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

Article de recherche

LES INFRASTRUCTURES CRITIQUES ESPAGNOLES DANS LE COLLIMATEUR DES TERRORISTES. ANALYSE DES VULNÉRABILITÉS, CADRE RÉGLEMENTAIRE ET STRATÉGIES DE PROTECTION

Traduction en français à l'aide de l'IA (DeepL)

Raúl Moreno Ruiz
Capitaine de la Guardia Civil
Spécialiste de la sécurité pénitentiaire (ministère de l'Intérieur)
Master en gestion opérationnelle de la sécurité - Licence en droit
raul.moreno@dgip.mir.es

Reçu le 23/03/2026
Accepté le 04/06/2026
Publié le 30/06/2026

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

Citation recommandée : Moreno, R. (2026). Les infrastructures critiques espagnoles dans le collimateur des terroristes. Analyse des vulnérabilités, cadre réglementaire et stratégies de protection. Revue Logos Guardia Civil, 4(2), pp. 281–302. https://doi.org/10.64217/logosguardiacivil.v4i2.8979

Dépôt légal : M-3619-2023
NIPO en ligne : 126-23-019-8
ISSN en ligne : 2952-394X

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

LES INFRASTRUCTURES CRITIQUES ESPAGNOLES DANS LE COLLIMATEUR DES TERRORISTES. ANALYSE DES VULNÉRABILITÉS, CADRE RÉGLEMENTAIRE ET STRATÉGIES DE PROTECTION

Résumé : La vulnérabilité des infrastructures critiques espagnoles face à la menace terroriste d'un point de vue juridique, institutionnel et opérationnel. Cette étude examine le cadre réglementaire existant — à travers la loi n° 8/2011 et la directive (UE) 2022/2557 relative à la résilience des entités critiques (CER) —, se concentre sur les secteurs clés les plus vulnérables au risque et évalue l'architecture institutionnelle du système de protection espagnol. Grâce à une méthodologie d'analyse documentaire et à l'examen de la littérature spécialisée, il apparaît que, malgré un système solide de protection des infrastructures critiques (PIC) en Espagne, il existe des lacunes importantes en matière de cybersécurité industrielle, de coordination interadministrative et de transposition des directives européennes, qui nécessitent une attention urgente. Les principales menaces à l'horizon 2025-2030 sont identifiées comme étant le terrorisme djihadiste, les acteurs étatiques hostiles et le cyberterrorisme.

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.

Mots-clés : infrastructures critiques ; terrorisme ; sécurité nationale ; cyberterrorisme ; menace hybride.

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

ABRÉVIATIONS

CCN-CERT : Centre cryptologique national – Équipe d'intervention en cas d'urgence informatique

CITCO : Centre de renseignement contre le terrorisme et le crime organisé

CNI : Centre national de renseignement

CNPIC : Centre national de protection des infrastructures critiques

DSN : Département de la sécurité nationale

ENISA : Agence de l'Union européenne pour la cybersécurité

ICS : Industrial Control Systems (systèmes de contrôle industriels)

ICE : Infrastructure critique européenne

ICN : Infrastructure critique nationale

IoT : Internet des objets

NAA : Niveau d'alerte antiterroriste

NIS : Sécurité des réseaux et de l'information

PES : Plan stratégique sectoriel

PIC : Protection des infrastructures critiques

PNPIC : Plan national de protection des infrastructures critiques

PSO : Plan de sécurité de l'opérateur

SCADA : Contrôle de supervision et acquisition de données

TE-SAT : Rapport de l'UE sur la situation et les tendances en matière de terrorisme

ENCOT : Stratégie nationale contre le terrorisme

1. INTRODUCTION

Le terrorisme a connu une transformation radicale au fil des ans, tant dans sa nature que dans les objectifs qu'il choisit de poursuivre. Au XXe siècle, les attentats terroristes visaient principalement un petit pourcentage de personnes : des dirigeants politiques, des militaires ou des civils dans des lieux publics. Aujourd'hui, cependant, la tendance actuelle est à une augmentation du nombre d'attaques contre les infrastructures et les systèmes vitaux qui permettent le développement et la vie d'un État moderne. Cette évolution stratégique n'est pas le fruit du hasard ; elle répond à une logique de maximisation de l'impact que les groupes terroristes et militants n'ont cessé de perfectionner au fil du temps : perturber les fondements matériels de la société génère un impact déstabilisateur et psychologique bien plus important que celui des attaques conventionnelles, à forte visibilité mais à faible impact structurel. Cela n'est pas une surprise pour l'Espagne.

Le 11 mars 2004, lorsque plusieurs trains de banlieue circulant sur le réseau de la Renfe à Madrid ont été détruits, faisant 193 morts et plus de 2 000 blessés, cet événement a constitué l'attaque terroriste la plus dévastatrice jamais perpétrée contre les infrastructures de transport espagnoles. À l'époque, le système de protection des infrastructures critiques en était à ses balbutiements, mais cet événement a catalysé un processus législatif et organisationnel qui a abouti à l'adoption de la loi n° 8/2011 du 28 avril, premier texte réglementaire complet à l'échelle nationale. À ce jour, l'expérience acquise a permis de mettre en place un système de protection qui est désormais confronté à des défis qualitatifs découlant précisément des enjeux qui avaient motivé sa création.

Au cours de la première moitié des années 2020, le contexte des menaces en Europe avait considérablement évolué. L'agression russe en cours contre l'Ukraine depuis février 2022 a mis en évidence la vulnérabilité des infrastructures énergétiques européennes face à des acteurs étatiques hostiles, comme l'a démontré le sabotage des gazoducs Nord Stream en septembre 2022. Par ailleurs, le terrorisme djihadiste, notamment lié à Daech et à Al-Qaïda, reste une menace persistante sur le continent européen, avec des cellules résiduelles actives et une capacité inquiétante de radicalisation en ligne qui alimente le phénomène dit du « loup solitaire ». De plus, l'extrémisme de droite connaît une résurgence inquiétante dans de nombreux pays de l'Union européenne, ce qui élargit le champ d'application des formes conventionnelles de menace terroriste, au-delà du simple appel au djihadisme.

Cet article vise à explorer, dans une perspective multidisciplinaire et académique, la menace que représentent les éléments terroristes pour les infrastructures critiques espagnoles. À cette fin, nous examinerons tant le cadre réglementaire de référence national en Espagne que les cadres européens et internationaux ; nous présenterons les secteurs stratégiques les plus vulnérables ; nous analyserons le cadre institutionnel de référence du système de protection des infrastructures critiques (CIP) espagnol ; et nous proposerons des mécanismes d'amélioration visant à renforcer la résilience du système pour la période 2025-2030.

La présente étude adopte une perspective intégratrice qui associe l'analyse juridique au prisme des sciences de la sécurité et de la criminologie, partant du principe que les complexités du phénomène exigent une approche pluridisciplinaire et complémentaire. L'hypothèse directrice qui guide la recherche s'exprime comme suit : l'Espagne dispose

d'un système réglementaire solide et d'un cadre institutionnel couvrant les infrastructures critiques conformément aux normes européennes, mais présente également des vulnérabilités structurelles, notamment en matière de cybersécurité industrielle et de partenariat public-privé, que les acteurs terroristes pourraient exploiter dans un contexte de menaces croissantes et diversifiées.

