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

Artigo de Investigação

AS INFRAESTRUTURAS CRÍTICAS ESPANHOLAS COMO ALVO DE GRUPOS TERRORISTAS. ANÁLISE DAS VULNERABILIDADES, QUADRO REGULAMENTAR E ESTRATÉGIAS DE PROTEÇÃO

Tradução para o português com ajuda de IA (DeepL)

Raúl Moreno Ruiz
Capitão da Guardia Civil
Especialista em Segurança Prisional (Ministério do Interior)
Mestrado em Gestão Operacional da Segurança - Licenciatura em Direito
raul.moreno@dgip.mir.es

Recebido em 23/03/2026
Aceite em 04/06/2026
Publicado em 30/06/2026

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

Citação recomendada: Moreno, R. (2026). As infraestruturas críticas espanholas como alvo de grupos terroristas. Análise das vulnerabilidades, quadro regulamentar e estratégias de proteção. Revista Logos Guardia Civil, 4(2), pp. 281–302. https://doi.org/10.64217/logosguardiacivil.v4i2.8979

Registo Legal: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

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

AS INFRAESTRUTURAS CRÍTICAS ESPANHOLAS COMO ALVO DE GRUPOS TERRORISTAS. ANÁLISE DAS VULNERABILIDADES, QUADRO REGULAMENTAR E ESTRATÉGIAS DE PROTEÇÃO

Resumo: A vulnerabilidade das infraestruturas críticas espanholas face à ameaça terrorista numa perspetiva jurídica, institucional e operacional. O estudo analisa o quadro normativo existente — através da Lei n.º 8/2011 e da Diretiva (UE) 2022/2557 relativa à resiliência das entidades críticas (CER) —, centra-se nos setores-chave mais vulneráveis ao risco e avalia a arquitetura institucional do sistema de proteção espanhol. Através de uma metodologia de análise documental e da revisão da literatura especializada, constata-se que, apesar de existir um sistema sólido de proteção das infraestruturas críticas (PIC) em Espanha, existem lacunas significativas na cibersegurança industrial, na coordenação interadministrativa e na transposição das diretivas europeias, que requerem atenção urgente. As principais ameaças para o horizonte 2025-2030 são identificadas como o terrorismo jihadista, os atores estatais hostis e o ciberterrorismo.

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.

Palavras-chave: infraestruturas críticas; terrorismo; segurança nacional; ciberterrorismo; ameaça híbrida.

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

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

ABREVIATURAS

CCN-CERT: Centro Criptológico Nacional – Equipa de Resposta a Emergências Informáticas

CITCO: Centro de Informações contra o Terrorismo e o Crime Organizado

CNI: Centro Nacional de Informações

CNPIC: Centro Nacional de Proteção de Infraestruturas Críticas

DSN: Departamento de Segurança Nacional

ENISA: Agência da União Europeia para a Cibersegurança

ICS: Industrial Control Systems (Sistemas de Controlo Industrial)

ICE: Infraestrutura Crítica Europeia

ICN: Infraestrutura Crítica Nacional

IoT: Internet das Coisas

NAA: Nível de Alerta Antiterrorista

NIS: Segurança das Redes e da Informação

PES: Plano Estratégico Setorial

PIC: Proteção de Infraestruturas Críticas

PNPIC: Plano Nacional de Proteção de Infraestruturas Críticas

PSO: Plano de Segurança do Operador

SCADA: Controlo de Supervisão e Aquisição de Dados

TE-SAT: Relatório da UE sobre a Situação e as Tendências do Terrorismo

ENCOT: Estratégia Nacional contra o Terrorismo

1. INTRODUÇÃO

O terrorismo sofreu uma transformação radical ao longo dos anos, tanto na sua natureza como nos objetivos que escolhe perseguir. Os ataques terroristas no século XX centravam-se predominantemente numa pequena percentagem de pessoas: líderes políticos, militares ou civis em instalações públicas. No entanto, atualmente, a tendência é para um aumento do número de ataques a infraestruturas e sistemas vitais que permitem o desenvolvimento e a vida de um Estado moderno. Esta evolução estratégica não é acidental; responde a uma lógica de maximização do impacto que os grupos terroristas e militantes têm vindo a aperfeiçoar ao longo do tempo: interromper os alicerces materiais da sociedade gera um impacto desestabilizador e psicológico muito maior do que o dos ataques convencionais, de elevada visibilidade mas de baixo impacto estrutural. Isto não é uma surpresa para a Espanha.

A 11 de março de 2004, quando vários comboios suburbanos que circulavam pela rede da Renfe em Madrid foram destruídos, tendo morrido 193 pessoas e ficado mais de 2 000 feridas, este constituiu o ataque terrorista mais devastador à infraestrutura de transportes de Espanha. Naquela altura, o sistema de proteção de infraestruturas críticas estava ainda na sua infância, mas o acontecimento catalisou um processo legislativo e organizacional que resultou na aprovação da Lei n.º 8/2011, de 28 de abril, o primeiro quadro regulamentar abrangente a nível nacional. Até ao momento, a experiência acumulada permitiu construir um sistema de proteção que agora enfrenta desafios qualitativos, decorrentes dos próprios desafios que estiveram na base da sua criação.

Na primeira metade da década de 2020, o contexto de ameaças na Europa tinha mudado consideravelmente. A agressão russa em curso contra a Ucrânia, desde fevereiro de 2022, demonstrou a vulnerabilidade das infraestruturas energéticas europeias face a atores estatais hostis, através do sabotagem dos gasodutos Nord Stream em setembro de 2022. E o terrorismo jihadista, particularmente ligado ao Daesh e à Al Qaeda, continua a ser uma ameaça persistente no contexto europeu, com células residuais ativas e uma preocupante capacidade de radicalização online para alimentar a figura do chamado «lobo solitário». Além disso, o radicalismo de direita tem registado um ressurgimento preocupante em muitos países da União Europeia, o que torna a aplicação de formas convencionais de ameaça terrorista mais abrangente, e não apenas um apelo ao jihadismo.

Este artigo pretende explorar, de um ponto de vista multidisciplinar e académico, a ameaça que os elementos terroristas representam para as infraestruturas críticas espanholas. Com vista a este objetivo, será analisada, tanto em Espanha como a nível europeu e internacional, a estrutura reguladora de referência; serão apresentados os setores estratégicos mais vulneráveis; será examinado o quadro institucional de referência do sistema CIP espanhol; e serão sugeridos mecanismos de melhoria, destinados a aumentar a capacidade de resiliência do sistema para o período de 2025 a 2030.

O presente estudo adota uma perspetiva integradora que combina a análise jurídica com a perspetiva das ciências da segurança e da criminologia, partindo do princípio de que as complexidades do fenómeno exigem uma abordagem plural e complementar. A hipótese orientadora que conduz a investigação é a seguinte: a Espanha dispõe de um sistema regulador robusto e de um quadro institucional que abrange as infraestruturas críticas de acordo com as normas europeias, mas também apresenta vulnerabilidades estruturais, especialmente no que diz respeito à cibersegurança industrial e à colaboração

público-privada, que os atores terroristas poderiam explorar num contexto de ameaça crescente e diversificada.

