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

Research Article

SPANISH CRITICAL INFRASTRUCTURE AS A TARGET FOR TERRORISTS. ANALYSIS OF VULNERABILITIES, REGULATORY FRAMEWORK AND PROTECTION STRATEGIES

English translation with AI assistance (DeepL)

Raúl Moreno Ruiz
Captain, Guardia Civil
Prison Security Specialist (Ministry of the Interior)
Master's Degree in Operational Security Management – Bachelor's Degree in Law
raul.moreno@dgip.mir.es

Received 23/03/2026
Accepted 04/06/2026
Published 30/06/2026

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

Recommended citation: Moreno, R. (2026). Spanish critical infrastructure as a target for terrorists. Analysis of vulnerabilities, regulatory framework and protection strategies. Revista Logos Guardia Civil, 4(2), pp. 281–302. https://doi.org/10.64217/logosguardiacivil.v4i2.8979

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

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

SPANISH CRITICAL INFRASTRUCTURE AS A TARGET FOR TERRORISTS. ANALYSIS OF VULNERABILITIES, REGULATORY FRAMEWORK AND PROTECTION STRATEGIES

Abstract: The vulnerability of Spain's critical infrastructure to the terrorist threat from a legal, institutional and operational perspective. The study examines the existing regulatory framework — through Law 8/2011 and Directive (EU) 2022/2557 on the resilience of critical entities (CER) — focuses on the key sectors most vulnerable to risk, and assesses the institutional architecture of the Spanish protection system. Using a methodology based on documentary analysis and a review of specialist literature, the study finds that, despite a robust critical infrastructure protection (CIP) system in Spain, there are significant gaps in industrial cybersecurity, inter-administrative coordination and the transposition of European directives, which require urgent attention. The main threats for the 2025–2030 period are identified as jihadist terrorism, hostile state actors and cyberterrorism.

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.

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

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

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

ABBREVIATIONS

CCN-CERT: National Cryptology Centre – Computer Emergency Response Team

CITCO: Centre for Intelligence against Terrorism and Organised Crime

CNI: National Intelligence Centre

CNPIC: National Centre for the Protection of Critical Infrastructure

DSN: Department of National Security

ENISA: European Union Agency for Cybersecurity

ICS: Industrial Control Systems

ICE: European Critical Infrastructure

ICN: National Critical Infrastructure

IoT: Internet of Things

NAA: Terrorist Threat Level

NIS: Network and Information Security

PES: Sectoral Strategic Plan

PIC: Critical Infrastructure Protection

PNPIC: National Plan for the Protection of Critical Infrastructure

PSO: Operator Security Plan

SCADA: Supervisory Control and Data Acquisition

TE-SAT: EU Terrorism Situation and Trend Report

ENCOT: National Counter-Terrorism Strategy

1. INTRODUCTION

Terrorism has undergone a radical transformation over the years, both in its nature and in the objectives it pursues. Terrorist attacks in the 20th century focused predominantly on a small percentage of people: political leaders, military personnel or civilians in public facilities. However, today, the current trend is an increase in the number of attacks on vital infrastructure and systems that enable the development and functioning of a modern state. This strategic shift is no accident; it follows a logic of maximising impact that terrorist and militant groups have refined over time: disrupting the material foundations of society generates a far greater destabilising and psychological impact than that of conventional attacks, which are high-profile but have little structural impact. This comes as no surprise to Spain.

On 11 March 2004, when several commuter trains operating on the Renfe network in Madrid were destroyed, killing 193 people and injuring more than 2,000, this constituted the most devastating terrorist attack on Spain's transport infrastructure. At that time, the critical infrastructure protection system was in its infancy, but the event catalysed a legislative and organisational process that resulted in the adoption of Law 8/2011 of 28 April, the first comprehensive regulatory framework at national level. To date, the experience gained has enabled the development of a protection system that now faces qualitative challenges arising from the very challenges that led to its creation.

By the first half of the 2020s, the threat landscape in Europe had changed considerably. The ongoing Russian aggression against Ukraine since February 2022 demonstrated the vulnerability of European energy infrastructure to hostile state actors through the sabotage of the Nord Stream gas pipelines in September 2022. And jihadist terrorism, particularly linked to Daesh and Al-Qaeda, remains a persistent threat across Europe, with active residual cells and a worrying capacity for online radicalisation to fuel the phenomenon of the so-called 'lone wolf'. Furthermore, right-wing radicalism has seen a worrying resurgence within many European Union nations, broadening the scope of conventional forms of terrorist threat beyond mere calls for jihadism.

This article aims to explore, from a multidisciplinary and academic perspective, the threat that terrorist elements pose to Spain's critical infrastructure. To this end, the study will examine the relevant regulatory frameworks at national, European and international levels in Spain; identify the most vulnerable strategic sectors; scrutinise the institutional framework of the Spanish Critical Infrastructure Protection (CIP) system; and propose improvement mechanisms designed to enhance the system's resilience for the period 2025 to 2030.

The present study adopts an integrative approach that combines legal analysis with the perspectives of security studies and criminology, on the basis that the complexities of the phenomenon require a multifaceted and complementary approach. The guiding hypothesis underpinning the research is expressed as follows: Spain has a robust regulatory system and an institutional framework covering critical infrastructure in line with European standards, but it also has structural vulnerabilities, particularly with regard to industrial cybersecurity and public-private partnerships, which terrorist actors could exploit in a context of growing and diversifying threats.

