ieee.es
Instituto Español de Estudios Estratégicos

Opinion Paper

120/2026 20/11/2026

Luis Jiménez Ortega

From a Sectoral Response to the Functional Integration of Capabilities to Address Hybrid Threats



From a Sectoral Response to the Functional Integration of Capabilities to Address Hybrid Threats

Abstract:

Changes in the strategic environment have increased the complexity of threats, contributing to the emergence of hybrid risks that may involve technological, economic and legal manipulation, the mobilisation of diverse actors in pursuit of different interests, and the threat or use of forms of violence that are not necessarily conventional. This reality calls into question the adequacy of traditional sectoral approaches and poses new challenges for national security models. This article analyses the implications of hybrid threats for the Spanish security model from a legal-strategic perspective, examining the current legal framework, specialised doctrine, and the main national and international strategic documents. The analysis concludes that the Spanish legal system provides a solid basis for addressing these threats, while recognising the need to further improve mechanisms for coordination and the functional integration of capabilities. The main challenge lies not in redefining the constitutional distribution of responsibilities, but in improving the integration of existing capabilities and enhancing their interoperability.

Keywords:

Hybrid threats; National Security; internal security; national defence; resilience.

How to quote:

JIMÉNEZ ORTEGA, Luis. De la respuesta sectorial a la integración funcional de capacidades frente a amenazas híbridas. Opinion Paper IEEE 120/2026.

NOTE:** The views expressed in ***Opinion Papers are the responsibility of their authors and do not necessarily reflect the views of the IEEE or the Ministry of Defence.

Introduction

Over the past two decades, changes in the strategic environment have profoundly altered the way States address security challenges. Growing economic and technological interdependence, the digitalisation of societies and intensified strategic competition have given rise to threats capable of producing simultaneous effects across multiple domains (land, maritime, air, cyberspace, space and cognitive[1]) and across a range of public and private sectors, including energy, ports, finance, transport and communications. Hybrid threats are particularly significant because they can combine conventional and unconventional techniques in a coordinated manner, gradually eroding the State's decision-making capacity without necessarily resorting to open armed conflict[2]. The main difficulty they pose for national security systems stems not only from the diversity of instruments involved, but also from the need to coordinate capabilities that fall under different areas of responsibility.

This new reality calls into question the adequacy of a sectoral approach to defence and security. However, this convergence does not necessarily entail expanding the powers constitutionally assigned to the Spanish Armed Forces[3] or diluting the democratic principles underpinning civilian control over the use of force[4]. On the contrary, it calls for stronger mechanisms to organise integrated responses under common direction, within a comprehensive governance model based on inter-institutional coordination (the Whole-of-Government approach)[5]. The challenge therefore lies in the State's ability to orchestrate existing capabilities, particularly when a situation requires information

[1] La doctrina española (PDC-01(B) (2025)) contempla el dominio cognitivo, mientras que la AJP-01(F) (2022) de la OTAN no lo reconoce como tal, sino como una dimensión, junto con las dimensiones física y virtual, sobre las que pueden producirse efectos.

[2] *HOFFMAN, Frank G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007.* https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

[3] MÁRQUEZ DE LA RUBIA, Francisco. «Las estrategias de seguridad nacional y defensa en Iberoamérica en el siglo XXI». En: CESEDEN. *Cuaderno de Estrategia 231: Los nuevos retos de seguridad y defensa en Iberoamérica ante los cambios globales*, cap. 5, 2025, pp. 133-173. https://www.defensa.gob.es/ceseden/-/cuaderno-de-estrategia-231

[4] HUNTINGTON, Samuel P. (1957). *The Soldier and the State: The Theory and Politics of Civil-Military Relations*. Cambridge (MA): Belknap Press of Harvard University Press. https://books.google.com/books?id=1PqFe0rsfdcC

[5] *DCAF. Gobernanza del sector de la seguridad: aplicación de los principios de buena gobernanza al sector de la seguridad. SSR Backgrounder nº 1.* https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_Gobernanza%20del%20Sector%20de%20Seguridad.pdf

sharing, the anticipation of developments, the activation of assets held by different organisations, and clear command and coordination arrangements.