Seguindo esta hipótese, o documento demonstrará que a resposta a esta ameaça requer uma nova abordagem, que implique não só reformar o atual quadro regulamentar para as infraestruturas críticas, mas também repensar os modelos de governação e a parceria entre o setor público e os operadores privados de infraestruturas críticas. Esta metodologia específica resulta da análise documental de fontes primárias — legislação, relatórios oficiais, documentos estratégicos — e de fontes secundárias — literatura académica especializada, relatórios de organizações internacionais — durante um período de referência que vai desde a aprovação da Lei n.º 8/2011 até 2025.

2. METODOLOGIA

A investigação adota um desenho qualitativo baseado na análise documental sistemática, uma abordagem adequada para o estudo de fenómenos jurídico-institucionais em que a compreensão do quadro normativo e conceptual é prévia e necessária para qualquer avaliação empírica. A lacuna que o presente trabalho pretende colmatar reside na ausência de estudos que integrem de forma articulada as três dimensões — jurídica, institucional e operacional — do sistema espanhol de PIC face à ameaça terrorista, incorporando os mais recentes desenvolvimentos normativos europeus (Diretiva CER e NIS2, ambas de 2022) e a nova Estratégia Nacional contra o Terrorismo de 2023.

As fontes primárias incluem: legislação nacional (Lei n.º 8/2011, Decreto Real n.º 704/2011, Lei Orgânica n.º 4/2015, Decreto Real n.º 311/2022 e Decreto Real n.º 1150/2021); legislação europeia (Diretiva CER 2022/2557, Diretiva NIS2 2022/2555 e Diretiva 2008/114/CE); instrumentos internacionais (Resoluções do Conselho de Segurança da ONU 1373/2001 e 2341/2017; CETS n.º 196); e documentos estratégicos oficiais (Estratégia de Segurança Nacional de 2021, ENCOT 2023, relatórios anuais do CNPIC). As fontes secundárias incluem literatura académica especializada em segurança nacional, proteção de infraestruturas críticas e terrorismo, obtida através de uma pesquisa sistemática nas bases de dados Scopus, Web of Science e Google Scholar, com as palavras-chave: «critical infrastructure protection», «terrorism», «hybrid threats», «CIP Spain», «infraestruturas críticas», «terrorismo» e «resiliência»; bem como relatórios de organismos internacionais (Europol TE-SAT, ENISA Threat Landscape). Foram aplicados como critérios de inclusão: publicações em espanhol ou inglês, período 2001-2025 e pertinência direta com o objeto de estudo. Foram excluídos os trabalhos de caráter exclusivamente descritivo, sem contribuição analítica ou propositiva, bem como fontes não verificáveis ou de difusão restrita.

3. QUADRO CONCEITUAL: O QUE SÃO AS INFRAESTRUTURAS CRÍTICAS?

A noção de «infraestrutura crítica» não é inequívoca no meio académico nem na regulamentação. À medida que as sociedades modernas têm vindo a depender cada vez mais de determinados sistemas ou serviços críticos, a sua definição tem vindo a evoluir. Para efeitos do presente trabalho, no âmbito e de acordo com os parâmetros da Lei n.º 8/2011, entende-se por infraestrutura crítica as instalações, redes, serviços e equipamentos de tecnologia da informação e comunicação cuja interrupção ou destruição teria um impacto significativo na saúde, segurança ou bem-estar económico dos cidadãos, ou no funcionamento eficaz das instituições do Estado e das Administrações Públicas.

Esta definição aponta para uma visão do impacto potencial que se centra não tanto na natureza da infraestrutura, mas sim nas consequências da sua falha ou destruição para a sociedade no seu conjunto.

3.1. CLASSIFICAÇÃO SETORIAL

O artigo 2.º do Real Decreto n.º 704/2011 identifica doze setores estratégicos sujeitos a proteção ao abrigo do sistema PIC espanhol: administração, água, alimentação, energia, espaço, indústria nuclear, indústria química, instalações de investigação, saúde, sistema financeiro e fiscal, tecnologias da informação e da comunicação (TIC) e transportes. Esta categorização é consistente com a descrição apresentada na Diretiva (UE) 2022/2557 (Diretiva CER), que alarga o conjunto de setores para onze e que define explicitamente a infraestrutura digital, o espaço e a administração pública como categorias específicas.

A ponderação relativa em termos de segurança dos setores varia consoante os diferentes tipos de ameaças e as possíveis consequências de uma interrupção, mas, essencialmente, os setores da energia, dos transportes e das TIC estão, no contexto espanhol, relativamente concentrados no que diz respeito aos seus ativos-chave. Com base nos dados fornecidos pelo CNPIC, a Espanha conta com mais de 3 700 operadores críticos designados, distribuídos pelos doze setores estratégicos, sendo os setores das TIC e da energia aqueles que concentram o maior número de operadores em termos absolutos.

3.2. INFRAESTRUTURAS CRÍTICAS NACIONAIS E INFRAESTRUTURAS CRÍTICAS EUROPEIAS

A diferença entre a infraestrutura crítica nacional (ICN) e a infraestrutura crítica europeia (ICE) é especialmente relevante à luz da legislação da UE. Uma infraestrutura é designada como ICE se a sua interrupção ou destruição afetar gravemente dois ou mais Estados-Membros, ou a UE no seu conjunto. A Diretiva 2008/114/CE foi a primeira a estabelecer este conceito; inicialmente, restringiu o seu âmbito aos setores da energia e dos transportes. A Diretiva CER de 2022 alarga o âmbito do conceito e reforça os meios para identificar e proteger estas infraestruturas. A Espanha classificou várias destas instalações como ICE, principalmente nos setores da energia e dos transportes, dado o papel estratégico do país como corredor de energia e comunicações entre a Europa e o Norte de África, uma posição geopolítica que, embora confira à Espanha um papel central na arquitetura de segurança europeia, aumenta a sua exposição a certas ameaças transnacionais.

3.3. O CONCEITO DE INTERDEPENDÊNCIA

Um tema central da análise das infraestruturas críticas é o problema da interdependência. Os sistemas críticos atuais não funcionam isoladamente; dependem em grande medida de outros sistemas dos quais dependem para o seu funcionamento. A indústria elétrica depende das infraestruturas de telecomunicações para a sua gestão automatizada; o transporte ferroviário é alimentado por energia elétrica; e o setor financeiro depende das TIC para praticamente todas as suas operações. Essa interdependência cria o que a literatura especializada denomina «efeitos em cascata»: a falha de uma infraestrutura pode causar a falha sucessiva de outras, com um resultado eventualmente devastador para todo o sistema (Rinaldi et al., 2001).

O aprofundamento da digitalização dos sistemas críticos — associado às tecnologias da Internet das Coisas (IoT), às plataformas de dados na nuvem e aos sistemas de controlo industrial SCADA — ampliou estas interdependências, dando origem a novos vetores de vulnerabilidade que grupos terroristas mais sofisticados estão a começar a explorar sistematicamente. Esta interdependência não é apenas uma questão de natureza técnica ou cibernética; envolve aspetos geográficos — infraestruturas transfronteiriças, como redes elétricas ou gasodutos —, cibernéticos — sistemas de controlo partilhados ou interligados — e organizacionais — operadores que gerem ativos em numerosos setores.