Conformément à cette hypothèse, le document montrera que la réponse à cette menace nécessite une nouvelle approche, impliquant non seulement de réformer le cadre réglementaire actuel des infrastructures critiques, mais aussi de repenser les modèles de gouvernance et le partenariat entre le secteur public et les opérateurs privés d'infrastructures critiques. Cette méthodologie particulière découle de l'analyse documentaire de sources primaires — législation, rapports officiels, documents stratégiques — et de sources secondaires — littérature académique spécialisée, rapports d'organisations internationales — sur une période de référence allant de l'adoption de la loi n° 8/2011 à 2025.

2. MÉTHODOLOGIE

La recherche adopte une approche qualitative fondée sur l'analyse documentaire systématique, une approche appropriée pour l'étude de phénomènes juridico-institutionnels dans lesquels la compréhension du cadre normatif et conceptuel est préalable et nécessaire à toute évaluation empirique. La lacune que ce travail vise à combler réside dans l'absence d'études intégrant de manière cohérente les trois dimensions — juridique, institutionnelle et opérationnelle — du système espagnol de PIC face à la menace terroriste, en tenant compte des dernières évolutions réglementaires européennes (directive CER et NIS2, toutes deux de 2022) et de la nouvelle stratégie nationale contre le terrorisme de 2023.

Les sources primaires comprennent : la législation nationale (loi n° 8/2011, décret royal n° 704/2011, loi organique n° 4/2015, décret royal n° 311/2022 et décret royal n° 1150/2021) ; la réglementation européenne (directive CER 2022/2557, directive NIS2 2022/2555 et directive 2008/114/CE) ; les instruments internationaux (résolutions du Conseil de sécurité de l'ONU 1373/2001 et 2341/2017 ; CETS n° 196) ; et documents stratégiques officiels (Stratégie de sécurité nationale 2021, ENCOT 2023, rapports annuels du CNPIC). Les sources secondaires comprennent la littérature académique spécialisée dans la sécurité nationale, la protection des infrastructures critiques et le terrorisme, obtenue grâce à une recherche systématique dans les bases de données Scopus, Web of Science et Google Scholar, à l'aide des mots-clés suivants : « critical infrastructure protection », « terrorism », « hybrid threats », « CIP Spain », « infraestructuras críticas », « terrorismo » et « resiliencia » ; ainsi que des rapports d'organismes internationaux (Europol TE-SAT, ENISA Threat Landscape). Les critères d'inclusion suivants ont été appliqués : publications en espagnol ou en anglais, période 2001-2025, et pertinence directe par rapport à l'objet de l'étude. Ont été exclus les travaux à caractère exclusivement descriptif sans apport analytique ou constructif, ainsi que les sources non vérifiables ou à diffusion restreinte.

3. CADRE CONCEPTUEL : QU'EST-CE QU'UNE INFRASTRUCTURE CRITIQUE ?

La notion d'« infrastructure critique » n'est pas univoque, que ce soit dans le milieu universitaire ou dans la réglementation. À mesure que les sociétés modernes sont devenues de plus en plus dépendantes de certains systèmes ou services critiques, sa définition a évolué. Aux fins du présent travail, dans le cadre et selon les paramètres de la loi n° 8/2011, on entend par « infrastructure critique » les installations, réseaux, services et équipements des technologies de l'information et de la communication dont l'interruption ou la destruction aurait un impact significatif sur la santé, la sécurité ou le bien-être économique des citoyens, ou sur le fonctionnement efficace des institutions de l'État et des administrations publiques. Cette définition reflète une vision de l'impact potentiel qui se concentre non pas tant sur la nature de l'infrastructure, mais plutôt sur les conséquences de sa défaillance ou de sa destruction pour la société dans son ensemble.

3.1. CLASSIFICATION SECTORIELLE

L'article 2 du décret royal 704/2011 identifie douze secteurs stratégiques soumis à une protection dans le cadre du système PIC espagnol : l'administration, l'eau, l'alimentation, l'énergie, l'espace, l'industrie nucléaire, l'industrie chimique, les installations de recherche, la santé, le système financier et fiscal, les technologies de l'information et de la communication (TIC) et les transports. Cette classification est conforme à la description donnée dans la directive (UE) 2022/2557 (directive CER), qui élargit l'ensemble des secteurs à onze et définit explicitement les infrastructures numériques, l'espace et l'administration publique comme des catégories spécifiques.

La pondération relative des secteurs en termes de sécurité varie selon les types de menaces et les conséquences possibles d'une perturbation, mais, en substance, les secteurs de l'énergie, des transports et des TIC sont, dans le contexte espagnol, relativement concentrés en ce qui concerne leurs actifs clés. D'après les données fournies par le CNPIC, l'Espagne compte plus de 3 700 opérateurs critiques désignés, répartis entre les douze secteurs stratégiques, les secteurs des TIC et de l'énergie concentrant le plus grand nombre d'opérateurs en termes absolus.

3.2. INFRASTRUCTURES CRITIQUES NATIONALES ET INFRASTRUCTURES CRITIQUES EUROPÉENNES

La distinction entre les infrastructures critiques nationales (ICN) et les infrastructures critiques européennes (ICE) revêt une importance particulière au regard de la législation de l'UE. Une infrastructure est qualifiée d'ICE si sa perturbation ou sa destruction affecterait gravement deux États membres ou plus, ou l'UE dans son ensemble. La directive 2008/114/CE a été la première à établir ce concept ; elle en limitait initialement le champ d'application aux secteurs de l'énergie et des transports. La directive CER de 2022 élargit la portée de ce concept et renforce les moyens permettant d'identifier et de protéger ces infrastructures. L'Espagne a désigné plusieurs de ces installations comme ICE, principalement dans les secteurs de l'énergie et des transports, compte tenu du rôle stratégique du pays en tant que corridor énergétique et de communication entre l'Europe et l'Afrique du Nord, une position géopolitique qui, si elle confère à l'Espagne un rôle central dans l'architecture de sécurité européenne, accroît son exposition à certaines menaces transnationales.

3.3. LE CONCEPT D'INTERDÉPENDANCE

Un thème central de l'analyse des infrastructures critiques est la question de l'interdépendance. Les systèmes critiques d'aujourd'hui ne fonctionnent pas de manière isolée ; ils dépendent fortement d'autres systèmes dont ils ont besoin pour fonctionner. Le secteur de l'électricité dépend des infrastructures de télécommunications pour sa gestion automatisée ; le transport ferroviaire est alimenté en énergie électrique ; et le secteur financier dépend des TIC pour pratiquement toutes ses opérations. Cette interdépendance engendre ce que la littérature spécialisée appelle des « effets en cascade » : la défaillance d'une infrastructure peut entraîner la défaillance successive d'autres infrastructures, avec des conséquences potentiellement dévastatrices pour l'ensemble du système (Rinaldi et al., 2001).

L'approfondissement de la numérisation des systèmes critiques — lié aux technologies de l'Internet des objets (IoT), aux plateformes de données dans le cloud et aux systèmes de contrôle industriel SCADA — a amplifié ces interdépendances, donnant lieu à de nouveaux vecteurs de vulnérabilité que des groupes terroristes plus sophistiqués commencent à exploiter systématiquement. Cette interdépendance n'est pas uniquement d'ordre technique ou cybernétique ; elle implique des aspects géographiques — infrastructures transfrontalières telles que les réseaux électriques ou les gazoducs —, cybernétiques — systèmes de contrôle partagés ou interconnectés — et organisationnels — opérateurs gérant des actifs dans de nombreux secteurs.