The gradual expansion of the concept of security is a direct consequence of this transformation of the environment. Hybrid threats combine influence and disinformation campaigns, cyberattacks, sabotage, political, diplomatic and economic coercion, the use of proxy actors, the exploitation of social and institutional vulnerabilities, and the threat or use of military force[6]. They may also involve espionage and interference[7], lawfare, the instrumentalisation of migration flows, cumulative coercion and attacks on critical infrastructure[8]. They may also exploit transnational organised crime groups to facilitate drug trafficking, illicit firearms trafficking, human trafficking, migrant smuggling, fraud and other financial crimes, corruption and environmental offences, against a backdrop of growing convergence between organised crime and terrorism[9].

The cross-cutting nature of these threats exceeds the capacity of public bodies acting in isolation and requires sustained interaction between civilian, military, police and intelligence capabilities. In this context, State effectiveness depends increasingly on the ability of institutions to work together rather than in isolation, coordinating their efforts across the branches of the State (legislative, judicial and executive) and integrating the Instruments of National Power (diplomacy, information, military power and the economy, together with society)[10]. This trend explains the gradual consolidation of comprehensive governance approaches by the North Atlantic Treaty Organization (NATO)[11], the

[6] GIANNOPOULOS, Georgios; SMITH, Hanna; THEOCHARIDOU, Marianthi (eds.). *The Landscape of Hybrid Threats: A Conceptual Model*. Hybrid CoE, 2021. https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/

[7] ESPAÑA. DEPARTAMENTO DE SEGURIDAD NACIONAL. *Informe Anual de Seguridad Nacional 2025*. Presidencia del Gobierno, 2026. https://www.dsn.gob.es/es/publicaciones/informes-anuales

[8] COLOM PIELLA, Guillem. *Desdibujar el umbral: zona gris, atribución y coerción acumulativa*. Documento de Opinión IEEE 47/2026. https://www.defensa.gob.es/ceseden/-/ieee-2026-zona-gris-opinion47

[9] EUROPOL. *European Union Serious and Organised Crime Threat Assessment – SOCTA 2025*. https://www.europol.europa.eu/publications-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2025

[10] ESPAÑA. Estado Mayor de la Defensa, PDC-01(B). Doctrina para el Empleo de las FAS (EMAD, 2025).

[11] OTAN, *Strategic Concept 2022.* https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept

European Union (EU)[12] and Spain's National Security Strategy (Estrategia de Seguridad Nacional, ESN)[13], all aimed at strengthening State resilience to complex threats. Resilience should not be understood solely as the ability to respond to and recover from a crisis, but also as the ability to anticipate it, adapt to its evolution and ensure the continuity of the essential functions of the State and society. It therefore extends beyond the strictly operational sphere and becomes a structural element of governance within a single response system[14].

Spain is a particularly relevant case for analysing this issue. Its security model is based on a clear functional distinction between national defence and internal security, established by the Constitution during Spain's democratic transition and subsequently developed through sectoral legislation. This process culminated in the establishment of the National Security System under Law 36/2015, with its strategic direction subsequently set out in the 2021 National Security Strategy. In April 2026, the National Security Council agreed to review the Strategy[15]. The system is assessed through the Annual National Security Report (Informe Annual de Seguridad Nacional, IASN), which examines developments in risks and threats and the main measures taken to address them. The National Security Council is therefore central to the governance framework for coordinating the responses of the various State administrations and institutions to complex threats, supported by the Department of National Security and a flexible network of specialised committees covering specific areas.

