundente marco punitivo para responder a la vulneración de dichas barreras preventivas. Es aquí donde el

ordenamiento jurídico-penal interviene, articulando las consecuencias últimas para quienes materializan este tipo de amenazas.

3.2 La respuesta punitiva: el Derecho penal frente a la amenaza híbrida

El ordenamiento jurídico-penal español ha desarrollado una arquitectura compleja y severa para hacer frente a la amenaza terrorista, especialmente en su potencial dimensión nuclear. Este andamiaje punitivo se caracteriza por una marcada estrategia de anticipación, que adelanta las barreras de protección a fases muy tempranas del *iter criminis*. El problema surge cuando, si bien esta orientación preventiva puede parecer una respuesta lógica a la magnitud del riesgo, un análisis dogmático revela profundas tensiones con los principios fundamentales del Derecho penal liberal, evidenciando la adopción de una lógica más propia del "Derecho penal del enemigo".

3.2.1 La lógica preventiva: delitos de peligro y anticipación punitiva

La primera línea de defensa penal frente a los riesgos nucleares se encuentra en el Capítulo II del Título XVII del Código Penal, dedicado a los "delitos de riesgo catastrófico" (arts. 341-345 CP). Estos tipos penales no castigan tanto la producción de un daño efectivo, sino la creación de una situación de peligro cualificado para la seguridad colectiva, un bien jurídico de naturaleza supraindividual que protege la suma de bienes fundamentales -vida, salud, patrimonio, medio ambiente- frente a un riesgo de escala excepcional. Son, por tanto, el exponente de una estrategia de anticipación punitiva.

La estructura de estos delitos revela su complejidad y su dependencia de la normativa extrapenal, configurándose como leyes penales en blanco que deben ser interpretadas a la luz de la legislación sectorial, como la Ley 25/1964 sobre Energía Nuclear. Este diseño se materializa en una escalada de anticipación punitiva. En un primer nivel, el art. 341 CP castiga la "liberación de energía nuclear o elementos radiactivos", un delito de resultado de peligro concreto diseñado para el escenario más catastrófico, como un sabotaje exitoso. A continuación, el art. 342 CP adelanta aún más la protección al sancionar la "perturbación del funcionamiento de una instalación nuclear o radiactiva", castigando como delito de mera actividad el acto previo que crea un "grave peligro" de que dicha liberación se produzca. Finalmente, la anticipación alcanza su máxima expresión en el art. 345 CP, que tipifica el "tráfico ilícito de materiales nucleares o radiactivos", sancionando actos que, en sí mismos, son preparatorios. Como señala Rodríguez Monserrat, la lógica subyacente a estos preceptos es la de criminalizar la gestión del riesgo, castigando la sustracción de materiales de alta peligrosidad del riguroso sistema de fiscalización estatal (2020: 1). En conjunto, estos delitos de peligro constituyen la base sobre la que se construirá la respuesta agravada frente al terrorismo.

3.2.2 La lógica de enemigo: cualificación por terrorismo y salto punitivo

La arquitectura penal española alcanza su máxima severidad cuando los delitos de peligro nuclear se conectan con la finalidad terrorista. El engranaje central de esta conexión es el artículo 573 CP, que funciona como una norma de calificación: transforma un delito común en un delito de terrorismo cuando se comete con fines como "subvertir el orden constitucional", "alterar gravemente la paz pública" o "provocar un estado de terror en la población", imponiendo la pena del delito base en su mitad superior. (Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, BOE núm. 281, de 24/11/1995, Art. 573). Esta técnica legislativa provoca lo que la doctrina denomina un "salto punitivo" extraordinario, especialmente visible en las fases preparatorias. La justificación dogmática reside en la pluriofensividad del delito de terrorismo: no se castiga solo el riesgo para la seguridad colectiva, sino también el ataque al orden constitucional y la paz pública. Sin embargo, como se evidencia en la Tabla 1, la magnitud de este incremento plantea serias dudas sobre su conformidad con el principio de proporcionalidad.