In line with this hypothesis, the paper will demonstrate that the response to this threat requires a new approach, involving not only reforming the current regulatory framework for critical infrastructure, but also rethinking governance models and the partnership between the public sector and private operators of critical infrastructure. This specific methodology is based on a documentary analysis of primary sources — legislation, official reports, strategic documents — and secondary sources — specialist academic literature, reports from international organisations — covering a reference period from the adoption of Law 8/2011 to 2025.

2. METHODOLOGY

The research adopts a qualitative design based on systematic documentary analysis, an approach suited to the study of legal and institutional phenomena in which an understanding of the regulatory and conceptual framework is a prerequisite for any empirical assessment. The gap that this study aims to fill lies in the absence of research that coherently integrates the three dimensions – legal, institutional and operational – of the Spanish CIP system in the face of the terrorist threat, incorporating the most recent European regulatory developments (the CER Directive and NIS2, both from 2022) and the new National Counter-Terrorism Strategy of 2023.

The primary sources comprise: national legislation (Law 8/2011, Royal Decree 704/2011, Organic Law 4/2015, Royal Decree 311/2022 and Royal Decree 1150/2021); European regulations (CERT Directive 2022/2557, NIS2 Directive 2022/2555 and Directive 2008/114/EC); international instruments (UN Security Council Resolutions 1373/2001 and 2341/2017; CETS No. 196); and official strategic documents (National Security Strategy 2021, ENCOT 2023, annual reports of the CNPIC). Secondary sources include specialist academic literature on national security, critical infrastructure protection and terrorism, retrieved through a systematic search of the Scopus, Web of Science and Google Scholar databases, using the following keywords: ‘critical infrastructure protection’, ‘terrorism’, ‘hybrid threats’, ‘CIP Spain’, ‘infraestructuras críticas’, ‘terrorismo’ and ‘resiliencia’; as well as reports from international organisations (Europol TE-SAT, ENISA Threat Landscape). The following inclusion criteria were applied: publications in Spanish or English, covering the period 2001–2025, and direct relevance to the subject of the study. Works of a purely descriptive nature offering no analytical or propositional contribution were excluded, as were unverifiable sources or those with restricted dissemination.

3. CONCEPTUAL FRAMEWORK: WHAT IS CRITICAL INFRASTRUCTURE?

The concept of ‘critical infrastructure’ is not unambiguous in academia or in regulation. As modern societies have become increasingly dependent on certain critical systems or services, its definition has evolved. For the purposes of this paper, within the scope and parameters of Law 8/2011, critical infrastructure refers to information and communication technology facilities, networks, services and equipment whose disruption or destruction would have a significant impact on the health, safety or economic well-being of citizens, or on the effective functioning of State institutions and public administrations. This definition reflects a perspective on potential impact that focuses not so much on the nature of the infrastructure, but rather on the consequences of its failure or destruction for society as a whole.

3.1. SECTORAL CLASSIFICATION

Article 2 of Royal Decree 704/2011 identifies twelve strategic sectors subject to protection under the Spanish PIC system: administration, water, food, energy, space, the nuclear industry, the chemical industry, research facilities, health, the financial and tax systems, information and communication technologies (ICT), and transport. This categorisation is consistent with the description given in Directive (EU) 2022/2557 (the CER Directive), which expands the set of sectors to eleven and explicitly defines digital infrastructure, space and public administration as specific categories.

The relative importance of sectors in terms of security varies according to different types of threats and the potential consequences of a disruption, but essentially, the energy, transport and ICT sectors in Spain are relatively concentrated in terms of their key assets. Based on data provided by the CNPIC, Spain has more than 3,700 designated critical operators spread across the twelve strategic sectors, with the ICT and energy sectors accounting for the largest number of operators in absolute terms.

3.2. NATIONAL CRITICAL INFRASTRUCTURE AND EUROPEAN CRITICAL INFRASTRUCTURE

The distinction between national critical infrastructure (NCI) and European critical infrastructure (ECI) is particularly relevant in the context of EU legislation. An infrastructure is designated as ECI if its disruption or destruction would seriously affect two or more Member States, or the EU as a whole. Directive 2008/114/EC was the first to establish this concept; it initially restricted its scope to the energy and transport sectors. The 2022 CER Directive broadens the scope of the concept and strengthens the means for identifying and protecting such infrastructure. Spain has designated several such facilities as ECI, mainly in the energy and transport sectors, given the country's strategic role as an energy and communications corridor between Europe and North Africa – a geopolitical position which, whilst granting Spain a central role in the European security architecture, increases its exposure to certain transnational threats.

3.3. THE CONCEPT OF INTERDEPENDENCE

A central theme in the analysis of critical infrastructure is the issue of interdependence. Today's critical systems do not operate in isolation; they are heavily reliant on other systems on which their operation depends. The electricity industry relies on telecommunications infrastructure for its automated management; rail transport is powered by electricity; and the financial sector depends on ICT for virtually all its operations. Such interdependence creates what the specialist literature refers to as 'cascading effects': the failure of one infrastructure can cause the successive failure of others, with potentially devastating consequences for the entire system (Rinaldi et al., 2001).