However, inter-institutional synchronisation must account for the simultaneous occurrence of risks of very different kinds. In this regard, the national civil protection system provides a multi-hazard framework for responding to events such as wildfires and

[12] UNIÓN EUROPEA. *A Strategic Compass for Security and Defence*. 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade

[13] *ESPAÑA. Estrategia de Seguridad Nacional 2021. Presidencia del Gobierno, 2021. https://www.boe.es/buscar/pdf/2021/BOE-A-2021-21884-consolidado.pdf*

[14] DCAF – CENTRO DE GINEBRA PARA LA GOBERNANZA DEL SECTOR DE SEGURIDAD. *El sector de seguridad*. Serie de Documentos Informativos de la RSS (SSR Backgrounder n.º 3). Ginebra: DCAF, 2015. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_3_El%20Sector%20de%20Seguridad.pdf

[15] ESPAÑA. Departamento de Seguridad Nacional. *Informe Anual de Seguridad Nacional 2025*. Presidencia del Gobierno, 2026, p. 14. https://www.dsn.gob.es/sites/default/files/2026-05/Informe%20Anual%20de%20Seguridad%20Nacional%202025%20-%20Accesible_2.pdf

floods, as well as seismic and volcanic hazards, integrating available capabilities effectively[16]. The summer of 2026 has once again tested the mobilisation and coordination of State capabilities amid a period of intense wildfire activity. This coincided with the migration crisis recorded in Ceuta in late July, when assets from the Armed Forces and Spain's State Security Forces and Corps (hereafter, law-enforcement agencies) were deployed[17]. This situation highlights the need to improve governance, information exchange and operational cooperation, particularly when the simultaneous occurrence of risks may generate cascading effects on National Security. In line with the 2025 IASN, it is necessary to strengthen anticipatory capabilities, prevention, resilience and coordinated response, as well as effective early-warning mechanisms[18].

For instance, one could envisage a scenario in which a major emergency, such as a wildfire suspected to have been deliberately started, coincides with increased irregular maritime migration, while non-State actors seek to exploit the situation for illicit purposes.

Against this background, this article argues that the main challenge does not lie in redefining the powers constitutionally assigned to the Armed Forces, the law enforcement agencies, or other competent bodies. Rather, it lies in determining the extent to which the Spanish model has effective mechanisms for coordinating existing capabilities in response to threats that transcend traditional defence and security boundaries. The study therefore focuses on threats deliberately generated by State and non-State actors, including proxies, terrorist groups, criminal organisations, and mercenaries. It focuses on four particularly relevant aspects: information exchange, threat anticipation, capability activation, and inter-organisational command and coordination mechanisms. Any potential redistribution of powers falls outside the scope of the study.

[16] ESPAÑA. Resolución de 16 de diciembre de 2020, por la que se publica el Acuerdo del Consejo de Ministros de 15 de diciembre de 2020, por el que se aprueba el Plan Estatal General de Emergencias de Protección Civil. *BOE*, núm. 328, de 17 de diciembre de 2020. https://www.boe.es/eli/es/res/2020/12/16/(1)/con

[17] RTVE. «Inmigrantes en Ceuta: resumen de la crisis el 31 de julio». 2026. https://www.rtve.es/noticias/20260731/crisis-inmigrantes-ceuta-hoy-ultima-hora-resumen/17175111.shtml

[18] JORDÁN, Javier. «Sorpresas estratégicas e Inteligencia de alerta temprana». *Global Strategy Reports*, n.º 56, 2020. Sorpresas estratégicas e Inteligencia de alerta temprana – Global Strategy | Geopolítica y Estudios Estratégicos

Hybrid threats and the erosion of functional boundaries

The profound changes in the international strategic environment over recent decades have significantly altered the context in which States develop their defence and security policies. Accelerating globalisation, the technological revolution, digital transformation, growing economic interdependence and the emergence of new non-State actors capable of influencing State stability have created a highly complex and uncertain environment in which risks rarely occur in isolation. In this context, security, both external and internal, is increasingly understood as the outcome of interaction among interdependent functional areas, rather than simply the sum of independent sectoral capabilities. According to Spanish doctrine, responding to complex threats requires the coherent integration and synchronisation of the capabilities associated with the Instruments of National Power[19], moving beyond traditional sectoral approaches, particularly when threats develop and produce simultaneous effects across several domains and affect multiple sectors and areas of State activity (defence, foreign affairs, internal security, civil protection, etc.). Capabilities may also be employed flexibly across different areas of State activity, including for tasks for which they were not originally designed, while maintaining appropriate coordination and operational direction. This can improve the overall efficiency of State action. The question is no longer simply what capability each institution possesses, but whether the system can identify in time the need to use it, share the necessary information and activate it under common operational direction.