La nature multiforme de cette interdépendance fait de l'analyse des risques liés aux infrastructures critiques un processus d'une immense complexité qui ne peut se réduire à l'examen de chaque infrastructure de manière indépendante.

4. CADRE RÉGLEMENTAIRE DE RÉFÉRENCE

La protection des infrastructures critiques contre les menaces terroristes et autres menaces intentionnelles s'articule autour d'un cadre réglementaire complexe à plusieurs niveaux, qui comprend des dispositions nationales, européennes et internationales. Cette architecture réglementaire reflète également la prise de conscience croissante que la menace pesant sur les infrastructures critiques transcende les frontières nationales et nécessite des réponses coordonnées à différents niveaux de gouvernance. Chacun de ces niveaux est abordé dans les sections suivantes, en mettant l'accent sur les dernières évolutions réglementaires et les défis posés par leur mise en œuvre.

4.1. RÉGLEMENTATION ESPAGNOLE

La loi n° 8/2011 du 28 avril constitue le fondement de la législation nationale espagnole en matière de protection des infrastructures critiques. Cette loi transpose la directive 2008/114/CE en droit espagnol et établit le Système de protection des infrastructures critiques, un dispositif qui repose sur trois principes fondamentaux : le Centre national de protection des infrastructures critiques (CNPIC), le Catalogue national des infrastructures stratégiques et la planification de la protection. Elle distingue, dans le cadre juridique espagnol, le Plan national de protection des infrastructures critiques (PNPIC), les Plans stratégiques sectoriels (PES) et les Plans de sécurité de l'exploitant (PSO), et prévoit un plan « par paliers et de haut niveau » qui s'articule du niveau général au niveau spécifique. La mise en œuvre réglementaire de la loi PIC est assurée par le décret royal n° 704/2011

du 20 mai, qui en précise l'application en matière de protection des infrastructures critiques.

Cette réglementation définit les critères de désignation des opérateurs critiques, le contenu minimal des plans de sécurité des opérateurs et des plans de protection spécifiques, ainsi que les responsabilités en matière de communication des incidents. L'article 24 revêt une importance particulière, car il établit le régime d'inspection et de supervision des opérateurs critiques, ce qui permet au CNPIC de vérifier le respect des obligations de sécurité. Plusieurs auteurs ont souligné que cette supervision de la conformité a, dans la pratique, été identifiée comme une faiblesse e du système, compte tenu du grand nombre d'opérateurs et des ressources limitées dont dispose l'administration opérationnelle. La Stratégie de sécurité nationale de 2021, telle qu'autorisée par le décret royal 1150/2021, identifie le terrorisme comme l'un des principaux risques et menaces pour l'Espagne, et considère la protection des infrastructures critiques comme un axe d'objectifs ambitieux du système de sécurité nationale, s'inscrivant dans l'approche holistique de la sécurité qui caractérise le système espagnol.

Dans cette optique, la Stratégie nationale contre le terrorisme (ENCOT) de 2023 — qui actualise et remplace la version de 2019 — structure la réponse antiterroriste de l'État autour de quatre piliers d'action (prévenir, protéger, poursuivre et réagir) et place la protection des infrastructures critiques au cœur du pilier « protéger ». L'ENCOT 2023 introduit une innovation conceptuelle majeure en admettant institutionnellement que l'invulnérabilité absolue est inatteignable, déplaçant ainsi l'axe stratégique de la simple protection statique vers la résilience globale, comprise comme la capacité à absorber l'impact d'un incident, à garantir la continuité des services essentiels et à rétablir rapidement la situation normale. Cette vision s'aligne pleinement sur l'approche de la directive CER de 2022, ce qui fait de l'ENCOT 2023 un pont doctrinal entre la stratégie antiterroriste nationale et le cadre européen des entités critiques. En outre, l'ENCOT 2023 met en garde contre le déplacement de la menace vers ce que l'on appelle les « cibles molles » — lieux de culte, manifestations rassemblant de grandes foules et espaces publics — qui, sans constituer des infrastructures critiques au sens technique du terme, s'avèrent déterminantes pour la sécurité des citoyens ; une réalité qui interpelle directement le champ d'application de la future législation de transposition. En matière de cybersécurité, le Schéma national de sécurité, approuvé par le décret royal 311/2022, prescrit des exigences minimales pour les systèmes d'information des administrations publiques et de leurs opérateurs de services essentiels, complétant ainsi le régime PIC en ce qui concerne les actifs d'information des opérateurs critiques.

La loi organique n° 4/2015 du 30 mars relative à la protection de la sécurité des citoyens introduit des mesures importantes de contrôle d'accès aux installations sensibles et de surveillance des environnements à risque, complétant ainsi le système de protection physique prévu par la réglementation PIC.

4.2. RÉGLEMENTATION EUROPÉENNE

Le cadre réglementaire de l'Union européenne a fait l'objet d'une révision en profondeur suite à l'adoption de la directive (UE) 2022/2557 (14 décembre 2022) relative à la résilience des entités critiques (directive CER). Cette réglementation remplace la directive 2008/114/CE et crée un cadre repensé qui met davantage l'accent sur la

résilience globale des entités exploitant des infrastructures, plutôt que sur la seule mise à disposition physique et la protection des systèmes, définie comme leur capacité à prévenir les incidents, à en supporter l'impact, à en gérer les conséquences et à se rétablir rapidement. Parmi les principales évolutions de la directive CER figurent l'élargissement du champ d'application sectoriel, qui passe de deux à onze secteurs, la nécessité de renforcer les exigences en matière d'analyse des risques et de signalement des incidents, ainsi que la mise en place d'un mécanisme européen destiné à aider les États membres à identifier les entités critiques, c'est-à-dire celles qui revêtent une importance particulière au niveau européen.

La date limite pour la transposition de la directive CER était fixée au 17 octobre 2024. L'Espagne n'avait pas achevé cette procédure à cette date, ce qui la plaçait dans une situation de non-conformité susceptible d'entraîner une procédure d'infraction de la part de la Commission européenne si elle se prolongeait. Ce retard résulte de la complexité technique et politique qu'implique une transposition nécessitant de modifier ou d'abroger la loi n° 8/2011 et son règlement d'application, ainsi qu'une révision du Catalogue national des infrastructures stratégiques afin de l'adapter aux nouveaux secteurs couverts et de réformer les mécanismes de coopération interministérielle et intersectorielle.

La directive NIS2 (directive (UE) 2022/2555), qui a été adoptée le même jour que la directive CER, révise et abroge la directive NIS de 2016 et établit des mesures visant à maintenir un niveau commun élevé de cybersécurité dans toute l'UE. Elle élargit considérablement le champ d'application de la réglementation en matière de cybersécurité, passant des « opérateurs de services essentiels » aux « entités essentielles et importantes », et implique des responsabilités renforcées fondées sur la gestion des risques, le signalement des incidents et la coopération transfrontalière.

L'interaction entre la directive CER et la directive NIS2 est l'un des aspects les plus complexes de ce nouveau cadre européen : ces deux directives s'appliquent à bon nombre des mêmes entités, mais sous des angles différents, à savoir (1) la résilience physique globale et (2) la cybersécurité, ce qui nécessite une coordination lors de leur transposition afin d'éviter les chevauchements et les contradictions.

4.3. CADRE INTERNATIONAL

Sur la scène internationale, la résolution 1373 (2001) du Conseil de sécurité des Nations unies définit les obligations de tous les États dans la lutte contre le terrorisme, notamment l'obligation de mettre en œuvre des mesures visant à empêcher l'utilisation de leur territoire à des fins terroristes et de partager des informations avec d'autres États.