Tabla 1. Comparativa del marco punitivo: delitos nucleares comunes vs. cualificación por terrorismo

Delito Base	Marco Penal Base (Prisión)	Delito con Finalidad Terrorista	Marco Penal Terrorista (Prisión)	Incremento Cuantitativo (Ratio Mínimo/Máximo)
Tráfico/Posesión ilícita de material nuclear (Art. 345.1 CP)	1 a 5 años	Posesión de material nuclear con finalidad terrorista (Art. 574.3 CP)	10 a 20 años	x10 / x4
Perturbación de instalación nuclear (Art. 342 CP)	4 a 10 años	Perturbación de instalación con finalidad terrorista (Art. 573 CP)	7 a 10 años	x1.75 / x1
Liberación de energía nuclear (Art. 341 CP)	15 a 20 años	Liberación de energía nuclear con resultado de muerte (Art. 573 bis.1.1ª CP)	Prisión Permanente Revisable	Salto cualitativo

Fuente: Elaboración propia a partir del Código Penal español.

3.3 La ejecución penal como instrumento de seguridad: peligrosidad y excepción penitenciaria

La "lógica de enemigo" no se agota en la tipificación de los delitos, sino que se proyecta sobre todo el sistema de justicia penal, alcanzando de forma especialmente intensa la fase de ejecución de la pena. En efecto, si en los apartados anteriores se aprecia cómo la seguridad nacional queda "garantizada" gracias al adelantamiento de las barreras punitivas, en esta fase, el tratamiento penitenciario de los condenados por terrorismo se articula en torno al concepto de "peligrosidad", configurando lo que Faraldo Cabana denomina un "subsistema penitenciario de excepción" (2006: 1).

El marco normativo general, compuesto por la Ley Orgánica General Penitenciaria (LOGP) de 1979 y el Reglamento Penitenciario de 1996, establece como fin primordial de la pena privativa de libertad la "reeducación y reinserción social" (art. 25.2 de la Constitución Española). Sin embargo, para los internos por terrorismo, este objetivo se ve subordinado a la neutralización del riesgo que se presume que continúan representando. Por ello, la clasificación en segundo grado penitenciario (régimen ordinario) se convierte en la norma, y el acceso al tercer grado (régimen de semilibertad) o a los permisos de salida se somete a requisitos extraordinariamente rigurosos, como la exigencia de una "declaración expresa de repudio de sus actividades delictivas y de abandono de la violencia", así como una "petición expresa de perdón a las víctimas" (Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria, BOE núm. 239, de 05/10/1979, art. 72.6).

Esta excepcionalidad, en consecuencia, se fundamenta en una presunción *iuris et de iure* de peligrosidad que transforma la naturaleza de la pena: deja de ser una respuesta a un hecho pasado para convertirse en un período de incapacitación y gestión de un riesgo futuro. De este modo, el interno no es visto como un ciudadano, sino como un "enemigo" cuya peligrosidad debe ser contenida. Programas como el "Programa Marco de intervención en radicalización violenta con internos islamistas" operan bajo esta misma lógica: son herramientas de evaluación y gestión del riesgo que consolidan un modelo donde la ejecución penal para terroristas se aleja de los principios generales para configurarse como un instrumento de seguridad, materializando en la práctica la distinción entre un Derecho penal para "ciudadanos" y otro para "enemigos". En definitiva, la progresión en el tratamiento penitenciario depende de la superación de un juicio de peligrosidad.

4. Conclusiones: propuestas para una política criminal racional frente a la amenaza híbrida

El análisis del modelo político-criminal español frente a la amenaza híbrida nuclear revela una profunda y preocupante deriva hacia una lógica de seguridad que sacrifica garantías fundamentales en aras de la prevención. Si bien la magnitud del riesgo exige una respuesta estatal robusta y eficaz, la estrategia adoptada parece haber traspasado los límites de un Derecho penal racional y proporcionado, acercándose

peligrosamente a los postulados del Derecho penal del enemigo que describen Jakobs y Cancio Meliá.

A lo largo del texto se aprecia cómo efectivamente la respuesta penal española, especialmente tras la reforma de 2015, se articula sobre una lógica de enemigo. Ésta se manifiesta en tres ámbitos interconectados que evidencian la tensión entre la seguridad y el Estado de Derecho: primero, en un "salto punitivo" desproporcionado que, a través de la cualificación por finalidad terrorista, impone penas extraordinariamente graves a conductas que, en su tipo básico, tienen una sanción mucho menor. Como se ha demostrado, el incremento punitivo en las fases preparatorias del tráfico de material nuclear es cuantitativamente irrazonable y pone en tela de juicio su adecuación al principio de proporcionalidad. Segundo, la criminalización de la peligrosidad subjetiva: la punición de actos preparatorios remotos difumina la frontera entre la ideología y la acción punible. Con ello, se transita desde un Derecho penal del hecho hacia un Derecho penal de autor que castiga la peligrosidad del sujeto en lugar de la lesividad objetiva de su conducta, un rasgo distintivo de la lógica de excepción. Tercero, en la configuración de un subsistema penitenciario de excepción basado en una presunción de peligrosidad que subordina el fin resocializador de la pena a la neutralización del interno, materializando así la distinción entre un Derecho penal para "ciudadanos" y otro para "enemigos". Bajo este paradigma, la lógica de enemigo se proyecta hasta la fase de ejecución penal.