The evolution of Western strategic thinking has consolidated this comprehensive vision of security. Both NATO and the EU have progressively incorporated the strengthening of national resilience, the protection of critical infrastructure, cognitive protection against disinformation and influence campaigns, and coordination between civilian and military instruments as essential elements in addressing complex threats. In Spain, the 2021 National Security Strategy explicitly reflects this cross-cutting and interdependent approach[20], identifying the interdependence of risks as one of the main challenges for

[19] Estado Mayor de la Defensa, PDC-01(B). Doctrina para el Empleo de las FAS (EMAD, 2025).
[20] JORDÁN, Javier. «Competición entre grandes potencias y militarización del espacio exterior». *Revista del IEEE*, 2023. https://dialnet.unirioja.es/descarga/articulo/9049318.pdf

State action and highlighting the need to integrate capabilities belonging to different public and private organisations under a common strategic direction[21].

This evolution is also evident in recent cases. Russia's invasion of Ukraine has shown how military operations can be accompanied by cyberattacks[22], disinformation campaigns, economic pressure, energy coercion and diplomatic initiatives conducted simultaneously. Similarly, the sabotage of the Nord Stream pipelines in 2022 and the damage to the Balticconnector pipeline and several submarine cables in the Baltic Sea between 2023 and 2024 highlighted the vulnerability of critical infrastructure and the need to strengthen international cooperation for its protection[23]. Beyond the specific circumstances of each incident, these cases illustrate how seemingly limited actions can produce political, economic and security effects far greater than the initial material damage, simultaneously engaging the responsibilities of multiple civilian and military bodies. This dynamic confirms that contemporary strategic competition is no longer conducted solely through the direct use of military force, but through a synchronised combination of instruments and techniques capable of generating synergies and cumulative strategic effects.

In line with the above, the protection of critical infrastructure, including maritime and submarine infrastructure[24], is becoming increasingly important as a field requiring cooperation between national defence and internal security authorities, strategic operators and joint international action[25], as noted in the 2025 IASN.

The value of the concept of hybrid threats extends beyond describing phenomena associated with confrontation between actors; it makes it possible to analyse risks that

[21] ESPAÑA. *Estrategia de Seguridad Nacional 2021*. Presidencia del Gobierno, 2021. https://www.boe.es/buscar/pdf/2021/BOE-A-2021-21884-consolidado.pdf

[22] CCN-CERT. *Informe de ciberamenazas y tendencias 2024*. https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html

[23] OTAN. *Protecting Critical Undersea Infrastructure*. https://www.nato.int/cps/en/natohq/topics_213172.htm; NORTH ATLANTIC TREATY ORGANIZATION. *Resilience, Civil Preparedness and Article 3*. 2024. https://www.nato.int/cps/en/natohq/topics_132722.htm

[24] RODRÍGUEZ DAPENA, Álvaro. «La importancia del sistema portuario de interés general para la defensa nacional». En: CESEDEN. *Cuaderno de Estrategia 234: Puertos del Estado y la defensa nacional*, cap. preliminar, 2026, pp. 18-36. https://www.defensa.gob.es/documents/2073105/3688535/CE_234_CapPreliminar.pdf/a6736536-3543-bf3f-992c-01cf9985e98f?t=1773916224323

[25] ESPAÑA. Orden PJC/501/2024, de 27 de mayo, por la que se publica la Estrategia Nacional de Seguridad Marítima 2024. *BOE*, núm. 130, de 29 de mayo de 2024. https://www.boe.es/eli/es/o/2024/05/27/pjc501

are common in the security field. International terrorism, transnational organised crime, cybercrime[26], disinformation campaigns and actions targeting critical infrastructure follow different dynamics but share an essential feature: they can all occur simultaneously across different strategic sectors, reinforcing one another and generating cumulative effects. This requires stronger integration mechanisms to coordinate capabilities across institutional boundaries[27], supported by public policies that adopt an integrated approach and modernize the State's capacity to address transnational threats—not only State actors and terrorism, but also transnational organised crime[28].