La résolution 2341 (2017) du Conseil de sécurité est le premier instrument de cet organisme spécifiquement consacré à la protection des infrastructures critiques contre le terrorisme ; elle exhorte les États à mettre en place des mesures de protection proportionnées au risque identifié, tout en encourageant la coopération internationale concernant la dimension cybernétique de la menace. La Convention pour la prévention du terrorisme (CETS n° 196), en vigueur depuis 2007, et son Protocole additionnel de 2015 créent des obligations en matière de criminalisation et de coopération judiciaire qui complètent le cadre de l'ONU.

5. LE TERRORISME EN TANT QUE MENACE SPÉCIFIQUE CONTRE LES INFRASTRUCTURES CRITIQUES

5.1. TYPOLOGIE DES GROUPES TERRORISTES S'INTÉRESSANT AUX INFRASTRUCTURES CRITIQUES

Le phénomène terroriste apparaît donc comme l'une des menaces les plus complexes et les plus multiformes qui pèsent sur les infrastructures essentielles de la société contemporaine. Contrairement à d'autres menaces telles que les catastrophes naturelles ou les défaillances technologiques accidentelles, le terrorisme se caractérise par une intention malveillante et une rationalité stratégique, ce qui signifie que les terroristes adaptent et renouvellent leurs tactiques, techniques et procédures en fonction des mesures de protection mises en place. Une réponse de protection efficace exige donc une réaction tout aussi dynamique et proactive face à la nature adaptative et e de la menace, qui ne peut se limiter à des mesures de sécurité physiques et logiques de nature statique.

5.1.1. Terrorisme djihadiste

Le terrorisme d'inspiration djihadiste, particulièrement associé à des groupes tels que Daech et Al-Qaïda, a exprimé à plusieurs reprises son intérêt stratégique pour des attaques contre des infrastructures clés dans les pays occidentaux. Dans des brochures publiées notamment dans Dabiq ou Inspire, ces deux groupes ont fourni des consignes explicites visant à attaquer des centrales électriques, des sources d'eau potable et des infrastructures de transport en Europe et en Amérique du Nord, en accordant une attention particulière aux effets en chaîne qu'entraînerait la perturbation d'infrastructures interconnectées.

En Espagne, plus précisément, l'attaque (en août 2017) perpétrée par une cellule de Daech sur la Rambla à Barcelone et à Cambrils a montré que la menace djihadiste restait présente au niveau national, même si, cette fois-ci, son objectif était de faire des victimes dans l'espace public plutôt que de s'en prendre à une infrastructure spécifique. Selon le rapport TE-SAT 2024 d'Europol, le terrorisme djihadiste reste la menace la plus grave pour l'Union européenne en termes de nombre d'opérations, d'arrestations et d'attaques perpétrées ou déjouées.

Dans ce contexte, l'Espagne se trouve dans une position particulièrement vulnérable : son statut de pays de transit entre l'Afrique du Nord et l'Europe, les flux migratoires qui traversent ses frontières méridionales et la présence de communautés présentant des degrés avérés de radicalisation. Le modèle du « loup solitaire », qui agit de manière autonome après s'être radicalisé par le biais des réseaux numériques, pose des défis uniques en matière de détection précoce et constitue actuellement le profil le plus probable des attentats terroristes d'inspiration djihadiste sur le sol espagnol.

5.1.2. Acteurs étatiques hostiles et menaces hybrides

Cette catégorie d'acteurs étatiques hostiles mérite une attention particulière dans le contexte des menaces pesant sur les infrastructures critiques. Les éléments de preuve recueillis depuis 2014 suggèrent que la Russie a développé et déployé des capacités avancées pour saboter les infrastructures critiques en Europe, par des moyens cybernétiques directs (notamment les attaques menées par le groupe Sandworm contre le

réseau électrique ukrainien en 2015 et 2016) et par le biais d'activités clandestines de sabotage physique.

Le cas le plus spectaculaire est celui du sabotage des gazoducs Nord Stream en septembre 2022, qui a interrompu l'approvisionnement en gaz naturel de l'Europe en provenance de Russie et démontre la volonté des acteurs étatiques de s'attaquer aux infrastructures européennes dans le but de s'en servir comme levier géopolitique.

Le concept de « menace hybride » désigne la combinaison d'une série d'outils traditionnels et inhabituels, notamment la désinformation, les cyberattaques, le sabotage physique et la pression économique, afin de créer une « stratégie de menace hybride » intégrée conçue pour affaiblir un État sans pour autant entrer dans la catégorie de la confrontation armée conventionnelle. Ce type de menace, dans lequel la Russie s'est imposée ces dernières années comme l'acteur le plus actif en Europe, pose un défi particulier aux systèmes dont l'objectif principal est de protéger les infrastructures critiques, alors que la menace sous-jacente y est traitée comme une succession de menaces traditionnelles individuelles. L'Iran et la Corée du Nord, qui sont également considérés par les experts comme des cyberattaquants ciblant les infrastructures critiques, ont démontré qu'ils disposaient de capacités de cyberattaque contre ces infrastructures, bien que le danger réel qu'ils représentent pour le territoire espagnol soit désormais jugé moins important que la menace russe.

5.1.3. Terrorisme d'extrême droite

Bien que le terrorisme d'extrême droite ne vise généralement pas les infrastructures comme le fait le terrorisme djihadiste, il a été associé à plusieurs incidents graves en Europe ces dernières années. Les attentats d'Utøya (Norvège, 2011), de Hanau (Allemagne, 2020) et de Christchurch (Nouvelle-Zélande, 2019) ont mis en évidence la capacité meurtrière de ce type d'acteurs.

Dans le domaine des infrastructures critiques, certaines cellules d'extrême droite ont manifesté leur intérêt pour des attaques contre les infrastructures de communication, d'énergie ou de transport, dans le but de déstabiliser la société et de provoquer l'effondrement de l'ordre établi, ce que ces groupes appellent « l'accélération ». Ce phénomène est reconnu comme une menace émergente par la Stratégie de l'UE pour l'Union de la sécurité 2020-2025, qui soutient que, tant dans le domaine du renseignement que dans celui des outils réglementaires, il doit être traité et abordé avec le même sérieux que le terrorisme djihadiste.

5.2. CAS HISTORIQUES SIGNIFICATIFS

L'attentat du 11 mars 2004 à Madrid reste sans aucun doute le cas de référence en Espagne. Aux heures de pointe du matin, la détonation coordonnée de dix engins explosifs dans des trains de banlieue a constitué une exploitation des vulnérabilités inhérentes aux systèmes de transport en commun : ceux-ci sont ouverts, les usagers y sont concentrés et il est difficile de mettre en place une infrastructure de sécurité complète sans sacrifier l'efficacité du service. L'attentat a fait 193 morts et plus de 2 000 blessés, et a eu un impact économique et social considérable (Reinares, 2014). Non seulement il a eu un effet immédiat, mais le 11 mars a également révélé que l'infrastructure ferroviaire présentait des vulnérabilités structurelles qui n'avaient pas été suffisamment prises en

compte dans les plans de sécurité de l'époque. Au niveau européen, l'attentat de 2016 à Bruxelles, qui a impliqué l'explosion d'engins à l'aéroport international de Zaventem et dans le métro de la ville, démontre comment les terroristes sont capables de frapper deux nœuds ou plus des infrastructures de transport en une seule fois, leur conférant ainsi un impact psychologique et médiatique maximal.