A natureza multifacetada dessa interdependência torna a análise do risco das infraestruturas críticas um processo de imensa complexidade que não pode ser reduzido à análise de cada infraestrutura de forma independente.

4. QUADRO NORMATIVO DE REFERÊNCIA

A proteção das infraestruturas críticas contra ameaças terroristas e outras ameaças intencionais articula-se através de um quadro regulamentar complexo e multinível, que inclui disposições nacionais, europeias e internacionais. Esta arquitetura regulamentar reflete também a compreensão crescente de que a ameaça às infraestruturas críticas transcende as fronteiras nacionais e exige respostas coordenadas a diferentes níveis de governação. Cada um destes níveis é abordado nas secções seguintes, com destaque para os mais recentes desenvolvimentos regulamentares e os desafios que a sua implementação coloca.

4.1. LEGISLAÇÃO ESPANHOLA

A Lei n.º 8/2011, de 28 de abril, constitui a base da legislação nacional espanhola em matéria de proteção das infraestruturas críticas. Esta lei transpõe a Diretiva 2008/114/CE para o direito espanhol e estabelece o Sistema de Proteção de Infraestruturas Críticas, um instrumento que se baseia em três princípios fundamentais: o Centro Nacional de Proteção de Infraestruturas Críticas (CNPIC), o Catálogo Nacional de Infraestruturas Estratégicas e o planeamento da proteção. Distingue entre o Plano Nacional de Proteção de Infraestruturas Críticas (PNPIC), os Planos Estratégicos Setoriais (PES) e os Planos de Segurança do Operador (PSO) no quadro jurídico espanhol e proporciona um plano «escalonado e de alto nível» que se desenvolve desde o nível geral até ao específico. A implementação normativa da Lei PIC é levada a cabo através do Real Decreto n.º 704/2011, de 20 de maio, que estabelece a aplicação para a proteção das infraestruturas críticas.

Esta regulamentação estabelece os critérios para a designação de operadores críticos, o conteúdo mínimo dos Planos de Segurança do Operador e dos Planos de Proteção Específicos, bem como as responsabilidades em matéria de comunicação de incidentes. É especialmente relevante o artigo 24.º, que estabelece o regime de inspeção/supervisão dos operadores críticos, o que, por sua vez, permite ao CNPIC verificar o cumprimento das obrigações de segurança. Vários autores têm salientado que esta supervisão do cumprimento, na prática, tem sido apontada como uma fra e do sistema, devido ao grande número de operadores e aos recursos limitados para a gestão operacional. A Estratégia de Segurança Nacional de 2021, nos termos do Real Decreto n.º 1150/2021, identifica o terrorismo como um dos principais riscos e ameaças para Espanha e considera a proteção das infraestruturas críticas como um dos objetivos

ambiciosos do sistema de segurança nacional, no âmbito da abordagem holística de segurança que caracteriza o sistema espanhol.

Em consonância com isto, a Estratégia Nacional contra o Terrorismo (ENCOT) de 2023 — que atualiza e substitui a versão de 2019 — estrutura a resposta antiterrorista do Estado em torno de quatro pilares de ação (prevenir, proteger, perseguir e responder) e coloca a proteção das infraestruturas críticas no centro do pilar «proteger». A ENCOT 2023 introduz uma novidade conceptual de primeira ordem ao assumir institucionalmente que a invulnerabilidade absoluta é inatingível, deslocando o foco estratégico da mera proteção estática para a resiliência integral, entendida como a capacidade de absorver o impacto de um incidente, garantir a continuidade dos serviços essenciais e restabelecer rapidamente a normalidade. Esta visão está em plena sintonia com a abordagem da Diretiva CER de 2022, o que torna a ENCOT 2023 uma ponte doutrinária entre a estratégia antiterrorista nacional e o quadro europeu de entidades críticas. Além disso, a ENCOT 2023 alerta para a deslocação da ameaça para os chamados «alvos fáceis» — locais de culto, celebrações com grande afluência de público e espaços públicos — que, sem constituírem infraestruturas críticas no sentido técnico, são determinantes para a segurança dos cidadãos; uma realidade que diz diretamente respeito ao âmbito de aplicação da futura legislação de transposição. Em termos de cibersegurança, o Esquema Nacional de Segurança, aprovado pelo Real Decreto n.º 311/2022, estabelece requisitos mínimos para os sistemas de informação das Administrações Públicas e dos seus operadores de serviços essenciais, completando assim o regime PIC no que diz respeito aos ativos de informação dos operadores críticos.

A Lei Orgânica n.º 4/2015, de 30 de março, relativa à Proteção da Segurança Cívica, introduz medidas relevantes de controlo de acesso a instalações sensíveis e de vigilância de ambientes de risco, complementando o sistema de proteção física previsto pelos regulamentos PIC.

4.2. REGULAMENTAÇÃO EUROPEIA

O quadro regulamentar da União Europeia foi profundamente revisto na sequência da aprovação da Diretiva (UE) 2022/2557 (14 de dezembro de 2022) relativa à resiliência das entidades críticas (Diretiva CER). Esta regulamentação substitui a Diretiva 2008/114/CE e cria um quadro reconcebido que se centra mais na resiliência integral das entidades que operam infraestruturas, em vez de apenas no fornecimento físico e na proteção dos sistemas, definida como a sua capacidade de evitar incidentes, suportar o seu impacto, responder às consequências e recuperar-se rapidamente. Os principais desenvolvimentos na Diretiva CER incluem o alargamento do âmbito setorial de dois setores para onze, a necessidade de requisitos reforçados em matéria de análise de riscos e relatórios de incidentes, e o estabelecimento de um mecanismo da UE para apoiar os Estados-Membros na identificação de entidades críticas, ou seja, aquelas com particular relevância europeia.

O prazo para a transposição da Diretiva CER terminou a 17 de outubro de 2024. A Espanha não tinha concluído este processo até essa data, o que a colocou numa situação de incumprimento que poderá conduzir a um processo de infração por parte da Comissão Europeia, caso se prolongue. Este atraso resulta da complexidade técnica e política que implica uma transposição que envolve a alteração ou revogação da Lei n.º 8/2011 e do seu regulamento de aplicação, bem como uma revisão do Catálogo Nacional de

Infraestruturas Estratégicas para o adaptar aos novos setores abrangidos e reformar os mecanismos de cooperação interministerial e intersetorial.

A Diretiva NIS2 (Diretiva (UE) 2022/2555), que foi aprovada no mesmo dia que a Diretiva CER, revê e revoga a Diretiva NIS de 2016 e estabelece medidas para manter um elevado nível comum de cibersegurança em toda a UE. Alarga consideravelmente o âmbito das regulamentações em matéria de cibersegurança, passando de «operadores de serviços essenciais» para «entidades essenciais e importantes», e implica responsabilidades reforçadas baseadas na gestão de riscos, na comunicação de incidentes e na cooperação transfronteiriça.