Spain's position on the EU's external border, its proximity to North Africa and the Sahel, the strategic importance of the Strait of Gibraltar, the extent of its maritime areas, and the presence of critical energy, port, airport and digital infrastructure create an environment in which hybrid threats and transnational risks may converge in the same physical and functional space. Protecting these assets generally requires coordinated action by the law-enforcement agencies, the Armed Forces, intelligence bodies, public administrations, private operators and civil society. Their cooperation involves sharing information and integrating their respective capabilities to support informed decision-making[29]. The 2025 IASN reinforces this assessment in the maritime domain, noting the growing exposure of ports, energy terminals, submarine cables and interconnectors to physical, operational and geopolitical risks, as well as the need to strengthen coordination between public administrations, together with early-warning and coordinated-response capabilities.

[26] CENTRO DE INTELIGENCIA CONTRA EL TERRORISMO Y EL CRIMEN ORGANIZADO (CITCO). *Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2025*. Ministerio del Interior, 2025. https://citco.interior.gob.es/publico/citco/dam/jcr:28e01cc6-e266-4082-9cf6-7703217a44f4/Estrategia%20Nacional%20contra%20el%20CO%20y%20la%20DG%202025.pdf

[27] ARTEAGA, Félix; ALONSO LECUIT, Javier. «La ciberresiliencia: entre la ciberseguridad y la resiliencia». *ARI 80/2024*. Real Instituto Elcano, 2024. https://www.realinstitutoelcano.org/analisis/la-ciberresiliencia-entre-la-ciberseguridad-y-la-resiliencia/

[28] SANCHO HIRANE, Carolina. «Construyendo una política latinoamericana contra la delincuencia organizada transnacional (DOT)». En: CESEDEN. *Cuaderno de Estrategia 231: Los nuevos retos de seguridad y defensa en Iberoamérica ante los cambios globales*. Madrid: IEEE-CESEDEN, 2025, pp. 87-112. https://www.defensa.gob.es/documents/2073105/2557568/CE_231_Cap03.pdf/3402037a-99b0-c04b-0014-3d21920455c5?t=1753172368341

[29] NIETO FERNÁNDEZ, Ignacio. «Información e inteligencia, condenados a entenderse». Documento de Opinión IEEE 107/2024, Instituto Español de Estudios Estratégicos, 2024, pp. 437-452. https://www.defensa.gob.es/ceseden/-/informacion_e_inteligencia_condenados_a_entenderse

Experience nevertheless shows that information exchange between organisations may be constrained by classification, the relevant access authorisations and the 'need-to-know' principle. This may limit the availability and circulation of information and make timely, complete sharing more difficult. The integration of the intelligence function must also be considered, given its role in the anticipation and decision-making[30]. These constraints can hinder coordination between ministries and public administrations, and even within a single ministry[31]. The challenge is therefore not merely to hold information in particular areas and agencies, but to transform it in a timely manner into knowledge that can inform State decisions and action.

From this perspective, the multi-domain concept goes beyond its strictly military application and becomes a useful tool for analysing the contemporary strategic environment. It helps explain how contemporary threats can produce simultaneous effects across different domains, organisations and actors[32], thereby increasing the need for capability integration. This is consistent with the gradual consolidation of national strategies based on a broader, multidimensional concept of security, characterised by constant interaction between threats, capabilities and institutions[33].

Consequently, analysing hybrid threats requires moving beyond sectoral approaches and adopting a comprehensive perspective that takes account of legislative, legal, diplomatic, informational, military, economic, police and social dimensions. An effective response depends not only on the availability of sufficient resources, but also on effective information-sharing arrangements, clear activation procedures, well-defined decision-making mechanisms, and effective operational execution and direction.