Como se aprecia a lo largo del texto, este modelo se aleja de los principios de racionalidad, necesidad y proporcionalidad que deben regir la intervención penal en un Estado de Derecho. La expansión del Derecho penal para gestionar riesgos, en lugar de castigar daños, conduce a una espiral punitiva que, además de ser cuestionable desde el punto de vista de los derechos fundamentales, puede resultar contraproducente, generando agravios que alimenten los propios procesos de radicalización que pretende combatir.

Reconducir el modelo español hacia una política criminal más garantista no implica renunciar a la seguridad, sino dotarla de racionalidad. Para ello, se proponen las siguientes medidas, que combinan la reforma legislativa con un enfoque integral de la prevención.

1. ***En el plano legislativo***:

En primer lugar, modular la proporcionalidad del art. 574 CP. Es fundamental reformar este artículo para introducir una mayor graduación en la respuesta punitiva. La pena debería poder modularse en función de criterios objetivos como la naturaleza del material, el grado de avance en el *iter criminis* y el contexto operativo del autor. Esto permitiría al juez imponer una pena ajustada a la gravedad concreta del hecho, evitando la rigidez actual. En segundo lugar, derogar o reformar sustancialmente el delito de autoadoctrinamiento del art. 575.2 CP. Este precepto, por su vaguedad, debería ser derogado o, al menos, reformado sustancialmente. En tercer lugar, la legislación española debe incorporar plenamente el espíritu de la Directiva (UE) 2017/541, no solo en la tipificación, sino también en sus cláusulas de salvaguardia. Esto incluye la obligación de que las sanciones sean "proporcionadas" y la introducción explícita de atenuantes por colaboración o desistimiento del art.

16, lo que incentivaría la desactivación temprana de amenazas.

2. ***En el plano de la política criminal integral***:

En este plano, la estrategia debe reorientarse hacia un enfoque proactivo y multifacético. En primer lugar, es fundamental priorizar la prevención social sobre la penal, desplazando el foco desde la punición de actos remotos hacia una inversión decidida en educación, programas de inclusión y el desarrollo de contranarrativas eficaces en colaboración con la sociedad civil. Paralelamente, se deben fortalecer las capacidades de inteligencia y ciberseguridad para la detección temprana de amenazas concretas, centrando los esfuerzos en el nexo entre el tráfico de materiales y las ciberamenazas a infraestructuras críticas, en línea con la Estrategia Nacional de Ciberseguridad y las recomendaciones del OIEA. Finalmente, es imprescindible racionalizar la política penitenciaria, reformando el tratamiento de los condenados por terrorismo para que, sin menoscabo de la seguridad, se base en programas de desradicalización individualizados y evaluados científicamente, que persigan una genuina reinserción y eviten que las prisiones se conviertan en focos de mayor radicalización.

En definitiva, solo una estrategia que combine la firmeza del Estado de Derecho con la inteligencia de una prevención integral y la proporcionalidad de sus instrumentos punitivos podrá hacer frente a la amenaza híbrida nuclear sin renunciar a los valores democráticos que, precisamente, pretende proteger.

Bibliografía

Referencias doctrinales

Baqués, J. (2017). "Hacia una definición del concepto «Gray Zone» (GZ)». *Documento de Investigación IEEE (Instituto Español de Estudios Estratégicos)*, 2/2017, 1-29. https://www.ieee.es/Galerias/fichero/docs_investig/2017/DIEEE-INV02-2017_Concepto_GaryZone_JosepBaques.pdf

Baylon, C., Brunt, R., & Livingstone, D. (2025). *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*. Londres: Chatham House, the Royal Institute of International Affairs. https://www.chathamhouse.org/archive/cyber-security-civil-nuclear-facilities-understanding-risks