A interação entre a Diretiva CER e a NIS2 é um dos aspetos mais complexos deste novo quadro europeu: ambas as diretivas aplicam-se a muitas das mesmas entidades, mas a partir de perspetivas diferentes, nomeadamente (1) a resiliência física integral e (2) a cibersegurança, o que implica uma abordagem que exigirá coordenação durante a transposição, a fim de evitar sobreposições e contradições.

4.3. QUADRO INTERNACIONAL

No cenário internacional, a Resolução 1373 (2001) do Conselho de Segurança das Nações Unidas estabelece as obrigações de todos os Estados na luta contra o terrorismo, que incluem requisitos para implementar medidas que impeçam a utilização do seu território para atividades terroristas e a troca de informações com outros Estados.

A Resolução 2341 (2017) do Conselho de Segurança é o primeiro instrumento deste órgão especificamente dedicado à proteção de infraestruturas críticas contra o terrorismo, instando os Estados a desenvolverem medidas de proteção proporcionais ao risco identificado, promovendo a cooperação internacional no que diz respeito à dimensão cibernética da ameaça. A Convenção para a Prevenção do Terrorismo (CETS n.º 196), em vigor desde 2007, e o seu Protocolo Adicional de 2015 estabelecem obrigações em matéria de criminalização e cooperação judicial que complementam o quadro da ONU.

5. O TERRORISMO COMO AMEAÇA ESPECÍFICA CONTRA INFRAESTRUTURAS CRÍTICAS

5.1. TIPOLOGIA DE GRUPOS TERRORISTAS COM INTERESSE EM INFRAESTRUTURAS CRÍTICAS

O fenómeno do terrorismo surge, portanto, como uma das ameaças mais complexas e multifacetadas às infraestruturas essenciais da sociedade contemporânea. Ao contrário de outras ameaças, como as catástrofes naturais ou as falhas tecnológicas acidentais, o terrorismo caracteriza-se por uma intenção maliciosa e uma racionalidade estratégica, o que significa que os terroristas adaptam e renovam as suas táticas, técnicas e procedimentos em função das medidas de proteção implementadas. Uma resposta de proteção eficaz exige, por isso, uma reação igualmente dinâmica e proativa face à natureza adaptativa e e e da ameaça, que não se pode limitar a medidas de segurança físicas e lógicas de caráter estático.

5.1.1. Terrorismo jihadista

O terrorismo inspirado por jihadistas, particularmente associado a grupos como o Daesh e a Al Qaeda, tem manifestado repetidamente o seu interesse estratégico em atacar infraestruturas-chave em países ocidentais. Nos folhetos publicados, por exemplo, na Dabiq ou na Inspire, ambos os grupos incluíram orientações explícitas para atacar centrais elétricas, fontes de água potável e instalações de transportes na Europa e na América do Norte, prestando especial atenção aos efeitos em cadeia decorrentes da interrupção de infraestruturas interligadas.

Em Espanha, mais especificamente, o ataque (em agosto de 2017) na Rambla, em Barcelona, e em Cambrils, perpetrado por uma célula do Daesh, refletiu como a ameaça jihadista continuava presente a nível nacional, embora, desta vez, o seu objetivo fosse causar baixas em espaços públicos, em vez de atacar uma infraestrutura específica. De acordo com o relatório TE-SAT 2024 da Europol, o terrorismo jihadista continua a ser a ameaça mais grave para a União Europeia em termos de número de operações, detenções e ataques cometidos ou frustrados.

Neste contexto, a Espanha encontra-se numa posição especialmente vulnerável: o seu estatuto de país de trânsito entre o Norte de África e a Europa, os fluxos migratórios que atravessam as suas fronteiras meridionais e a presença de comunidades com níveis documentados de radicalização. O modelo do «lobo solitário», que age de forma autónoma após ter sido radicalizado através de meios digitais, apresenta desafios únicos em termos de deteção precoce e é, atualmente, o perfil mais provável de ataques terroristas inspirados por jihadistas em solo espanhol.

5.1.2. Atores estatais hostis e ameaças híbridas

Este tipo de atores estatais hostis merece uma consideração especial no âmbito das ameaças à infraestrutura crítica. O conjunto de provas recolhidas desde 2014 sugere que a Rússia desenvolveu e mobilizou capacidades avançadas para sabotar infraestruturas críticas na Europa, através de meios cibernéticos diretos (incluindo ataques do grupo Sandworm contra a rede elétrica ucraniana em 2015 e 2016) e por meio de atividades encobertas de sabotagem física.

O caso mais espetacular é a sabotagem dos gasodutos Nord Stream em setembro de 2022, que interrompeu o fornecimento de gás natural da Rússia para a Europa e demonstra a disposição dos atores estatais para atacar as infraestruturas da Europa com a intenção de as utilizar como alavanca geopolítica.

O conceito de «ameaça híbrida» refere-se à combinação de uma série de ferramentas tradicionais e não convencionais, incluindo desinformação, ciberataques, sabotagem física e pressão económica, para criar uma «estratégia de ameaça híbrida» integrada, concebida para enfraquecer um Estado sem entrar na categoria de confronto armado convencional. Este tipo de ameaça, em que a Rússia tem assumido o papel de força mais ativa na Europa nos últimos anos, apresenta uma dificuldade particular para os sistemas cujo objetivo principal é proteger as infraestruturas críticas, onde a ameaça subjacente é abordada como se fossem ameaças tradicionais isoladas. O Irão e e a Coreia do Norte, que também são considerados pelos especialistas como atacantes cibernéticos de infraestruturas críticas, demonstraram possuir capacidades de ciberataque contra

infraestruturas críticas, embora o seu perigo real para o território espanhol seja agora considerado menos substancial do que a ameaça russa.

5.1.3. Terrorismo de extrema-direita

Embora o terrorismo de extrema-direita geralmente não se concentre em atacar infraestruturas como o terrorismo jihadista, tem sido associado a vários incidentes graves na Europa nos últimos anos. Os ataques em Utøya (Noruega, 2011), Hanau (Alemanha, 2020) e Christchurch (Nova Zelândia, 2019) destacaram a capacidade letal deste tipo de atores.

No âmbito das infraestruturas críticas, algumas células extremistas de direita têm demonstrado interesse em atacar infraestruturas de comunicações, energia ou transportes como forma de desestabilizar a sociedade e provocar um colapso da ordem estabelecida, o que estes grupos designam por «aceleração». Este fenómeno é reconhecido como uma ameaça emergente pela Estratégia da UE para a União da Segurança 2020-2025, que defende que, tanto no domínio da informação como no das ferramentas regulatórias, deve ser tratado e abordado com a mesma seriedade que o terrorismo jihadista.

5.2. CASOS HISTÓRICOS RELEVANTES

O ataque de 11 de março de 2004 em Madrid continua a ser, sem dúvida, o caso de referência em Espanha. Durante as horas de ponta da manhã, a detonação coordenada de dez explosivos em comboios suburbanos constituiu uma exploração das vulnerabilidades inerentes aos sistemas de transportes públicos; estes são abertos, os utilizadores estão concentrados e é difícil implementar uma infraestrutura de segurança integral sem sacrificar a eficiência do serviço. O ataque resultou em 193 mortos e mais de 2 000 feridos e teve um grande impacto económico e social (Reinares, 2014). Não só teve um efeito imediato: o dia 11 de março revelou que a infraestrutura de transporte ferroviário apresentava vulnerabilidades estruturais que não tinham sido suficientemente consideradas nos planos de segurança da época. A nível europeu, o ataque de 2016 em Bruxelas, que envolveu a explosão de engenhos explosivos no Aeroporto Internacional de Zaventem e no metro da cidade, demonstra como os terroristas são capazes de atacar dois ou mais nós das infraestruturas de transportes de uma só vez, obtendo o máximo efeito psicológico e mediático.