[30] SIMÓN SERNA, Ricardo. «Integración de la inteligencia en el Sistema de Seguridad Nacional». CESEDEN, 2025. https://www.defensa.gob.es/ceseden/-/integracion-inteligencia-en-sistema-seguridad-nacional

[31] OECD. Greece: Review of the Central Administration. OECD Public Governance Reviews. Paris: OECD Publishing, 2011. https://doi.org/10.1787/9789264102880-en

[32] NORTH ATLANTIC TREATY ORGANIZATION. *Allied Joint Doctrine AJP-01(F)* 2022. https://nso.nato.int/nso/nsdd/main/standards/ap-details/3081/EN?u=

[33] MÁRQUEZ DE LA RUBIA, Francisco. «Las estrategias de seguridad nacional y defensa en Iberoamérica en el siglo XXI». En: CESEDEN. *Cuaderno de Estrategia 231: Los nuevos retos de seguridad y defensa en Iberoamérica ante los cambios globales*, cap. 5, 2025, pp. 133-173. https://www.defensa.gob.es/ceseden/-/cuaderno-de-estrategia-231

The Spanish model and the convergence of defence and security

The evolution of the strategic environment described above does not in itself call into question the institutional architecture underpinning Spain's security model. This model continues to rest on a fully valid functional distribution of responsibilities: Article 8 of the Constitution assigns the Armed Forces the mission of safeguarding Spain's sovereignty and independence, defending its territorial integrity and constitutional order, while Article 104[34] entrusts the State Security Forces and Corps with protecting the free exercise of rights and freedoms and ensuring public security[35]. Rather than establishing opposing spheres, these provisions reflect a logic of functional specialisation that is one of the pillars of the social and democratic rule of law, providing legal certainty, clarity of responsibilities and civilian control over the use of force. The increasing complexity of the strategic environment does not undermine this architecture; instead, it highlights the need to interpret the model in functional terms, thereby facilitating coordinated action by institutions employing distinct capabilities to address complex and interdependent threats[36].

This approach is carried forward in subsequent legislation. The National Defence Act[37] and Organic Law 2/1986 on the State Security Forces and Corps define each institution's responsibilities precisely, consolidating a model based on functional specialisation. However, the gradual emergence of threats affecting several strategic sectors simultaneously prompted the system to evolve, culminating in the adoption of Law 36/2015 on National Security. This law introduces an integrated concept of security by establishing the National Security System as a permanent coordination instrument capable of synchronising the capabilities of different administrations and bodies without altering the constitutional distribution of powers. Security is thus conceived as a State policy which, without replacing sectoral policies, seeks to coordinate them through joint

[34] ESPAÑA. Constitución Española, de 29 de diciembre de 1978, arts. 8 y 104. https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

[35] ESPAÑA. Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. https://www.boe.es/buscar/act.php?id=BOE-A-1986-6859

[36] BALLESTEROS MARTÍN, Miguel Ángel. En busca de una Estrategia de Seguridad Nacional. Madrid: Ministerio de Defensa, 2016. https://www.defensa.gob.es/ceseden/-/participacion-fas-seguridad-publica-en-espanna

[37] ESPAÑA. Ley Orgánica 5/2005, de la Defensa Nacional. https://www.boe.es/buscar/act.php?id=BOE-A-2005-18933

planning, continuous information exchange, ongoing risk assessment and common strategic direction[38]. In practice, the challenge is to ensure that these mechanisms turn available information into anticipation, anticipation into decisions, and decisions into effective and efficient integrated action.

The protection of critical infrastructure is one of the clearest examples of this evolution, particularly with regard to integration, anticipation, resilience and ongoing coordination among the actors involved[39]. Law 8/2011 establishes a system based on permanent cooperation between public administrations, the law-enforcement agencies, strategic operators and other competent bodies to ensure the continuity of essential services[40]. The experience documented in the 2025 IASN confirms the importance of this cooperation, highlighting the strengthening of coordination between the National Centre for the Protection of Critical Infrastructure, the law-enforcement agencies, and the Ministry of Defence in the areas of information exchange, risk analysis and contingency-plan updates. This area clearly shows that the effectiveness of the system depends not only on the availability of distinct capabilities, but also on the ability to share information and translate it into coordinated decisions and action.