Un aéroport international est considéré comme une cible délibérée : ce type d'aéroport concentre de grands volumes de personnes de différentes nationalités en un seul et même lieu, qui bénéficie d'une forte couverture médiatique internationale, à tel point que sa perturbation entraîne des répercussions économiques et d'image disproportionnées par rapport au coût matériel de l'attaque. Dans le contexte espagnol, une série d'actes de sabotage visant des infrastructures de fibre optique signalés dans plusieurs communautés autonomes en 2024 a mis en évidence la vulnérabilité des réseaux de télécommunications face à des actes de destruction intentionnels ; cela démontre que la mise hors service d'infrastructures vitales peut être réalisée à l'aide de techniques relativement simples lorsque les actifs ne bénéficient pas d'une protection physique adéquate.

5.3. LE CYBERTERRORISME ET LES ATTAQUES HYBRIDES : UNE NOUVELLE FRONTIÈRE

Le cyberterrorisme, défini comme l'utilisation intentionnelle de capacités informatiques (à des fins d'intimidation ou de pression politique) pour causer des ravages dans les infrastructures critiques, constitue l'aspect le plus récent, et peut-être le plus perturbateur, des attaques terroristes visant des infrastructures de grande valeur. Et contrairement au terrorisme traditionnel, les cyberattaques peuvent être menées à distance, dans certains cas sans pouvoir être identifiées, et depuis différents endroits, ce qui rend l'attribution et le contrôle beaucoup plus complexes pour les autorités.

L'interconnexion et la fusion du cyberespace et des systèmes de contrôle industriels ont donné naissance à ce que certains appellent le « cinquième domaine de la guerre » (Clarke et Knake, 2010), où les terroristes sont capables d'infliger des dommages physiques réels à des infrastructures critiques sans avoir à s'en approcher. L'attaque menée par les États-Unis contre le Colonial Pipeline (mai 2021) à l'aide d'un rançongiciel a mis en évidence à quel point les infrastructures énergétiques critiques sont vulnérables face à de telles cyberattaques et à quelle vitesse celles-ci peuvent entraîner des pénuries d'approvisionnement et susciter l'inquiétude de la population.

En Europe, les cyberattaques menées en 2015 et 2016 contre la compagnie d'électricité ukrainienne Ukrenergo par des individus liés à l'État russe ont privé de courant de vastes régions d'Ukraine pendant plusieurs heures, laissant présager que des attaques contre les infrastructures énergétiques en Europe pourraient survenir dans un contexte de conflit géopolitique croissant.

Selon l'enquête « ENISA Threat Landscape 2024 », la cybermenace pesant sur les infrastructures industrielles dans les secteurs essentiels a augmenté de 78 % en Europe entre 2022 et 2023, ce qui témoigne de la tendance à la hausse de ce type d'attaques.

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

6. VULNÉRABILITÉS DES INFRASTRUCTURES CRITIQUES ESPAGNOLES

Afin d'analyser les vulnérabilités du système d'infrastructures critiques espagnoles face à la menace terroriste, l'approche doit être à la fois sectorielle — en tenant compte des caractéristiques spécifiques de chaque secteur stratégique — et transversale, afin d'identifier les faiblesses structurelles communes à l'ensemble du système. Les sections suivantes abordent tout d'abord les vulnérabilités spécifiques des secteurs les plus exposés, puis examinent les facteurs transversaux de vulnérabilité.

6.1. ANALYSE SECTORIELLE DES VULNÉRABILITÉS

6.1.1. Secteur énergétique

Le secteur énergétique représente l'une des cibles prioritaires des groupes terroristes sophistiqués en raison de l'ampleur de l'impact potentiel d'une attaque réussie. L'Espagne exploite un réseau électrique à haute tension, qui relie le réseau péninsulaire aux îles Canaries et aux Baléares, ainsi qu'à la France et au Portugal via les interconnexions pyrénéennes, et qui est géré par Red Eléctrica de España (REE). La concentration d'actifs cruciaux dans certains nœuds du réseau — centrales de production, centres de dispatching ou transformateurs haute tension — et le fait que leur remplacement après des dommages graves, qui prend des mois, crée des vulnérabilités particulières face à des attaques physiques ou cybernétiques coordonnées. De plus, les centrales nucléaires existantes et en service en Espagne — Almaraz, Ascó, Cofrentes, entre autres — nécessitent une protection à différents niveaux en raison des effets potentiellement catastrophiques d'incidents sur ces sites, mais leur sécurité physique et radiologique est surveillée en permanence par le Conseil de sécurité nucléaire (CSN).

6.1.2. Secteur des transports

L'Espagne dispose de l'un des réseaux ferroviaires à grande vitesse les plus étendus au monde, avec plus de 3 900 kilomètres de lignes à grande vitesse en service. Cette infrastructure, caractérisée par une concentration de voyageurs dans les grandes gares — Atocha, Sants, Santa Justa — ainsi que par certains éléments qui la rendent vulnérable, tels que les tunnels, les viaducs et les systèmes de signalisation, constitue une cible de choix pour les terroristes. L'aéroport Adolfo Suárez Madrid-Barajas, quatrième aéroport le plus fréquenté d'Europe avec plus de 62 millions de passagers par an, et le port d'Algeciras, principal port à conteneurs d'Espagne et porte d'entrée pour les marchandises en provenance d'Afrique du Nord, présentent des caractéristiques à haut risque qui exigent des mesures de sécurité particulièrement rigoureuses.

6.1.3. Secteur des TIC

L'infrastructure numérique espagnole s'est rapidement développée ces dernières années en raison de la numérisation de l'économie, ainsi que de la 5G et du déploiement d'infrastructures de cloud computing. Les câbles de communication sous-marins qui relient l'Espagne au reste du monde — y compris ceux qui relient la péninsule ibérique aux îles Canaries et au continent américain — sont également devenus un vecteur de vulnérabilité de premier ordre, comme en témoignent les incidents survenus en mer Rouge et en mer Baltique entre 2023 et 2025. Ces câbles concentrent la majeure partie du trafic international de données et de voix, et leur endommagement intentionnel pourrait

entraîner une perte de capacité de communication à l'échelle continentale. Compte tenu de la dispersion géographique des actifs TIC et de l'évolution rapide tant des technologies que des vecteurs d'attaque, le CNPIC a souligné que le secteur des TIC pose certains des défis les plus urgents en matière de protection.

6.2. RISQUES LIÉS À LA NUMÉRISATION ET À LA CONNECTIVITÉ

L'adoption des technologies de l'information (TI) et des technologies opérationnelles (OT) dans les contextes industriels est l'une des tendances les plus importantes — et les plus préoccupantes du point de vue de la sécurité — de ces dix dernières années. Ce que l'on appelle la « brèche aérienne » entre les systèmes de contrôle industriel (ICS/SCADA) et les réseaux d'entreprise ainsi qu'Internet a entraîné une intégration progressive des systèmes informatiques au sein des environnements numériques afin d'améliorer l'efficacité opérationnelle et la gestion des réparations à distance.