Um aeroporto internacional é considerado um alvo deliberado: este tipo de aeroporto concentra grandes volumes de pessoas de diferentes nacionalidades em locais únicos, que recebem grande atenção mediática internacional, a tal ponto que a sua interrupção gera efeitos económicos e de imagem desproporcionais em relação ao custo material do ataque. No contexto espanhol, uma série de sabotagens a infraestruturas de fibra ótica registadas em várias comunidades autónomas em 2024 sublinhou a vulnerabilidade das redes de telecomunicações face a atos intencionais de destruição; demonstrando que a desativação de infraestruturas vitais pode ser levada a cabo com técnicas relativamente simples, nos casos em que os ativos apresentam uma proteção física inadequada.

5.3. O CIBERTERRORISMO E OS ATAQUES HÍBRIDOS COMO NOVA FRONTEIRA

O ciberterrorismo, definido como a utilização intencional de capacidades informáticas (para intimidação ou pressão política) com o objetivo de causar estragos em infraestruturas críticas, é o aspeto mais recente — e possivelmente mais disruptivo — do ataque terrorista contra infraestruturas de elevado valor. E, ao contrário do terrorismo tradicional, os ciberataques podem ser levados a cabo à distância, em alguns casos sem serem identificáveis, e a partir de diferentes locais, o que torna a atribuição de responsabilidades e o controlo um desafio muito mais complexo para as autoridades.

A interligação e a fusão do ciberespaço com o controlo industrial conduziram ao que alguns designam como o «quinto domínio da guerra» (Clarke e Knake, 2010), onde os terroristas são capazes de infligir danos físicos reais a estruturas críticas sem terem de se encontrar nas suas proximidades. O ataque dos Estados Unidos à Colonial Pipeline (maio de 2021), utilizando ransomware, sublinhou o quão indefesas as infraestruturas energéticas críticas estão perante tais ciberataques e a rapidez com que esses ataques podem conduzir à escassez de abastecimento e ao alarme social.

Na Europa, os ciberataques à empresa de eletricidade ucraniana Ukrenergo em 2015 e 2016, levados a cabo por indivíduos associados ao Estado russo, deixaram vastas áreas da Ucrânia sem eletricidade durante várias horas, um prenúncio de que os ataques às infraestruturas energéticas na Europa poderiam surgir num momento de crescente conflito geopolítico.

De acordo com o inquérito «ENISA Threat Landscape 2024», a ameaça cibernética às infraestruturas industriais em setores essenciais aumentou na Europa em 78 % entre 2022 e 2023, demonstrando as tendências crescentes neste tipo de ataques.

6. VULNERABILIDADES DAS INFRAESTRUTURAS CRÍTICAS ESPANHOLAS

Num esforço para analisar as vulnerabilidades do sistema de infraestruturas críticas espanhol face à ameaça terrorista, a abordagem deve ser setorial — tendo em conta as características específicas de cada setor estratégico — e transversal, identificando as fraquezas estruturais comuns a todo o sistema. As secções que se seguem abordam, em primeiro lugar, as vulnerabilidades específicas dos setores de maior risco, seguidas de uma análise dos fatores transversais de vulnerabilidade.

6.1. ANÁLISE SETORIAL DAS VULNERABILIDADES

6.1.1. Setor energético

O setor energético representa um dos alvos prioritários para os grupos terroristas sofisticados, devido à magnitude do impacto potencial de um ataque bem-sucedido. A Espanha opera uma rede elétrica de alta tensão, que liga o sistema peninsular às Ilhas Canárias e Baleares e à França e Portugal através dos interligadores pirenaicos, sendo operada pela Red Eléctrica de España (REE). A concentração de ativos cruciais em alguns nós da rede — centrais de produção, centros de dispatching ou transformadores de alta tensão — e o facto de a sua substituição, após danos graves, demorar meses, cria

vulnerabilidades específicas a ataques físicos ou cibernéticos coordenados. Além disso, as centrais nucleares existentes e em funcionamento em Espanha — Almaraz, Ascó, Cofrentes, entre outras — necessitam de proteção a diferentes níveis devido aos efeitos potencialmente catastróficos de incidentes nas instalações, mas a sua segurança física e radiológica é monitorizada em permanência pelo Conselho de Segurança Nuclear (CSN).

6.1.2. Setor dos Transportes

A Espanha possui uma das redes ferroviárias de alta velocidade mais extensas do mundo, com mais de 3 900 quilómetros de linhas de alta velocidade em funcionamento. Esta infraestrutura, com a concentração de passageiros em grandes estações — Atocha, Sants, Santa Justa —, além de certos elementos que a tornam vulnerável, como túneis, viadutos e sistemas de sinalização, representa alvos principais para os terroristas explorarem. O Aeroporto Adolfo Suárez Madrid-Barajas, o quarto aeroporto mais movimentado da Europa, com mais de 62 milhões de passageiros por ano, e o Porto de Algeciras, o principal porto de contentores de Espanha e uma porta de entrada para mercadorias provenientes do Norte de África, apresentam características de alto risco que exigem medidas de segurança particularmente rigorosas.

6.1.3. Setor das TIC

A infraestrutura digital de Espanha tem crescido rapidamente nos últimos anos devido à digitalização da economia, bem como à tecnologia 5G e à implementação de infraestruturas de computação em nuvem. Os cabos de comunicações submarinos que ligam a Espanha ao resto do mundo — incluindo aqueles que ligam a Península Ibérica às Ilhas Canárias e ao continente americano — também se tornaram um vetor de vulnerabilidade de primeira ordem, tal como comprovam os incidentes registados no Mar Vermelho e no Mar Báltico entre 2023 e 2025. Estes cabos concentram a maior parte do tráfego internacional de dados e voz, e os seus danos intencionais poderiam conduzir a uma perda de capacidade de comunicação à escala continental. Dada a dispersão geográfica dos ativos das TIC e a rápida evolução tanto das tecnologias como dos vetores de ataque, o CNPIC salientou que o setor das TIC coloca alguns dos desafios mais urgentes em termos de proteção.

6.2. RISCOS DECORRENTES DA DIGITALIZAÇÃO E DA CONECTIVIDADE

A adoção de tecnologias da informação (TI) e tecnologias operacionais (OT) em contextos industriais é uma das tendências mais importantes — e mais preocupantes do ponto de vista da segurança — dos últimos dez anos. A chamada «brecha de ar» entre os sistemas de controlo industrial (ICS/SCADA) e as redes corporativas e a Internet provocou uma integração gradual dos sistemas de TI em ambientes digitais, com o objetivo de melhorar a eficácia operacional e a gestão de reparações remotas.