The increasing digitalisation of critical systems — linked to IoT technologies, cloud-based data platforms and SCADA industrial control systems — has amplified these interdependencies, giving rise to new vectors of vulnerability that more sophisticated terrorist groups are beginning to exploit systematically. This interdependence is not merely a technical or cyber issue; it involves geographical aspects — cross-border infrastructure such as electricity grids or gas pipelines — cyber aspects — shared or

interconnected control systems — and organisational aspects — operators managing assets across numerous sectors.

The multifaceted nature of such interdependence makes the analysis of critical infrastructure risk an immensely complex process that cannot be reduced to examining each piece of infrastructure in isolation.

4. REGULATORY FRAMEWORK

The protection of critical infrastructure against terrorist threats and other deliberate threats is structured through a complex, multi-level regulatory framework, comprising national, European and international provisions. This regulatory architecture also reflects the growing understanding that the threat to critical infrastructure transcends national borders and requires coordinated responses at different levels of governance. Each of these levels is discussed in subsequent sections, with a focus on the latest regulatory developments and the challenges posed by their implementation.

4.1. SPANISH LEGISLATION

Law 8/2011 of 28 April forms the basis of Spanish national legislation on the protection of critical infrastructure. This Act transposes Directive 2008/114/EC into Spanish law and establishes the Critical Infrastructure Protection System, a framework based on three fundamental principles: the National Centre for the Protection of Critical Infrastructure (CNPIC), the National Catalogue of Strategic Infrastructure and protection planning. It distinguishes between the National Plan for the Protection of Critical Infrastructure (PNPIC), the Sectoral Strategic Plans (PES) and the Operator Security Plans (PSO) within Spain's legal framework and provides a 'tiered, high-level' plan that is developed from the general to the specific level. The PIC Act is implemented through Royal Decree 704/2011 of 20 May, which sets out the provisions for the protection of critical infrastructure.

This regulation sets out the criteria for the designation of critical operators, the minimum content of Operator Security Plans and Specific Protection Plans, and the responsibilities regarding the reporting of incidents. Of particular relevance is Article 24, which establishes the inspection and supervision regime for critical operators, thereby enabling the CNPIC to verify compliance with security obligations. Several authors have highlighted how this compliance oversight has, in practice, been identified as a weakness in the system, given the large number of operators and the limited resources available for operational management. The 2021 National Security Strategy, as authorised by Royal Decree 1150/2021, identifies terrorism as one of the key risks of concern and threats to Spain, and regards the protection of critical infrastructure as a key objective of the national security system, within the holistic approach to security that characterises the Spanish system.

In line with this, the 2023 National Counter-Terrorism Strategy (ENCOT) — which updates and replaces the 2019 version — structures the State's counter-terrorism response around four pillars of action (prevent, protect, pursue and respond) and places the protection of critical infrastructure at the heart of the 'protect' pillar. The 2023 ENCOT introduces a major conceptual innovation by institutionally acknowledging that absolute invulnerability is unattainable, shifting the strategic focus from mere static protection

towards comprehensive resilience, understood as the capacity to absorb the impact of an incident, ensure the continuity of essential services and restore normality swiftly. This vision is fully aligned with the approach of the 2022 CER Directive, making ENCOT 2023 a doctrinal bridge between the national counter-terrorism strategy and the European framework for critical entities. Furthermore, ENCOT 2023 highlights the shift in the threat towards so-called 'soft targets' — places of worship, mass gatherings and public spaces — which, whilst not constituting critical infrastructure in the technical sense, are crucial to public safety; a reality that directly challenges the scope of application of the future transposition legislation. In terms of cybersecurity, the National Security Framework, approved by Royal Decree 311/2022, sets out minimum requirements for the information systems of public administrations and their essential service operators, thereby complementing the PIC regime with regard to the information assets of critical operators.

Organic Law 4/2015 of 30 March on the Protection of Public Safety introduces significant measures for controlling access to sensitive facilities and monitoring high-risk environments, complementing the physical protection system provided by the PIC regulations.

4.2. EUROPEAN LEGISLATION

The European Union's regulatory framework has been thoroughly revised following the adoption of Directive (EU) 2022/2557 (14 December 2022) on the resilience of critical entities (the CER Directive). This regulation replaces Directive 2008/114/EC and establishes a reconceptualised framework that focuses on the comprehensive resilience of entities operating infrastructure, rather than solely on the physical provision and protection of systems; resilience is defined as their ability to prevent incidents, withstand their impact, respond to the consequences and recover swiftly. Key developments in the CER Directive include the expansion of the sectoral scope from two sectors to eleven, the need for strengthened requirements on risk analysis and incident reporting, and the establishment of an EU mechanism to support Member States in identifying critical entities—those of particular European significance.

The deadline for transposing the CER Directive was 17 October 2024. Spain had not completed this process by that date, leaving it in a state of non-compliance which could lead to infringement proceedings by the European Commission if the situation persists. This delay stems from the technical and political complexity involved in transposition, which entails amending or repealing Law 8/2011 and its implementing regulations, as well as revising the National Catalogue of Strategic Infrastructures to bring it into line with the new sectors covered and to reform the mechanisms for interministerial and intersectoral cooperation.