Cette connectivité crée de nouvelles surfaces d'attaque susceptibles d'être exploitées par des groupes terroristes dotés de capacités cybernétiques avancées. Le nombre d'appareils IoT installés comme éléments clés de systèmes critiques — tels que les capteurs de température, les caméras de sécurité et les systèmes de contrôle d'accès — exacerbe la menace en intégrant des composants qui ne sont pas intrinsèquement sécurisés lorsqu'ils sont intégrés à des systèmes opérationnels critiques pour la sécurité. L'absence de mises à jour de sécurité d' s appareils intégrés, l'existence de protocoles de communication industriels obsolètes dépourvus de capacités cryptographiques et le manque d'experts professionnels en cybersécurité au sein du secteur industriel aggravent considérablement ce niveau de vulnérabilité.

6.3. COORDINATION PUBLIC-PRIVÉ : LE DÉFI À RELEVER

Une caractéristique systémique du système d'infrastructures critiques espagnol, qui a engendré des vulnérabilités spécifiques, réside dans le fait que la plupart des opérateurs critiques sont des entités privées. Sur les quelque 3 700 opérateurs désignés en Espagne, la majorité sont des entités privées ou mixtes, ce qui représente un défi permanent face à des intérêts privés qui privilégient les profits et l'efficacité au détriment de la sécurité nationale.

À cet égard, et dans le cadre de ces obligations, combinées aux dispositions de la loi PIC, les opérateurs critiques doivent élaborer des plans de sécurité de l'opérateur et des plans de protection spécifiques à leur activité ; toutefois, les investissements consacrés à ces dispositifs dépassent souvent les exigences minimales de conformité à la loi PIC, du moins lorsqu'il existe très peu de raisons économiques justifiant un tel engagement financier. L'échange d'informations et la confiance mutuelle entre les secteurs public et privé sont mis en avant par la littérature spécialisée comme des éléments essentiels à l'efficacité du système PIC (Moteff, 2014).

À cet égard, l'Espagne a mis en place des mécanismes d'échange d'informations et des systèmes d'alerte précoce par l'intermédiaire du CNPIC ; toutefois, l'intégration complète des opérateurs privés dans le système de renseignement sur les menaces reste un domaine critique où les progrès ne doivent pas être limités. L'asymétrie d'information entre les autorités compétentes, qui peuvent avoir accès à des renseignements classifiés sur les menaces, et les opérateurs privés, qui ont besoin de ces informations pour ajuster

leurs investissements en matière de sécurité, constitue l'un des obstacles les plus tenaces à la mise en place d'une coopération public-privé efficace dans le domaine de la PIC.

7. LE SYSTÈME ESPAGNOL DE PROTECTION DES INFRASTRUCTURES CRITIQUES

7.1. ARCHITECTURE INSTITUTIONNELLE

Le système espagnol de protection des infrastructures critiques repose sur une structure institutionnelle complexe qui relie des institutions de tailles et de spécialités diverses. Le CNPIC, rattaché au Secrétariat d'État à la Sécurité du ministère de l'Intérieur, est chargé de développer, de coordonner et de superviser le système. Il est responsable de la réglementation du Catalogue national des infrastructures stratégiques, l'inventaire classifié du pays sur les infrastructures critiques, de la planification de plans de protection coordonnés et du contrôle du respect des obligations par les opérateurs critiques.

Le CNPIC bénéficie de la coopération permanente du Centre de renseignement contre le terrorisme et le crime organisé (CITCO), l'institution chargée de fournir des renseignements antiterroristes et des informations sur l'Espagne, afin de mettre en place des mesures de protection fondées sur les risques et permettant de les contrer. Le Centre national du renseignement (CNI), par l'intermédiaire du Centre cryptologique national (CCN) et de son équipe d'intervention en cas d'incident CCN-CERT, est l'organisme compétent en matière d' t de cybersécurité pour les administrations publiques et les systèmes d'information des opérateurs de services essentiels.

La complémentarité inhérente aux deux fonctions du CNPIC (axées sur la protection physique et la planification de la sécurité) et du CCN-CERT (axée sur la cybersécurité) est essentielle pour assurer une protection efficace des infrastructures critiques face à une menace pouvant revêtir une dimension à la fois physique et cybernétique. La coordination opérationnelle récente entre ces deux organisations a considérablement évolué et les a amenées à unir leurs forces pour mettre en place des groupes de travail et des protocoles visant à partager des informations sur les incidents à caractère mixte.

Le Département de la sécurité nationale (DSN) est chargé de la coordination stratégique de l'ensemble du système de sécurité nationale, y compris la protection des infrastructures critiques, et relève de la présidence du gouvernement. En matière de sécurité nationale, le DSN assure l'élaboration et le suivi des stratégies de sécurité nationale et assure la liaison avec les outils de coordination stratégique de l'OTAN et de l'UE.

Les forces et corps de sécurité de l'État — la Police nationale et la Guardia Civil — ainsi que les forces armées, par le biais de leurs unités spécialisées, complètent le cadre institutionnel avec une expertise nationale en matière de protection physique, d'intervention lors d'incidents graves et de soutien aux autorités civiles. Le rôle opérationnel de la Guardia Civil au sein de ce système mérite une attention particulière. Par le biais de ses unités spécialisées — en particulier l'Unité centrale opérationnelle (UCO), l'Unité de lutte contre la cybercriminalité (UCC) et les équipes d'intervention NBC —, la Guardia Civil déploie des capacités spécifiques de réponse aux incidents physico-cybernétiques touchant les infrastructures critiques de nature rurale, industrielle

et de transport, qui sont précisément les environnements les plus exposés aux menaces hybrides. La coordination technique et policière étroite entre la Guardia Civil et le CNPIC s'articule autour de protocoles d'action conjointe qui permettent d'activer, en fonction du niveau d'alerte antiterroriste en vigueur, des dispositifs spécifiques de protection des infrastructures dans les secteurs de l'énergie, des transports et de l'eau. Cette complémentarité entre la capacité de renseignement tactique des forces et corps de sécurité et la fonction de coordination stratégique du CNPIC constitue l'un des atouts distinctifs du modèle espagnol de PIC dans le contexte européen comparatif.

7.2. LE SYSTÈME DES NIVEAUX D'ALERTE ANTITERRORISTE (NAA)

Le niveau d'alerte antiterroriste (NAA) désigne le mécanisme mis en place pour mettre en œuvre des mesures de protection adaptées à la menace terroriste du moment. Le NAA à cinq niveaux, mis à jour par la résolution du secrétaire d'État à la Sécurité en 2019 — allant de 1 (faible) à 5 (très élevé) —, est complété par un catalogue de mesures de sécurité appliquées progressivement à divers secteurs stratégiques.

Depuis juin 2015, le niveau 4 (élevé) est en vigueur en Espagne ; il comprend la mise en place de dispositifs de sécurité renforcés pour tous les secteurs stratégiques, tels que des contrôles autour des infrastructures de transport, le renforcement de la surveillance périmétrique des institutions clés et le déploiement de protocoles de communication prioritaires en cas d'incident.

Le lien entre le NAA et le système PIC s'établit par le biais de plans d'intervention, qui déterminent les actions spécifiques que les opérateurs critiques doivent entreprendre en fonction du niveau d'alerte actuel. Cela permet une réponse progressive et coordonnée à mesure que le niveau de menace évolue. Cependant, le maintien du niveau d'alerte 4 pendant plus de dix ans pourrait entraîner une certaine « fatigue de l'alerte » chez les opérateurs critiques, dont les mesures de protection associées à ce niveau risquent de devenir une routine et une partie de leur travail où la vigilance fait défaut.