Beckmann, C. (2015). "Las armas nucleares nos cuestan la Tierra". *Revista Tiempo de Paz*, 156, 22-29. https://revistatiempodepaz.org/revista-156/

Candau Romero, J. (2011a). "Estrategias nacionales de ciberseguridad: Ciberterrorismo". *Cuadernos de estrategia*, 149, Instituto Español de Estudios Estratégicos (Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio), 257-322. https://dialnet.unirioja.es/servlet/articulo?codigo=3837524

Candau Romero, J. (2011b). "Líneas de acción de la estrategia nacional de ciberseguridad". *Cuadernos de estrategia*, 149, Instituto Español de Estudios Estratégicos (Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio), 336-344. https://dialnet.unirioja.es/servlet/articulo?codigo=3837589

Candau Romero, J. (2013). "Prioridades nacionales en ciberseguridad". En *Ciberseguridad global: Oportunidades y compromisos en el uso del ciberespacio*. Granada: Universidad de Granada, 209-239.

Candau Romero, J. (2021). "Ciberseguridad: Evolución y tendencias". *Boletín IEEE (Instituto Español de Estudios Estratégicos)*, 23, 460-494. https://dialnet.unirioja.es/servlet/articulo?codigo=8175398

Cruz-Palmera, R. (2023). "El delito de autoadroctrinamiento terrorista, art. 575.2. Del Código Penal español. Un análisis en clave de imputación". *Estudios de Deusto*, 71(1), 131-160. https://doi.org/10.18543/ed.2803

Díez Ripollés, J. L. (2003). *La racionalidad de las leyes penales: Práctica y teoría*. Madrid: Trotta.

Falliere, N., O. Murchu, L., & Chien, E. (2011). *W32 Stuxnet Dossier (Version 1.4)*. Cupertino: Symantec. http://archive.org/details/w32_stuxnet_dossier

Faraldo Cabana, P. (2006). "Medidas premiales durante la ejecución de condenas por terrorismo y delincuencia organizada: Consolidación de un subsistema penitenciario de excepción". En M. Cancio Meliá & C. Gómez-Jara Díez (Eds.), *Derecho penal del enemigo: El discurso penal de la exclusión* (pp. 757-798). Madrid: Edisofer.

Garrido Rebolledo, V. (2025a). "Introducción". En *Panorama nuclear global, Cuadernos de Estrategia*, 229, 256. https://www.defensa.gob.es/ceseden/-/cuaderno-de-estrategia-229

Garrido Rebolledo, V. (2025b). "La crisis del régimen de no proliferación nuclear". *Tiempo de Paz*, 156, 52-64. https://openurl.ebsco.com/contentitem/gcd:185910019?sid=ebsco:plink:crawler&id=ebsco:gcd:185910019

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies. https://www.potomacinstitute.us/reports/19-reports/1163-conflict-in-the-21st-century-the-rise-of-hybrid-wars

Jakobs, G., & Cancio Meliá, M. (2003). *Derecho penal del enemigo* (1. ed). Madrid: Thomson Civitas.

Jordán Enamorado, J. J. (2022). "La disuasión en la zona gris: Una exploración teórica". *Revista española de ciencia política*, 59, 65-88. https://dialnet.unirioja.es/servlet/articulo?codigo=8528414

Llorente Aguilera, C. (2021). "Investigación forense nuclear como herramienta fundamental en la lucha contra el terrorismo nuclear". *Instituto Español de Estudios Estratégicos (IEEE)*, 130, 844-857.

Muñoz Conde, F. (2003). "El nuevo derecho penal autoritario". En E. O. de T. y Ubieto, M. G. Sierra, E. C. Bechiarelli, & L. F. R. Antón (Eds.), *Estudios penales en recuerdo del profesor Ruiz Antón* (pp. 803-824). Valencia: Tirant lo Blanch.