Nevertheless, recent episodes, as well as the waves of irregular migration affecting Andalusia in 2018 and the Canary Islands in 2006, illustrate the difficulties involved in anticipating developments and activating planned measures. These situations prompted ad hoc responses tailored to the circumstances of each case and subsequently led to the establishment of coordination bodies, including the Strait Coordination Centre (CCOE, from its Spanish name), established in 2018, and the Canary Islands Regional Coordination Centre (CCRC, from its Spanish name), created in 2006 in response to the

[38] *ESPAÑA. Estrategia de Seguridad Nacional 2021. Presidencia del Gobierno, 2021.* *https://www.boe.es/buscar/pdf/2021/BOE-A-2021-21884-consolidado.pdf*

[39] GONZÁLEZ-CANCELAS, Nicoletta. «La gobernanza portuaria. Un elemento clave de la defensa nacional». En: CESEDEN. *Cuaderno de Estrategia 234: Puertos del Estado y la defensa nacional*, cap. 2, 2026, pp. 67-89. https://www.defensa.gob.es/documents/2073105/3688535/CE_234_Cap02.pdf/dca403af-1187-9a7d-a99c-43419709def5?t=1773916213786

[40] *ESPAÑA. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. BOE, núm. 102, de 29 de abril de 2011. Texto consolidado.* *https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630*

initial waves of irregular migration in the respective territories. These episodes illustrate the challenges of translating available capabilities into a coordinated and timely response.

Along the same lines, Law 5/2014 incorporates private security as a complementary element of public security[41], particularly in areas such as energy facilities, ports, airports, transport networks and communications infrastructure. Rather than privatising security, this model strengthens the State's preventive capacity by adding capabilities for early risk detection, surveillance and cooperation with the competent authorities. Convergence between public administrations at different levels, strategic operators and the private sector is therefore a practical expression of the governance model promoted by the National Security System and strengthens the response to hybrid threats.

Spanish operational experience shows that functional convergence between defence and security can be achieved without changing the constitutional distribution of powers when each institution contributes the capabilities for which it was specifically designed, acting in coordination within the existing legal framework[42]. The Navy's participation in *Operation Atalanta* is a representative example. In this operation, the Armed Forces employ highly specialised capabilities in maritime surveillance, intelligence gathering, command and control, naval projection, and special operations against piracy, including hostage rescue and the apprehension of suspected offenders, thereby helping to protect one of the main maritime routes for international trade[43]. Similarly, combating illicit trafficking by sea in waters under national sovereignty shows how cooperation between the Armed Forces, the law-enforcement agencies and the Customs Surveillance Service can integrate complementary capabilities in a single operational effort[44]. While police

[41] ESPAÑA. Ley 5/2014, de 4 de abril, de Seguridad Privada. *BOE*, núm. 83, de 5 de abril de 2014, pp. 28975-29024. https://www.boe.es/eli/es/l/2014/04/04/5/con

[42] PLANCHUELO CASTIÑEIRA, Juan Miguel. (2025). Análisis del impacto de una mayor participación de las Fuerzas Armadas en la seguridad pública en España. CESEDEN, 2025. *https://www.defensa.gob.es/ceseden/-/participacion-fas-seguridad-publica-en-espanna*

[43] MINISTERIO DE DEFENSA. «Operación Atalanta: la fragata "Victoria" y su equipo de operaciones especiales liberan a la tripulación de un barco asaltado por piratas». 2025 https://emad.defensa.gob.es/operaciones/operaciones-en-el-exterior/42-ATALANTA/Noticias/listado/251111-ni-atalanta-buque-liberado.html; *La fragata «Reina Sofía» apresa un «dhow» con 16 presuntos piratas a bordo:* https://www.defensa.gob.es/gabinete/notasPrensa/2012/04/DGC-120416-atalanta-detencion-piratas.html