Il en résulte la nécessité de revoir périodiquement le système d'alerte et de mettre en place des mécanismes permettant d'évaluer l'efficacité réelle de toutes les mesures prises.

7.3. COOPÉRATION INTERNATIONALE

La dimension internationale de la protection des infrastructures critiques revêt une importance croissante dans un contexte où les menaces sont de nature transnationale. L'Espagne participe activement à diverses initiatives de coopération multilatérale dans ce domaine. Au sein d'Europol, le réseau Atlas des unités d'intervention spéciales facilite la coopération opérationnelle entre les forces de police des États membres dans les situations de crise terroriste susceptibles d'affecter les infrastructures critiques.

Le Conseil consultatif de l'Association pour les infrastructures critiques de l'UE (CP-ISAC) encourage l'échange d'informations et de bonnes pratiques entre les autorités nationales et les opérateurs d'infrastructures critiques européens. Dans le cadre de l'OTAN, l'Espagne participe aux mécanismes de protection des infrastructures critiques de l'Alliance, qui ont été considérablement renforcés après le sommet de Madrid de 2022,

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

reconnaissant la résilience des infrastructures critiques comme un élément central de la défense collective.

8. DÉFIS ET PROPOSITIONS D'AMÉLIORATION

L'analyse préalable permet d'identifier les défis et les lacunes du système espagnol de protection des infrastructures critiques qui nécessitent une attention urgente. Les propositions formulées ici sont loin d'être exhaustives, mais elles définissent les axes d'action les plus urgents et les plus susceptibles d'apporter des changements positifs pour améliorer la résilience du système face à la menace terroriste.

8.1. TRANSPOSITION URGENTE DE LA DIRECTIVE CER

Il est donc nécessaire de modifier le cadre réglementaire conformément aux dispositions de la directive CER, afin d'atteindre le niveau requis pour maintenir la cohérence du système espagnol avec le cadre européen et tirer pleinement parti des mécanismes de soutien prévus par la directive.

Il est vivement recommandé d'adopter cette législation, sous la forme d'une loi de réadoption couvrant la protection des infrastructures et des entités critiques, qui abroge la loi n° 8/2011 et fusionne les éléments de la directive CER avec les dispositions de la directive NIS2 en un régime réglementaire unique, assorti d'améliorations significatives des mécanismes de contrôle de la conformité des opérateurs. Cette nouvelle réglementation devrait mettre en place un système d'incitations — déductions fiscales ou accès préférentiel au financement public — afin que les opérateurs privés investissent volontairement dans des mesures visant à renforcer la résilience au-delà des minima légaux. Il est donc nécessaire que la nouvelle loi exige la participation active des opérateurs critiques au processus, de manière à s'aligner formellement sur la réalité opérationnelle de chaque secteur.

8.2. RENFORCEMENT DE LA CYBERSÉCURITÉ INDUSTRIELLE

La convergence IT-OT dans les environnements critiques nécessite un investissement continu dans la cybersécurité industrielle allant au-delà de la simple conformité réglementaire minimale. Il est recommandé de mettre en œuvre un plan national de cybersécurité industrielle afin de définir des normes spécifiques pour les systèmes SCADA/ICS des opérateurs critiques, de promouvoir la certification des composants industriels en référence au règlement (UE) 2019/881, et de soutenir la mise à niveau des systèmes hérités présentant des vulnérabilités connues. Le CCN-CERT devrait encore renforcer sa capacité à accompagner les opérateurs du secteur privé critique en matière de cybersécurité industrielle en créant des équipes sectorielles spécialisées (prioritairement dans les domaines de l'énergie, des transports et de l'eau) capables d'apporter un soutien technique spécifique en cas d'incidents mixtes physiques et cybernétiques.

8.3. AMÉLIORATION DE LA COORDINATION ENTRE LES SECTEURS PUBLIC ET PRIVÉ

La création de plateformes sectorielles pour l'échange d'informations sur les menaces, sur le modèle des Centres d'échange et d'analyse d'informations (ISAC) des États-Unis,

constitue une priorité pour améliorer la coopération entre le secteur public et les opérateurs privés. Ces plateformes, qui devraient fonctionner sous l'égide du CNPIC et avec la participation du CCN-CERT et du CITCO, permettraient un flux bidirectionnel d'informations sur les menaces, les vulnérabilités et les incidents, ce qui renforcerait la capacité de réaction de l'ensemble du système.

Une condition essentielle à leur efficacité est l'adoption d'un cadre juridique garantissant la confidentialité des informations partagées par les opérateurs privés, éliminant ainsi le risque que leur divulgation n'entraîne des responsabilités juridiques ou ne procure des avantages concurrentiels à leurs concurrents.

8.4. FORMATION ET EXERCICES DE SIMULATION

La résilience des infrastructures critiques face aux attaques terroristes dépend dans une large mesure de la préparation du personnel chargé de leur gestion et de leur protection. Il est recommandé d'institutionnaliser un programme national de formation à la protection des infrastructures critiques, comprenant des modules spécifiques destinés aux opérateurs de différents secteurs, ainsi que la mise en œuvre annuelle d'exercices de simulation de crise envisageant des scénarios d'attaques combinées physiques et cybernétiques. Ces exercices, qui devraient impliquer simultanément les autorités compétentes, les forces de sécurité et les opérateurs d'infrastructures critiques, permettent d'identifier les lacunes dans les plans d'intervention, de renforcer la coordination entre les acteurs et de maintenir à jour la culture de sécurité des organisations. Le Centre européen d'excellence pour la lutte contre les menaces hybrides (Hybrid CoE) à Helsinki est un partenaire important pour la conception et la mise en œuvre de ces exercices à l'échelle transnationale.

8.5. RENSEIGNEMENT PRÉVENTIF

Anticiper les menaces terroristes pesant sur les infrastructures critiques nécessite de renforcer les capacités de renseignement stratégique du CITCO et du CNI, en accordant une attention particulière à l'analyse des tendances dans les aspirations opérationnelles des groupes terroristes et des acteurs étatiques hostiles à l'encontre d'objectifs d'infrastructure. L'intégration de données issues de sources ouvertes, y compris la surveillance systématique des forums extrémistes sur le dark web et l'analyse des publications d'organisations terroristes, devrait être systématisée dans le cadre de l'évaluation spécifique des menaces pesant sur chaque secteur stratégique.

Le développement de capacités d'intelligence artificielle appliquées à l'analyse des menaces pesant sur les infrastructures critiques constitue un axe d'investissement prometteur, même si sa mise en œuvre doit s'accompagner de garanties juridiques adéquates préservant les droits fondamentaux.

9. CONCLUSIONS

L'analyse présentée dans ce document nous permet de tirer les conclusions suivantes concernant la menace terroriste qui pèse sur les infrastructures critiques espagnoles et l'état actuel du système de protection.

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

Tout d'abord, l'Espagne dispose d'un cadre réglementaire et institutionnel pour la protection des infrastructures critiques, qui, dans son ensemble, offre un niveau de protection adéquat selon les critères comparatifs européens. La loi n° 8/2011 et ses textes d'application constituent la pierre angulaire d'un système cohérent qui a démontré, depuis plus de dix ans, son efficacité en matière de coordination interinstitutionnelle et de gestion des incidents. Cependant, le retard pris dans la transposition de la directive CER de 2022 crée un vide réglementaire source d'incertitude qui affaiblit la position de l'Espagne au sein du système européen de protection des infrastructures critiques et doit être comblé de toute urgence par une nouvelle législation intégrant l'approche de résilience globale qui caractérise le nouveau cadre européen.