The NIS2 Directive (Directive (EU) 2022/2555), which was adopted on the same day as the CER Directive, revises and repeals the 2016 NIS Directive and sets out measures to maintain a high common level of cybersecurity across the EU. It greatly broadens the scope of cybersecurity regulations, moving from 'operators of essential services' to 'essential and important entities', and entails strengthened responsibilities based on risk management, incident reporting and cross-border cooperation.

The interaction between the CER Directive and NIS2 is one of the most complex aspects of this new European framework: both directives apply to many of the same entities, yet from different perspectives – namely (1) comprehensive physical resilience and (2) cybersecurity – and therefore require a coordinated approach during transposition to avoid overlaps and contradictions.

4.3. INTERNATIONAL FRAMEWORK

On the international stage, United Nations Security Council Resolution 1373 (2001) sets out the obligations of all States in the fight against terrorism, including requirements to implement measures to prevent the use of their territory for terrorist activities and to exchange information with other States.

Security Council Resolution 2341 (2017) is the Council's first instrument specifically dedicated to the protection of critical infrastructure against terrorism, urging States to develop protective measures proportionate to the identified risk and promoting international cooperation in relation to the cyber dimension of the threat. The Convention on the Prevention of Terrorism (CETS No. 196), in force since 2007, and its 2015 Additional Protocol establish obligations regarding criminalisation and judicial cooperation that complement the UN framework.

5. TERRORISM AS A SPECIFIC THREAT TO CRITICAL INFRASTRUCTURE

5.1. TYPES OF TERRORIST GROUPS TARGETING CRITICAL INFRASTRUCTURE

Terrorism therefore stands as one of the most complex and multifaceted threats to the critical infrastructure of contemporary society. Unlike other threats such as natural disasters or accidental technological failures, terrorism is characterised by malicious intent and strategic rationality, meaning that terrorists adapt and refine their tactics, techniques and procedures in response to the protective measures deployed. An effective protective response therefore requires an equally dynamic and proactive reaction to the adaptive nature of the threat, which cannot be limited to static physical and logical security measures.

5.1.1. Jihadist terrorism

Jihadist-inspired terrorism, particularly associated with groups such as Daesh and Al-Qaeda, has repeatedly expressed a strategic interest in attacking key infrastructure in Western countries. In pamphlets published, for example, in *Dabiq* or *Inspire*, both groups have included explicit guidance on attacking power stations, drinking water sources and transport facilities in Europe and North America, paying particular attention to the knock-on effects of disrupting interconnected infrastructure.

In Spain, more specifically, the attack (in August 2017) on La Rambla in Barcelona and Cambrils by a Daesh cell demonstrated how the jihadist threat remained present at a national level, although, on this occasion, its aim was to inflict casualties in public spaces rather than to attack a specific piece of infrastructure. According to Europol's TE-SAT 2024 report, jihadist terrorism remains the most serious threat to the European Union in terms of the number of operations, arrests and attacks carried out or foiled.

In this context, Spain finds itself in a particularly vulnerable position: its status as a transit country between North Africa and Europe, the migratory flows crossing its southern borders, and the presence of communities with documented levels of radicalisation. The 'lone wolf' model, in which an individual acts autonomously after being radicalised via digital channels, poses unique challenges for early detection and currently represents the most likely profile for jihadist-inspired terrorist attacks on Spanish soil.

5.1.2. Hostile state actors and hybrid threats

This category of hostile state actors warrants special consideration within the context of threats to critical infrastructure. The body of evidence gathered since 2014 suggests that Russia has developed and deployed advanced capabilities to sabotage critical infrastructure in Europe, through direct cyber means (including attacks by the Sandworm group against the Ukrainian power grid in 2015 and 2016) and through covert physical sabotage activities.

The most spectacular example is the sabotage of the Nord Stream gas pipelines in September 2022, which cut off the supply of natural gas to Europe from Russia and demonstrates the willingness of state actors to attack Europe's infrastructure with the intention of using it as a geopolitical lever.

The concept of a 'hybrid threat' refers to the combination of a range of traditional and unconventional tools, including disinformation, cyber-attacks, physical sabotage and economic pressure, to create an integrated 'hybrid threat strategy' designed to weaken a state without crossing the threshold into conventional armed conflict. This type of threat – in which Russia has emerged as the most active actor in Europe in recent years – poses a particular challenge for systems whose primary objective is to protect critical infrastructure, where the underlying threat is typically addressed as a series of individual traditional threats. Iran and North Korea, which are also viewed by experts as cyber attackers targeting critical infrastructure, have demonstrated cyberattack capabilities against critical infrastructure, although the actual danger they pose to Spanish territory is now considered less substantial than the Russian threat.

5.1.3. Far-right terrorism

Although far-right terrorism does not generally focus on attacking infrastructure in the same way as jihadist terrorism, it has been linked to several serious incidents in Europe in recent years. The attacks in Utøya (Norway, 2011), Hanau (Germany, 2020) and Christchurch (New Zealand, 2019) have highlighted the lethal capacity of such actors.

In the field of critical infrastructure, some far-right extremist cells have shown an interest in targeting communications, energy or transport infrastructure as a means of destabilising society and bringing about a collapse of the established order – a process these groups refer to as 'acceleration'. This phenomenon is recognised as an emerging threat by the EU Strategy for the Security Union 2020–2025, which maintains that, in the field of intelligence as well as in regulatory frameworks, it must be treated and addressed with the same seriousness as jihadist terrorism.