Esta conectividade cria novas superfícies de ataque que podem ser exploradas por grupos terroristas com capacidades cibernéticas avançadas. O número de dispositivos IoT instalados como elementos-chave em sistemas críticos — tais como: sensores de temperatura, câmaras de segurança e sistemas de controlo de acesso — agrava a ameaça ao incluir componentes que não são inerentemente seguros quando integrados em sistemas operacionais críticos para a segurança. A ausência de atualizações de segurança de dispositivos integrados, a existência de protocolos de comunicação industrial obsoletos

sem capacidades criptográficas e a falta de profissionais especializados em cibersegurança no setor industrial aumentam significativamente este nível de vulnerabilidade.

6.3. COORDENAÇÃO PÚBLICO-PRIVADA: O DESAFIO PENDENTE

Uma característica sistémica do sistema de infraestruturas críticas de Espanha que criou vulnerabilidades específicas é o facto de a maioria dos operadores críticos ser de propriedade privada. Dos cerca de 3 700 operadores designados em Espanha, a maioria são entidades privadas ou mistas, o que representa um desafio contínuo para os interesses privados que privilegiam os lucros e a eficiência em detrimento da segurança nacional.

Neste sentido, e no contexto destas obrigações, em combinação com o disposto na Lei PIC, os operadores críticos devem elaborar Planos de Segurança do Operador e Planos de Proteção Específicos para a sua operação; no entanto, o investimento realizado nestes esquemas excede frequentemente os requisitos mínimos de conformidade com a Lei PIC, pelo menos nos casos em que existem muito poucas razões económicas para aceitar tal montante de capital. A partilha de informação e a confiança mútua entre os setores público e privado são destacadas pela literatura especializada como componentes críticos para a eficácia do sistema PIC (Moteff, 2014).

A este respeito, a Espanha estabeleceu mecanismos para a troca de informações e sistemas de alerta precoce através do CNPIC; no entanto, a integração completa dos operadores privados no sistema de inteligência de ameaças continua a ser uma área crítica em que o progresso não pode ser limitado. A assimetria de informação entre as autoridades competentes, que podem recorrer a informações classificadas sobre ameaças, e os operadores privados, que necessitam desse conhecimento para calibrar os seus investimentos em segurança, constitui um dos obstáculos mais persistentes à construção de uma cooperação público-privada eficaz no âmbito da PIC.

7. O SISTEMA ESPANHOL DE PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

7.1. ARQUITETURA INSTITUCIONAL

O Sistema de Proteção de Infraestruturas Críticas de Espanha assenta numa estrutura institucional complexa que interliga instituições de diversos tamanhos e especialidades. O CNPIC, no âmbito da Secretaria de Estado da Segurança do Ministério do Interior, assume a função de desenvolver, coordenar e supervisionar o sistema. É responsável pela regulamentação do Catálogo Nacional de Infraestruturas Estratégicas, o inventário classificado do país sobre infraestruturas críticas, pelo planeamento de esquemas de proteção coordenados e pelo acompanhamento do cumprimento por parte dos operadores críticos.

O CNPIC conta com a cooperação permanente do Centro de Informações contra o Terrorismo e o Crime Organizado (CITCO), a instituição encarregada de fornecer informações antiterroristas e sobre a Espanha, para proporcionar medidas de proteção baseadas no risco que possam neutralizar ameaças. O Centro Nacional de Informações (CNI), através do Centro Criptológico Nacional (CCN) e da sua equipa de resposta a incidentes CCN-CERT, é o organismo competente em matéria de cibersegurança para as

administrações públicas e os sistemas de informação dos operadores de serviços essenciais.

A complementaridade inerente às funções do CNPIC (centradas na proteção física e no planeamento da segurança) e do CCN-CERT (centrada na cibersegurança) é fundamental para a proteção eficaz das infraestruturas críticas face a uma ameaça que pode ser concebida tanto como física como cibernética. A recente coordenação operacional entre ambas as organizações evoluiu significativamente, levando-as a unir forças para criar grupos de trabalho e protocolos destinados à partilha de informações sobre incidentes de natureza mista.

O Departamento de Segurança Nacional (DSN) é responsável pela coordenação estratégica de todo o sistema de segurança nacional, incluindo a proteção das infraestruturas críticas, e está subordinado à Presidência do Governo. Em matéria de segurança nacional, o DSN encarrega-se do desenvolvimento e acompanhamento das Estratégias de Segurança Nacional e atua como elo de ligação com os instrumentos de coordenação estratégica da OTAN e da UE.

As Forças e Corpos de Segurança do Estado — Polícia Nacional e Guardia Civil — e as Forças Armadas, através das suas unidades especializadas, completam o quadro institucional com especialização nacional em proteção física, intervenção em incidentes graves e apoio às autoridades civis. Merece especial atenção o papel operacional da Guardia Civil neste sistema. Através das suas unidades especializadas — em particular a Unidade Central Operativa (UCO), a Unidade de Cibercriminalidade (UCC) e as Equipas de Ativação de NBQR —, a Guardia Civil mobiliza capacidades específicas de resposta a incidentes físico-cibernéticos em infraestruturas críticas de natureza rural, industrial e de transportes, que são precisamente os ambientes mais expostos a ameaças híbridas. A estreita coordenação técnico-policial entre a Guardia Civil e o CNPIC articula-se através de protocolos de ação conjunta que permitem ativar, em função do nível de alerta antiterrorista em vigor, dispositivos específicos de proteção de infraestruturas nos setores da energia, dos transportes e da água. Esta complementaridade entre a capacidade de inteligência tática das Forças e Corpos de Segurança e a função de coordenação estratégica do CNPIC constitui um dos ativos diferenciadores do modelo espanhol de PIC no contexto europeu comparativo.

7.2. O SISTEMA DE NÍVEIS DE ALERTA ANTITERRORISTA (NAA)

O Nível de Alerta Antiterrorista (NAA) refere-se ao mecanismo estabelecido para implementar medidas de proteção que correspondam à ameaça terrorista existente nesse momento. O NAA de cinco níveis, que foi atualizado pela Resolução do Secretário de Estado da Segurança em 2019 — que vai do 1 (baixo) ao 5 (muito elevado) —, é complementado por um catálogo de medidas de segurança aplicadas progressivamente a vários setores estratégicos.

Desde junho de 2015, tem sido aplicado em Espanha o nível 4 (alto), que inclui a implementação de estruturas de segurança reforçadas para todos os setores estratégicos, tais como controlos em torno das infraestruturas de transportes, o reforço da vigilância perimetral de instituições-chave e a ativação de protocolos de comunicação prioritários em caso de incidentes.

A ligação entre o NAA e o sistema PIC é assegurada através de Planos de Resposta, que determinam as ações específicas que os operadores críticos devem tomar de acordo com o nível de alerta atual. Isto permite uma resposta escalonada e coordenada à medida que o nível de ameaça varia. No entanto, manter o nível de alerta 4 durante mais de dez anos poderá conduzir a uma certa «fadiga de alerta» por parte dos operadores críticos, cujas medidas de proteção associadas a esse nível podem tornar-se uma rotina e uma parte do seu trabalho em que a vigilância é insuficiente.