Deuxièmement, le terrorisme djihadiste reste la principale menace terroriste pesant sur les infrastructures critiques espagnoles en termes de probabilité de survenue, comme en témoignent la persistance de cellules actives sur le territoire espagnol et la diffusion continue de propagande incitant à des attaques contre des infrastructures dans toute l'Europe. L'ENCOT 2023 partage cette analyse, soulignant la multiplication des acteurs isolés qui, après des processus d'autoradicalisation dans les environnements numériques, mènent des actions avec des moyens rudimentaires mais d'une grande létalité — un schéma illustré par les attentats de Las Ramblas et de Cambrils —, ce qui représente un défi majeur pour les systèmes de détection précoce. Cependant, la menace que représentent les acteurs étatiques hostiles — en particulier la Russie — et les attaques inspirées par des extrémistes de diverses orientations idéologiques doit être traitée par des efforts stratégiques comparables, compte tenu de leur potentiel à causer des dommages catastrophiques aux infrastructures essentielles.

Troisièmement, la numérisation et la convergence IT-OT ont transformé le paysage des vulnérabilités des infrastructures critiques espagnoles et ont créé de nouveaux vecteurs d'attaque que les systèmes de protection existants ne sont pas toujours en mesure de neutraliser efficacement. Le renforcement de la cybersécurité industrielle doit être considéré comme une priorité nationale de premier ordre, qui ne peut être atteinte que par des investissements soutenus dans la technologie, la formation spécialisée et la mise à jour des cadres réglementaires et des normes techniques.

En quatrième lieu, la coordination entre les secteurs public et privé, bien qu'elle ait considérablement évolué depuis l'adoption de la loi n° 8/2011, reste un domaine critique à améliorer dans le système espagnol. Les infrastructures critiques appartenant au secteur privé nécessitent des mécanismes plus sophistiqués pour harmoniser les incitations et échanger des informations classifiées entre le secteur public et les opérateurs, mécanismes qui ne peuvent être mis en place que sur la base d'un cadre juridique garantissant la confiance et la confidentialité de toutes les parties.

En cinquième lieu, la coopération internationale, non seulement au sein de l'Union européenne, mais aussi au sein de l'OTAN et d'autres instances multilatérales, est un facteur déterminant pour l'efficacité du système de protection des infrastructures critiques espagnoles. La position géographique de l'Espagne, en tant que porte d'entrée entre l'Europe et l'Afrique du Nord, devrait se traduire par un rôle unique dans l'architecture de sécurité européenne, et donc par un engagement spécifique envers les mécanismes de coopération multilatérale existants et le développement de ses propres capacités afin d'apporter une valeur ajoutée à l'ensemble du système.

De futures recherches dans ce domaine devraient se concentrer sur l'analyse sectorielle des vulnérabilités à l'aide de méthodologies d'évaluation quantitative des risques, sur l'étude comparative des modèles de transposition de la directive CER adoptés par les principaux États membres de l'Union européenne, et sur l'évaluation empirique de l'efficacité des mécanismes de coordination public-privé existants à l'aide de méthodologies de recherche primaire menées auprès des opérateurs critiques.

10. RÉFÉRENCES BIBLIOGRAPHIQUES

Arteaga, F. (2023). Infrastructures critiques et sécurité nationale en Espagne. *Real Instituto Elcano.* https://www.realinstitutoelcano.org

Boin, A. et McConnell, A. (2007). Se préparer aux défaillances des infrastructures critiques : les limites de la gestion de crise et la nécessité de la résilience. *Journal of Contingencies and Crisis Management, 15*(1), 50-59. https://doi.org/10.1111/j.1468-5973.2007.00504.x

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

Ministère de la Sécurité nationale. (2021). *Stratégie nationale de sécurité.* Présidence du gouvernement espagnol.

ENISA. (2024). *ENISA Threat Landscape 2024.* Agence de l'Union européenne pour la cybersécurité. https://www.enisa.europa.eu

Europol. (2023). *Rapport sur la situation et les tendances du terrorisme dans l'Union européenne (TE-SAT) 2023.* Office des publications de l'Union européenne.

Europol. (2024). *Rapport sur la situation et les tendances du terrorisme dans l'Union européenne (TE-SAT) 2024.* Office des publications de l'Union européenne. https://www.europol.europa.eu

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

Masse, T. (2020). *Terrorisme et infrastructures critiques : évaluation de la menace.* Service de recherche du Congrès.

Ministère de l'Intérieur. (2023). *Stratégie nationale contre le terrorisme (ENCOT) 2023.* Secrétariat d'État à la Sécurité. https://www.dsn.gob.es/es/publicaciones/estrategias-sectoriales/ENCOT2023

Moteff, J. D. (2014). *Infrastructures critiques : contexte, politique et mise en œuvre.* Service de recherche du Congrès.

Reinares, F. (2014). Al-Qaïda et le 11-M en Espagne. *Revista de Occidente, 400,* 75-95.

Reinares, F. et García-Calvo, C. (2022). *Le terrorisme djihadiste en Espagne : caractéristiques et tendances.* Real Instituto Elcano. https://www.realinstitutoelcano.org

Rinaldi, S. M., Peerenboom, J. P. et Kelly, T. K. (2001). Identifier, comprendre et analyser les interdépendances des infrastructures critiques. *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. RÉGLEMENTATION

Nations Unies. Résolution 1373 (2001) du 28 septembre. Conseil de sécurité des Nations Unies. S/RES/1373 (2001).

Conseil de l'Europe. Convention sur la prévention du terrorisme (STE n° 196). Varsovie, 16 mai 2005. En vigueur depuis le 1er juin 2007.

Union européenne. Directive 2008/114/CE du Conseil, du 8 décembre 2008, relative à l'identification et à la désignation des infrastructures critiques européennes. *Journal officiel de l'Union européenne*, L 345, du 23 décembre 2008.

Espagne. Loi n° 8/2011 du 28 avril établissant des mesures pour la protection des infrastructures critiques. *Journal officiel de l'État*, n° 102, du 29 avril 2011.

Espagne. Décret royal n° 704/2011 du 20 mai approuvant le règlement relatif à la protection des infrastructures critiques. *Journal officiel de l'État*, n° 121, du 21 mai 2011.

Espagne. Loi organique n° 4/2015 du 30 mars relative à la protection de la sécurité des citoyens. *Journal officiel de l'État*, n° 77, du 31 mars 2015.

Nations Unies. Résolution 2341 (2017), du 13 février. Conseil de sécurité des Nations Unies. S/RES/2341 (2017).

Espagne. Décret royal n° 1150/2021 du 28 décembre portant approbation de la stratégie nationale de sécurité. *Journal officiel de l'État*, n° 311, du 29 décembre 2021.

Espagne. Décret royal n° 311/2022 du 3 mai régissant le dispositif national de sécurité. *Journal officiel de l'État*, n° 105, du 4 mai 2022.

Union européenne. Directive (UE) 2022/2555 du Parlement européen et du Conseil, du 14 décembre 2022, relative aux mesures visant à garantir un niveau commun élevé de cybersécurité dans l'ensemble de l'Union (directive NIS2). *Journal officiel de l'Union européenne*, L 333, du 27 décembre 2022.

Union européenne. Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 relative à la résilience des entités critiques (directive CER). *Journal officiel de l'Union européenne*, L 333, du 27 décembre 2022.