5.2. RELEVANT HISTORICAL CASES

The attack of 11 March 2004 in Madrid remains, without doubt, the benchmark case in Spain. During the morning rush hour, the coordinated detonation of ten explosive devices on commuter trains exploited the inherent vulnerabilities of mass transit systems; these systems are open, passengers are concentrated, and it is difficult to implement a comprehensive security infrastructure without sacrificing the efficiency of the service. The attack resulted in 193 deaths and over 2,000 injuries, and had a major economic and social impact (Reinares, 2014). Not only was it immediately effective: 11 March exposed the rail transport infrastructure as having structural vulnerabilities that had not been sufficiently taken into account in the security plans of the time. In the European context, the 2016 attack in Brussels, which involved the detonation of explosive devices at Zaventem International Airport and within the city's metro system, demonstrates how terrorists are capable of striking two or more transport infrastructure hubs simultaneously, maximising the psychological and media impact.

An international airport is considered a deliberate target: this type of airport brings together large numbers of people of different nationalities in a single location, which attracts significant international media attention; indeed, disruption to such an airport creates economic and reputational consequences that are disproportionate to the material cost of the attack. In the Spanish context, a series of acts of sabotage against fibre-optic infrastructure reported in several autonomous communities in 2024 highlighted the vulnerability of telecommunications networks to deliberate acts of destruction; demonstrating that the disruption of vital infrastructure can be carried out using relatively simple technical methods where assets lack adequate physical protection.

5.3. CYBERTERRORISM AND HYBRID ATTACKS AS THE NEW FRONTIER

Cyberterrorism, defined as the deliberate use of computer capabilities (for intimidation or political pressure) to wreak havoc on critical infrastructure, is the newest – and possibly most disruptive – aspect of terrorist attacks against high-value infrastructure. And unlike traditional terrorism, cyber-attacks can be carried out remotely, in some cases without being traceable, and from various locations, making attribution and control a far more complex challenge for the authorities.

The interconnection and convergence of cyberspace and industrial control systems has led to what some call the 'fifth domain of warfare' (Clarke and Knake, 2010), where terrorists are able to inflict real physical damage on critical infrastructure without having to be in close proximity to it. The US attack on the Colonial Pipeline (May 2021) using ransomware highlighted just how vulnerable critical energy infrastructure is to such cyberattacks and how quickly such attacks can lead to supply shortages and public alarm.

In Europe, the cyber-attacks on the Ukrainian electricity company Ukrenergo in 2015 and 2016, carried out by individuals associated with the Russian state, left large areas of Ukraine without electricity for several hours, a harbinger that attacks on energy infrastructure in Europe could emerge at a time of growing geopolitical conflict.

According to the ENISA Threat Landscape 2024 survey, the cyber threat to industrial infrastructure in critical sectors in Europe rose by 78% between 2022 and 2023, demonstrating the growing trend in this type of attack.

6. VULNERABILITIES OF SPANISH CRITICAL INFRASTRUCTURE

In an effort to analyse the vulnerabilities of Spain's critical infrastructure system in the face of the terrorist threat, the approach must be both sector-specific — taking into account the specific characteristics of each strategic sector — and cross-cutting, identifying the structural weaknesses common to the entire system. The sections below first address the specific vulnerabilities of the sectors at greatest risk, followed by an examination of cross-cutting vulnerability factors.

6.1. SECTORAL ANALYSIS OF VULNERABILITIES

6.1.1. Energy Sector

The energy sector represents one of the priority targets for sophisticated terrorist groups due to the magnitude of the potential impact of a successful attack. Spain operates a high-voltage electricity grid, which connects the mainland system with the Canary Islands and the Balearic Islands, and with France and Portugal via the Pyrenean interconnectors, and is operated by Red Eléctrica de España (REE). The concentration of critical assets at certain network nodes — power stations, load dispatch centres and high-voltage transformers — and the fact that replacing them following severe damage takes months, creates particular vulnerabilities to coordinated physical or cyber attacks. Furthermore, the existing and operational nuclear power stations in Spain — Almaraz, Ascó, Cofrentes, amongst others — require protection at various levels due to the potentially catastrophic effects of incidents at these sites, but their physical and radiological security is monitored at all times by the Nuclear Safety Council (CSN).

6.1.2. Transport Sector

Spain has one of the most extensive high-speed rail networks in the world, with over 3,900 kilometres of operational high-speed lines. This infrastructure, with passenger concentrations at major stations — Atocha, Sants, Santa Justa — as well as certain elements that make it vulnerable, such as tunnels, viaducts and signalling systems, represents prime targets for terrorists to exploit. Adolfo Suárez Madrid-Barajas Airport, the fourth busiest airport in Europe with over 62 million passengers a year, and the Port of Algeciras, Spain's main container port and a gateway for goods from North Africa, present high-risk characteristics that require particularly rigorous security measures.

6.1.3. ICT Sector

Spain's digital infrastructure has grown rapidly in recent years due to the digitalisation of the economy, as well as the roll-out of 5G and the adoption of cloud computing infrastructure. The submarine communications cables connecting Spain to the rest of the world — including those linking the Iberian Peninsula to the Canary Islands and the Americas — have also become a major vulnerability, as evidenced by the incidents recorded in the Red Sea and the Baltic Sea between 2023 and 2025. These cables carry the bulk of international data and voice traffic, and their deliberate damage could lead to a loss of communication capacity on a continental scale. Given the geographical dispersion of ICT assets and the rapid evolution of both technologies and attack vectors, the CNPIC noted that the ICT sector presents some of the most pressing challenges in terms of protection.