A implicação é que é necessário rever periodicamente o sistema de alerta e estabelecer mecanismos para avaliar a verdadeira eficácia de todas as medidas tomadas.

7.3. COOPERAÇÃO INTERNACIONAL

A dimensão internacional da proteção das infraestruturas críticas é cada vez mais relevante num contexto em que as ameaças são de natureza transnacional. A Espanha participa ativamente em diversas iniciativas de cooperação multilateral neste domínio. No âmbito da Europol, a Rede Atlas de Unidades de Intervenção Especial facilita a cooperação operacional entre as forças policiais dos Estados-Membros em situações de crise terrorista que possam afetar as infraestruturas críticas.

O Conselho Consultivo da Associação para as Infraestruturas Críticas da UE (CP-ISAC) promove o intercâmbio de informações e de melhores práticas entre as autoridades nacionais e os operadores críticos europeus. No âmbito da OTAN, a Espanha participa nos mecanismos de proteção das infraestruturas críticas da Aliança, que foram significativamente reforçados após a cimeira de Madrid de 2022, reconhecendo a resiliência das infraestruturas críticas como um elemento central da defesa coletiva.

8. DESAFIOS E PROPOSTAS DE MELHORIA

A análise preliminar permite identificar os desafios e as lacunas no sistema espanhol de proteção das infraestruturas críticas que requerem atenção urgente. As propostas aqui apresentadas estão longe de ser exaustivas, mas delineiam as linhas de ação mais urgentes com maior potencial de mudança positiva para melhorar a resiliência do sistema face à ameaça terrorista.

8.1. TRANSPOSIÇÃO URGENTE DA DIRETIVA CER

Por conseguinte, é necessário alterar o quadro regulamentar de acordo com os termos da Diretiva CER, de modo a atingir o nível necessário para manter a coerência do sistema espanhol com o quadro europeu e tirar o máximo partido dos mecanismos de apoio integrados na diretiva.

Recomenda-se vivamente a aprovação desta legislação, através de uma lei de re-promulgação que abranja a proteção de infraestruturas e entidades críticas, que revogue a Lei n.º 8/2011 e que funda os elementos da Diretiva CER com as disposições da NIS2 num único regime regulamentar, com melhorias significativas nos mecanismos de monitorização do cumprimento por parte dos operadores. Esta nova regulamentação deverá implementar um sistema de incentivos — deduções fiscais ou acesso preferencial ao financiamento público — para que os operadores privados invistam voluntariamente em medidas destinadas a aumentar a resiliência para além dos mínimos legais. Por

conseguinte, é necessário que a nova lei exija a participação ativa dos operadores críticos no processo, de modo a alinhar-se formalmente com a realidade operacional de cada setor.

8.2. REFORÇO DA CIBERSEGURANÇA INDUSTRIAL

A convergência entre TI e OT em ambientes críticos requer um investimento contínuo em cibersegurança industrial que vá além do cumprimento mínimo dos requisitos regulamentares. Recomenda-se a implementação de um Plano Nacional de Cibersegurança Industrial para estabelecer normas específicas para os sistemas SCADA/ICS de operadores críticos, promover a certificação de componentes industriais com referência ao Regulamento (UE) 2019/881 e apoiar a atualização de sistemas legados com vulnerabilidades conhecidas. O CCN-CERT deverá melhorar ainda mais a sua capacidade de apoiar os operadores do setor privado crítico em matéria de cibersegurança industrial, criando equipas setoriais especializadas (energia, transportes e água, como prioridade) que possam prestar apoio técnico específico em caso de incidentes mistos físico-cibernéticos.

8.3. MELHORIA DA COORDENAÇÃO PÚBLICO-PRIVADA

A criação de plataformas setoriais para o intercâmbio de informações sobre ameaças, em consonância com o modelo dos Centros de Intercâmbio e Análise de Informações dos Estados Unidos (ISAC), representa uma prioridade para melhorar a cooperação entre o setor público e os operadores privados. Estas plataformas, que deveriam funcionar sob a égide do CNPIC e com a participação do CCN-CERT e do CITCO, permitiriam um fluxo bidirecional de informação sobre ameaças, vulnerabilidades e incidentes, o que reforçaria a capacidade de resposta de todo o sistema.

Uma condição essencial para a sua eficácia é a adoção de um quadro jurídico que garanta a confidencialidade da informação partilhada pelos operadores privados, eliminando o risco de que a sua divulgação gere responsabilidades legais ou vantagens competitivas para os seus concorrentes.

8.4. FORMAÇÃO E EXERCÍCIOS DE SIMULAÇÃO

A resiliência das infraestruturas críticas face a ataques terroristas depende, em grande medida, da preparação do pessoal que as gere e proteja. Recomenda-se a institucionalização de um programa nacional de formação em proteção de infraestruturas críticas, com módulos específicos para operadores em diferentes setores, e a realização anual de exercícios de simulação de crises que contemplem cenários de ataques físicos e cibernéticos combinados. Estes exercícios, que devem envolver simultaneamente as autoridades competentes, as forças de segurança e os operadores críticos, permitem identificar lacunas nos planos de resposta, reforçar a coordenação entre os intervenientes e manter atualizada a cultura de segurança das organizações. O Centro Europeu de Excelência para o Combate às Ameaças Híbridas (Hybrid CoE), em Helsínquia, é um parceiro relevante para a conceção e implementação destes exercícios na dimensão transnacional.

8.5. INTELIGÊNCIA ANTECIPATÓRIA

Antecipar as ameaças terroristas contra infraestruturas críticas requer o reforço das capacidades de inteligência estratégica do CITCO e do CNI, com especial atenção à análise das tendências nas aspirações operacionais de grupos terroristas e atores estatais hostis contra alvos de infraestrutura. A integração de dados de fontes abertas, incluindo a monitorização sistemática de fóruns extremistas na dark web e a análise de publicações de organizações terroristas, deve ser sistematizada como parte da avaliação específica das ameaças contra cada setor estratégico.

O desenvolvimento de capacidades de inteligência artificial aplicadas à análise de ameaças contra infraestruturas críticas representa uma linha de investimento promissora, embora a sua implementação deva ser acompanhada de garantias legais adequadas que salvaguardem os direitos fundamentais.

9. CONCLUSÕES

A análise desenvolvida neste documento permite-nos extrair as seguintes conclusões sobre a ameaça terrorista que paira sobre as infraestruturas críticas espanholas e o estado atual do sistema de proteção.

Em primeiro lugar, a Espanha dispõe de um quadro normativo e institucional para a proteção das infraestruturas críticas, que, no seu conjunto, proporciona um nível de proteção adequado em termos comparativos europeus. A Lei n.º 8/2011 e a sua regulamentação de execução constituem a pedra angular de um sistema coerente que tem demonstrado, ao longo de mais de dez anos, a sua eficácia na coordenação interinstitucional e na gestão de incidentes. No entanto, o atraso na transposição da Diretiva CER de 2022 deixa um vazio de incerteza normativa que prejudica a posição da Espanha no sistema europeu de proteção das infraestruturas críticas e deve ser resolvido com urgência através de nova legislação que incorpore a abordagem de resiliência integral que caracteriza o novo quadro europeu.