Pérez Gil, L. V. (2025). "Poderío nuclear de Rusia: Nuevos planteamientos sobre capacidades y doctrina de empleo". *Cuadernos de estrategia*, 229 (Panorama nuclear global), 71-106. https://www.defensa.gob.es/ceseden/-/cuaderno-de-estrategia-229

Rodríguez Monserrat, M. (2020). "La "seguridad nuclear" a juicio: Análisis del sistema punitivo español aplicable a los peligros y daños generados por el uso de la energía nuclear". *Actualidad Jurídica Ambiental*, 107 (Diciembre), 7-68. https://www.actualidadjuridicaambiental.com/wp-content/uploads/2020/12/2020_12_Recopilatorio-107-AJA-diciembre.pdf

Sánchez Goicochea, M. E., Solleiro Rebolledo, J. L., & Castañón Ibarra, R. (2024). *Organismos de política y gestión de ciberseguridad*. Ciudad de México: Instituto de Ciencias Aplicadas y Tecnología, UNAM. https://doi.org/10.13140/RG.2.2.35129.99684

Silva Sánchez, J.-M. (2025). "Expansión 2.0: Los nuevos riesgos". *InDret*, 2, I-IV.

https://raco.cat/index.php/InDret/article/view/10000000176

Silva Sánchez, J.-M., & Kretschmer, B. (2011). *La expansión del derecho penal: Aspectos de la política criminal en las sociedades postindustriales*. Madrid; Montevideo: Edisofer; B de F.

Terradillos Basoco, J. M. (2016). "Terrorismo yihadista y política criminal del siglo XXI". *Nuevo Foro Penal*, 87, 18-59. https://dialnet.unirioja.es/servlet/articulo?codigo=5838393

Fuentes normativas y documentos oficiales

Convenio internacional para la represión de los actos de terrorismo nuclear, hecho en Nueva York el 13 de abril de 2005 y ratificado por España el 29 de enero de 2007 (BOE núm. 146, de 19 de junio de 2007). https://treaties.un.org/doc/db/Terrorism/spanish-18-15.pdf.

Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo. Doc. DOUE núm. 333, de 27 de diciembre de 2022. https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81965.

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. Doc. DOUE núm. 333, de 27 de diciembre de 2022. https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963.

High Representative of the Union for Foreign Affairs and Security Policy. (2016). Joint Framework on countering hybrid threats a European Union response. Doc. JOIN(2016) 18 final. Bruselas: European Parliament and the Council. https://doi.org/10.1093/law-oeeul/e66.013.66.

Ley 25/1964, de 29 de abril, sobre energía nuclear (BOE núm. 107, de 04/05/1964). https://www.boe.es/buscar/act.php?id=BOE-A-1964-7544.

Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria. (BOE núm. 239, de 05/10/1979). https://www.boe.es/eli/es/lo/1979/09/26/1.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. «BOE» núm. 281, de 24/11/1995. https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

OIEA. (2011). Recomendaciones de Seguridad Física Nuclear sobre la Protección Física de los Materiales y las Instalaciones Nucleares (INFCIRC/225/Rev.5). Viena: OIEA. https://www.iaea.org/sites/default/files/publications/documents/infcircs/1975/pub1481s_web.pdf.

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019 (BOE núm. 103, de 30 de abril de 2019). https://www.boe.es/eli/es/o/2019/04/26/pci487.

Organismo Internacional de Energía Atómica. (2025). *Illicit Trafficking Database (ITDB) fact sheet*. Viena: IAEA. https://www.iaea.org/sites/default/files/25/03/itdb-factsheet.pdf.

Real Decreto 1029/2022, de 20 de diciembre, por el que se aprueba el Reglamento sobre protección de la salud contra los riesgos derivados de la exposición a las radiaciones ionizantes. (BOE núm. 305, de 21/12/2022). https://www.boe.es/buscar/act.php?id=BOE-A-2022-21682.

Resolución 1373 (2001), aprobada por el Consejo de Seguridad en su 4385a sesión, celebrada el 28 de septiembre de 2001, Doc. S/RES/1373. https://docs.un.org/es/s/res/1373(2001).

Resolución 1540 (2004), aprobada por el Consejo de Seguridad en su 4956a sesión, celebrada el 28 de abril de 2004. Doc. S/RES/1540(2004). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/328/46/PDF/N0432846.pdf?OpenElement.

Resolución 2341 (2017), aprobada por el Consejo de Seguridad en su 7882.a sesión, celebrada el 13 de febrero de 2017. Doc. S/RES/2341 (2017). https://digitallibrary.un.org/record/858856.

Tratado sobre la No Proliferación de Armas Nucleares (Doc. INFCIRC/140), hecho en Londres, Moscú y Washington el 1 de julio de 1968 y ratificado por España el 29 de diciembre de 1987 (BOE núm. 313, de 31 de diciembre de 1987). https://www.iaea.org/sites/default/files/publications/documents/infcircs/1970/infcirc140_sp.pdf.