6.2. RISKS ARISING FROM DIGITALISATION AND CONNECTIVITY

The adoption of information technology (IT) and operational technology (OT) in industrial contexts is one of the most significant—and most worrying from a security perspective—trends of the last ten years. The so-called 'air gap' between industrial control systems (ICS/SCADA) and corporate networks and the internet has led to the gradual integration of IT systems into digital environments to improve operational efficiency and the management of remote repairs.

This connectivity creates new attack surfaces that can be exploited by terrorist groups with advanced cyber capabilities. The number of IoT devices installed as key components of critical systems—such as temperature sensors, security cameras and access control systems—exacerbates the threat by introducing components that are not inherently secure when integrated into security-critical operating systems. The absence of security updates for embedded devices, the existence of outdated industrial communication protocols lacking cryptographic capabilities, and the shortage of professional cybersecurity experts within the industrial sector severely increase this level of vulnerability.

6.3. PUBLIC–PRIVATE COORDINATION: THE CHALLENGE AHEAD

A systemic characteristic of Spain's critical infrastructure system that has created specific vulnerabilities is that the majority of critical operators are privately owned. Of the approximately 3,700 designated operators in Spain, the majority are private or mixed-ownership entities, which presents an ongoing challenge given that private interests prioritise profit and efficiency over national security.

In this regard, and in the context of these obligations, combined with the provisions of the Critical Infrastructure Act (PIC), critical operators must draw up Operator Security Plans and Specific Protection Plans for their operations; however, the investment made in these schemes often exceeds the minimum compliance requirements of the PIC Act, at least where there are very few economic reasons to commit such a sum of capital. The exchange of information and mutual trust between the public and private sectors are highlighted in the specialist literature as critical components for the effectiveness of the CIP system (Moteff, 2014).

In this regard, Spain has established mechanisms for information exchange and early-warning systems through the CNPIC; however, the full integration of private operators into the threat intelligence system remains a critical area where progress must not be limited. The information asymmetry between the competent authorities, who have access to classified threat intelligence, and private operators, who require this knowledge to gauge their security investments, is one of the most enduring barriers to forging effective public–private cooperation in CIP.

7. THE SPANISH CRITICAL INFRASTRUCTURE PROTECTION SYSTEM

7.1. INSTITUTIONAL ARCHITECTURE

Spain's Critical Infrastructure Protection System is based on a complex institutional structure linking institutions of various sizes and specialisms. The CNPIC, within the

State Secretariat for Security of the Ministry of the Interior, is responsible for developing, coordinating and supervising the system. It is responsible for regulating the National Catalogue of Strategic Infrastructure – the country's classified inventory of critical infrastructure – planning coordinated protection schemes and monitoring compliance by critical operators.

The CNPIC benefits from the ongoing cooperation of the Centre for Intelligence against Terrorism and Organised Crime (CITCO), the institution responsible for providing counter-terrorism intelligence and information on Spain, in order to deliver risk-based protection measures capable of countering such threats. The National Intelligence Centre (CNI), through the National Cryptology Centre (CCN) and its incident response team, CCN-CERT, is the competent body for cybersecurity for public administrations and the information systems of essential service operators.

The inherent complementarity between the roles of the CNPIC (focused on physical protection and security planning) and the CCN-CERT (focused on cybersecurity) is key to the effective protection of critical infrastructure against a threat that can manifest itself in both physical and cyber forms. Recent operational coordination between the two organisations has evolved significantly, leading them to join forces to set up working groups and develop protocols for sharing information on incidents of a hybrid nature.

The Department of National Security (DSN) is responsible for the strategic coordination of the entire national security system, including the protection of critical infrastructure, and reports to the Office of the Prime Minister. In matters of national security, the DSN develops and monitors National Security Strategies and acts as a liaison with NATO and the EU's strategic coordination mechanisms.

The State Security Forces and Corps — the National Police Force and the Guardia Civil — and the Armed Forces, through their specialised units, complete the institutional framework with national expertise in physical protection, response to major incidents and support for civil authorities. The operational role of Guardia Civil within this system deserves special attention. Through its specialised units — in particular the Central Operational Unit (UCO), the Cybercrime Unit (UCC) and the CBRN Response Teams — the Guardia Civil deploys specific capabilities to respond to physical and cyber incidents affecting critical infrastructure in rural, industrial and transport sectors, which are precisely the environments most exposed to hybrid threats. Close technical and police coordination between the Guardia Civil and the CNPIC is organised through joint action protocols which enable the activation, depending on the current counter-terrorism alert level, of specific infrastructure protection measures in the energy, transport and water sectors. This complementarity between the tactical intelligence capabilities of the security forces and the strategic coordination function of the CNPIC constitutes one of the distinguishing features of the Spanish CIP model in a comparative European context.