Em segundo lugar, o terrorismo jihadista continua a ser a principal ameaça terrorista para as infraestruturas críticas espanholas em termos de probabilidade de ocorrência, tal como comprovado pela persistência de células ativas no território espanhol e pela difusão contínua de propaganda que promove ataques contra alvos de infraestruturas em toda a Europa. A ENCOT 2023 concorda com esta avaliação, destacando o aumento dos atores solitários que, após processos de auto-radicalização em ambientes digitais, executam ações com meios rudimentares, mas de elevada letalidade — padrão ilustrado pelos atentados de Las Ramblas e Cambrils —, o que representa um enorme desafio para os sistemas de deteção precoce. No entanto, o perigo representado pelos atores estatais hostis — especialmente a Rússia — e pelos ataques inspirados por extremistas de diversas orientações ideológicas deve ser abordado com esforços estratégicos comparáveis, tendo em conta o seu potencial para causar danos catastróficos às infraestruturas essenciais.

Em terceiro lugar, a digitalização e a convergência entre TI e OT transformaram o panorama das vulnerabilidades das infraestruturas críticas espanholas e criaram novos vetores de ataque que os sistemas de proteção existentes nem sempre conseguem neutralizar eficazmente. O reforço da cibersegurança industrial deve ser considerado uma prioridade nacional de primeira ordem, que só pode ser alcançada através de

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

investimentos sustentados em tecnologia, formação especializada e atualização dos quadros normativos e das normas técnicas.

Em quarto lugar, a coordenação público-privada, embora tenha evoluído consideravelmente desde a adoção da Lei n.º 8/2011, continua a ser uma área crítica a melhorar no sistema espanhol. Os ativos de infraestruturas críticas de propriedade privada requerem mecanismos mais sofisticados para alinhar incentivos e trocar informações classificadas entre o setor público e os operadores, que só podem ser desenvolvidos com base num quadro jurídico que garanta a confiança e a confidencialidade de todas as partes.

Em quinto lugar, a cooperação internacional, não só no âmbito da UE, mas também no seio da OTAN e de outros fóruns multilaterais, é um fator determinante para a eficácia do sistema de proteção das infraestruturas críticas espanholas. A localização da Espanha como porta de entrada entre a Europa e o Norte de África deveria traduzir-se num papel único na arquitetura de segurança europeia e, por conseguinte, num compromisso específico com os mecanismos de cooperação multilateral existentes e no desenvolvimento das suas próprias capacidades para proporcionar um valor diferencial a todo o sistema.

Deverão ser realizadas futuras investigações nesta área, centradas na análise setorial das vulnerabilidades que utilize metodologias de avaliação quantitativa de riscos, no estudo comparativo dos modelos de transposição da Diretiva CER adotados pelos principais Estados-Membros da União Europeia e na avaliação empírica da eficácia dos mecanismos de coordenação público-privada existentes, através de metodologias de investigação primária com operadores críticos.

10. REFERÊNCIAS BIBLIOGRÁFICAS

Arteaga, F. (2023). Infraestruturas críticas e segurança nacional em Espanha. *Real Instituto Elcano.* https://www.realinstitutoelcano.org

Boin, A. e 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. e Knake, R. (2010). *Guerra cibernética: a próxima ameaça à segurança nacional e o que fazer a esse respeito.* HarperCollins.

Departamento de Segurança Nacional. (2021). *Estratégia Nacional de Segurança.* Presidência do Governo de Espanha.

ENISA. (2024). *ENISA Threat Landscape 2024.* Agência da União Europeia para a Cibersegurança. https://www.enisa.europa.eu

Europol. (2023). *Relatório sobre a Situação e as Tendências do Terrorismo na União Europeia (TE-SAT) 2023.* Serviço das Publicações da União Europeia.

Europol. (2024). *Relatório sobre a Situação e as Tendências do Terrorismo na União Europeia (TE-SAT) 2024.* Serviço das Publicações da União Europeia. https://www.europol.europa.eu

Luiijf, E., Besseling, K. e De Graaf, P. (2013). Dezanove estratégias nacionais de cibersegurança. *International Journal of Critical Infrastructures, 9*(1-2), 3-31. https://doi.org/10.1504/IJCIS.2013.052819

Masse, T. (2020). *Terrorismo e Infraestruturas Críticas: Avaliação da Ameaça.* Serviço de Investigação do Congresso.

Ministério do Interior. (2023). *Estratégia Nacional contra o Terrorismo (ENCOT) 2023.* Secretaria de Estado da Segurança. https://www.dsn.gob.es/es/publicaciones/estrategias-sectoriales/ENCOT2023

Moteff, J. D. (2014). *Infraestruturas Críticas: Contexto, Política e Implementação.* Serviço de Investigação do Congresso.

Reinares, F. (2014). A Al-Qaeda e o 11-M em Espanha. *Revista de Occidente, 400*, 75-95.

Reinares, F. e García-Calvo, C. (2022). *Terrorismo jihadista em Espanha: Características e tendências.* Real Instituto Elcano. https://www.realinstitutoelcano.org

Rinaldi, S. M., Peerenboom, J. P. e Kelly, T. K. (2001). Identificar, compreender e analisar as interdependências das infraestruturas críticas. *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. REGULAMENTAÇÃO

Nações Unidas. Resolução 1373 (2001), de 28 de setembro. Conselho de Segurança das Nações Unidas. S/RES/1373 (2001).

Conselho da Europa. Convenção sobre a Prevenção do Terrorismo (CETS n.º 196). Varsóvia, 16 de maio de 2005. Em vigor desde 1 de junho de 2007.

União Europeia. Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação de infraestruturas críticas europeias. *Jornal Oficial da União Europeia*, L 345, de 23 de dezembro de 2008.

Espanha. Lei n.º 8/2011, de 28 de abril, que estabelece medidas para a proteção das infraestruturas críticas. *Boletim Oficial do Estado*, n.º 102, de 29 de abril de 2011.

Espanha. Decreto Real n.º 704/2011, de 20 de maio, que aprova o Regulamento de proteção das infraestruturas críticas. *Boletim Oficial do Estado*, n.º 121, de 21 de maio de 2011.

Espanha. Lei Orgânica n.º 4/2015, de 30 de março, relativa à Proteção da Segurança Cívica. *Boletim Oficial do Estado*, n.º 77, de 31 de março de 2015.

Nações Unidas. Resolução 2341 (2017), de 13 de fevereiro. Conselho de Segurança das Nações Unidas. S/RES/2341 (2017).

Espanha. Decreto Real n.º 1150/2021, de 28 de dezembro, que aprova a Estratégia Nacional de Segurança. *Boletim Oficial do Estado*, n.º 311, de 29 de dezembro de 2021.

Espanha. Decreto Real n.º 311/2022, de 3 de maio, que regulamenta o Esquema Nacional de Segurança. *Boletim Oficial do Estado*, n.º 105, de 4 de maio de 2022.

União Europeia. Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa às medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União (Diretiva NIS2). *Jornal Oficial da União Europeia*, L 333, de 27 de dezembro de 2022.

União Europeia. Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas (Diretiva CER). *Jornal Oficial da União Europeia*, L 333, de 27 de dezembro de 2022.