7.2. THE SYSTEM OF COUNTER-TERRORISM ALERT LEVELS (NAA)

The Counter-Terrorism Alert Level (NAA) refers to the mechanism established to implement protective measures commensurate with the terrorist threat at any given time. The five-level NAA, which was updated by the Resolution of the Secretary of State for Security in 2019 — ranging from 1 (low) to 5 (very high) — is complemented by a catalogue of security measures applied progressively across various strategic sectors.

Since June 2015, Level 4 (high) has been in force in Spain, involving the implementation of enhanced security arrangements for all strategic sectors, such as checks at transport infrastructure, increased perimeter surveillance of key institutions and the deployment of priority communication protocols for incidents.

The link between the NAA and the PIC system is established through Response Plans, which set out the specific actions that critical operators must take according to the current alert level. This enables a phased and coordinated response as the threat level changes. However, maintaining alert level 4 for more than ten years could lead to a certain degree of 'alert fatigue' amongst critical operators, whose protective measures associated with this level may become routine and an insufficiently vigilant part of their work.

The implication is that the alert system needs to be reviewed periodically and mechanisms established to assess the true effectiveness of all measures taken.

7.3. INTERNATIONAL COOPERATION

The international dimension of critical infrastructure protection is becoming increasingly relevant in a context where threats are transnational in nature. Spain actively participates in various multilateral cooperation initiatives in this field. Within Europol, the Atlas Network of Special Intervention Units facilitates operational cooperation between the police forces of member states in terrorist crisis situations that may affect critical infrastructure.

The Advisory Board of the EU Critical Infrastructure Partnership (CP-ISAC) promotes the exchange of information and best practice between national authorities and European critical infrastructure operators. Within the framework of NATO, Spain participates in the Alliance's critical infrastructure protection mechanisms, which were significantly strengthened following the 2022 Madrid summit, recognising the resilience of critical infrastructure as a central element of collective defence.

8. CHALLENGES AND PROPOSALS FOR IMPROVEMENT

The preliminary analysis identifies the challenges and gaps in the Spanish system for the protection of critical infrastructure that require urgent attention. The proposals set out here are far from exhaustive, but they do outline the most urgent courses of action with the greatest potential for positive change to improve the system's resilience in the face of the terrorist threat.

8.1. URGENT TRANSPOSITION OF THE CER DIRECTIVE

It is therefore necessary to amend the regulatory framework in accordance with the terms of the CER Directive to the standard required to ensure the Spanish system remains consistent with the European framework and to make the most of the support mechanisms incorporated into the Directive.

It is strongly recommended that this legislation be adopted, in the form of a re-enactment act covering the protection of critical infrastructure and entities, which repeals Law 8/2011 and merges the elements of the CER Directive with the provisions of NIS2 into a single regulatory regime, with significant improvements to the mechanisms for

monitoring operators' compliance. This new regulation should implement a system of incentives — such as tax deductions or preferential access to public funding — to encourage private operators to invest voluntarily in measures to increase resilience beyond the legal minimums. It is therefore necessary for the new law to require the active participation of critical operators in the process, so that it is formally aligned with the operational reality of each sector.

8.2. STRENGTHENING INDUSTRIAL CYBERSECURITY

The convergence of IT and OT in critical environments requires ongoing investment in industrial cybersecurity that goes beyond minimum regulatory compliance. It is recommended that a National Industrial Cybersecurity Plan be implemented to set out specific standards for critical operators' SCADA/ICS systems, promote the certification of industrial components in accordance with Regulation (EU) 2019/881, and support the upgrading of legacy systems with known vulnerabilities. The CCN-CERT should further enhance its capacity to support operators in the critical private sector with industrial cybersecurity by establishing specialised sectoral teams (prioritising energy, transport and water) that can provide specific technical support in the event of hybrid physical-cyber incidents.

8.3. IMPROVING PUBLIC-PRIVATE COORDINATION

The creation of sector-specific platforms for the exchange of threat intelligence, in line with the model of the US Information Sharing and Analysis Centres (ISACs), is a priority for improving cooperation between the public sector and private operators. These platforms, which should operate under the umbrella of the CNPIC and with the participation of the CCN-CERT and CITCO, would enable a two-way flow of information on threats, vulnerabilities and incidents, thereby strengthening the response capacity of the entire system.

An essential condition for their effectiveness is the adoption of a legal framework that guarantees the confidentiality of information shared by private operators, eliminating the risk that its disclosure might give rise to legal liabilities or confer competitive advantages on their competitors.

8.4. TRAINING AND SIMULATION EXERCISES

The resilience of critical infrastructure to terrorist attacks depends largely on the preparedness of the staff who manage and protect it. It is recommended that a national training programme on critical infrastructure protection be institutionalised, with specific modules for operators in different sectors, and that annual crisis simulation exercises be carried out, covering scenarios involving combined physical and cyber attacks. These exercises, which should simultaneously involve the relevant authorities, security forces and critical operators, enable the identification of gaps in response plans, strengthen coordination between stakeholders and keep organisations' security culture up to date. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki is a key partner in the design and implementation of these exercises at the transnational level.

8.5. FORESIGHT INTELLIGENCE

Anticipating terrorist threats against critical infrastructure requires strengthening the strategic intelligence capabilities of CITCO and the CNI, with particular attention to analysing trends in the operational aspirations of terrorist groups and hostile state actors targeting infrastructure. The integration of open-source data, including the systematic monitoring of extremist forums on the dark web and the analysis of publications by terrorist organisations, should be systematised as part of the specific threat assessment for each strategic sector.

The development of artificial intelligence capabilities applied to the analysis of threats against critical infrastructure represents a promising area for investment, although its implementation must be accompanied by adequate legal safeguards to protect fundamental rights.

9. CONCLUSIONS

The analysis presented in this document allows us to draw the following conclusions regarding the terrorist threat facing Spain's critical infrastructure and the current state of the protection system.

Firstly, Spain has a regulatory and institutional framework for the protection of critical infrastructure, which, taken together, provides an adequate level of protection by European standards. Law 8/2011 and its implementing regulations form the cornerstone of a coherent system that has, for more than ten years, demonstrated its effectiveness in inter-institutional coordination and incident management. However, the delay in transposing the 2022 CER Directive has created a regulatory vacuum that undermines Spain's position within the European critical infrastructure protection system and must be urgently resolved through new legislation that incorporates the comprehensive resilience approach characteristic of the new European framework.

Secondly, jihadist terrorism remains the main terrorist threat to Spain's critical infrastructure in terms of probability of occurrence, as evidenced by the persistence of active cells within Spain and the continued dissemination of propaganda promoting attacks against infrastructure targets across Europe. The ENCOT 2023 report concurs with this assessment, highlighting the rise in lone actors who, following processes of self-radicalisation in digital environments, carry out attacks using rudimentary yet highly lethal means — a pattern illustrated by the attacks on Las Ramblas and in Cambrils — which poses a major challenge for early-warning systems. However, the threat posed by hostile state actors — particularly Russia — and attacks inspired by extremists of various ideological persuasions must be addressed with comparable strategic efforts, given their potential to cause catastrophic damage to critical infrastructure.

Thirdly, digitalisation and IT-OT convergence have transformed the landscape of vulnerabilities for Spain's critical infrastructure and created new attack vectors that existing protection systems cannot always neutralise effectively. Strengthening industrial cybersecurity must be considered a top national priority, which can only be achieved through sustained investment in technology, specialised training and the updating of regulatory frameworks and technical standards.

Fourthly, public-private coordination, although it has evolved considerably since the adoption of Law 8/2011, remains a critical area for improvement within the Spanish system. Privately-owned critical infrastructure assets require more sophisticated mechanisms to align incentives and exchange classified information between the public sector and operators; these can only be developed on the basis of a legal framework that guarantees the trust and confidentiality of all parties.

Fifthly, international cooperation – not only within the EU framework, but also within NATO and other multilateral forums – is a key factor in the effectiveness of Spain's critical infrastructure protection system. Spain's location as a gateway between Europe and North Africa should translate into a unique role within the European security architecture and, consequently, a specific commitment to existing multilateral cooperation mechanisms and the development of its own capabilities to provide added value to the entire system.

Future research in this area should focus on sector-specific vulnerability analyses using quantitative risk assessment methodologies; a comparative study of the models for transposing the CIP Directive adopted by the main Member States of the European Union; and an empirical evaluation of the effectiveness of existing public-private coordination mechanisms through primary research methodologies involving critical operators.

10. REFERENCES

Arteaga, F. (2023). Critical infrastructure and national security in Spain. *Elcano Royal Institute*. https://www.realinstitutoelcano.org

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

Ministry of National Security. (2021). *National Security Strategy*. Office of the Prime Minister of Spain.

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

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

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

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

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

Ministry of the Interior. (2023). *National Counter-Terrorism Strategy (ENCOT) 2023.* State Secretariat for Security. https://www.dsn.gob.es/es/publicaciones/estrategias-sectoriales/ENCOT2023

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

Reinares, F. (2014). Al-Qaeda and the 11 March attacks in Spain. *Revista de Occidente, 400,* 75–95.

Reinares, F. and García-Calvo, C. (2022). *Jihadist terrorism in Spain: Characteristics and trends.* Elcano Royal Institute. https://www.realinstitutoelcano.org

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

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

11. LEGISLATION

United Nations. Resolution 1373 (2001), 28 September. United Nations Security Council. S/RES/1373 (2001).

Council of Europe. Convention on the Prevention of Terrorism (CETS No. 196). Warsaw, 16 May 2005. In force since 1 June 2007.

European Union. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures. *Official Journal of the European Union*, L 345, 23 December 2008.

Spain. Act 8/2011 of 28 April, establishing measures for the protection of critical infrastructure. *Official State Gazette*, No. 102, 29 April 2011.

Spain. Royal Decree 704/2011 of 20 May, approving the Regulations on the protection of critical infrastructure. *Official State Gazette*, No. 121, 21 May 2011.

Spain. Organic Law 4/2015, of 30 March, on the Protection of Public Safety. *Official State Gazette*, No. 77, of 31 March 2015.

United Nations. Resolution 2341 (2017), of 13 February. United Nations Security Council. S/RES/2341 (2017).

Spain. Royal Decree 1150/2021, of 28 December, approving the National Security Strategy. *Official State Gazette*, No. 311, of 29 December 2021.

Spain. Royal Decree 311/2022, of 3 May, regulating the National Security Framework. *Official State Gazette*, No. 105, of 4 May 2022.

European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, L 333, 27 December 2022.

European Union. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive). *Official Journal of the European Union*, L 333, 27 December 2022.

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