[44] MINISTERIO DEL INTERIOR. «Grande-Marlaska presenta dos operaciones antidroga que marcan un "contundente y decisivo avance estratégico" en la lucha contra el crimen organizado transnacional». 8 de mayo de 2026. https://www.interior.gob.es/opencms/ca/detalle/articulo/Grande-Marlaska-presenta-dos-operaciones-antidroga-

authorities carry out judicial investigations and policing functions assigned to them by law, the Armed Forces provide air and naval platforms, surveillance systems, projection assets, command-and-control capabilities and highly specialised units that increase the effectiveness of the overall operation.

However, bringing different capabilities together in a single operational effort under the direction of the competent authority requires interministerial agreements and specific inter-agency protocols. Responsibility for activating or authorising these capabilities rests with senior authorities. This may cause delays and introduce additional decision points across different chains of command, potentially constraining their timely deployment or freedom of action. One example is the procedure governing the deployment of the Military Emergency Unit, which provides for the sequential involvement of civil protection authorities, the Ministry of the Interior and the Ministry of Defence in requesting, assessing and authorising its deployment[45]. This procedure shows that the availability of a capability does not in itself guarantee its immediate activation, which depends on the established decision-making and coordination mechanisms.

Other Western models offer different solutions for integrating military capabilities in support of security. France allows the Armed Forces to support internal security through arrangements such as *Operation Sentinelle*, under civilian coordination , while its *Code de la défense* providesthe legal framework for deploying military forces on national territory[46]. Italy maintains *Operation Strade Sicure*, launched in 2008 and based on Law No. 125/2008, under which military personnel guard sensitive sites and targets and conduct joint patrols with police forces[47]. Portugal provides for cooperation between the Armed Forces and civilian authorities in security matters, including the maritime domain,

que-marcan-un-contundente-y-decisivo-avance-estrategico-en-la-lucha-contra-el-crimen-organizado-transnacional/

[45] ESPAÑA. Real Decreto 1097/2011, de 22 de julio, por el que se aprueba el Protocolo de Intervención de la Unidad Militar de Emergencias. Boletín Oficial del Estado, núm. 178, de 26 de julio de 2011. https://www.boe.es/eli/es/rd/2011/07/22/1097

[46] MINISTÈRE DES ARMÉES. «Opération Sentinelle: engagement des armées pour sécuriser la Fête des Lumières à Lyon». 2025. https://www.defense.gouv.fr/operations/actualites/operation-sentinelle-engagement-armees-securiser-fete-lumieres-lyon; FRANCE, Code de la défense, arts. L1321-1 y ss., https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006151474

[47] ESERCITO ITALIANO. «Operazione Strade Sicure». https://www.esercito.difesa.it/operazioni/operazioni-nazionali/operazione-strade-sicure/93922.html; ITALIA. Ministero della Difesa, «Operazione Strade Sicure», https://www.difesa.it/operazionimilitari/nazionaliincorso/stradesicure/index.html

under the *Lei de Segurança Interna* and the *Lei de Defesa Nacional*[48]. The United Kingdom uses the *Military Aid to the Civil Authorities* (MACA) system, through which the Armed Forces may support civilian authorities when a specific need has been identified and the tasks are clearly defined, subject to ministerial approval[49]. The application of this approach was demonstrated by *Operation Temperer*, activated in May 2017 following the Manchester attack to reinforce the protection of sensitive sites and release armed police officers for other duties[50]. The United States, for its part, maintains a generally restrictive framework under the *Posse Comitatus Act*[51], alongside statutory exceptions to the use of military capabilities. In this context, on 27 October 2025, U.S. forces attacked four vessels suspected of carrying drugs in the eastern Pacific[52]. These models show that the functional integration of military and civilian capabilities can take different forms without necessarily changing the distribution of powers.

Despite the differences between these systems, it is particularly important to establish procedures and plans in advance, together with rules of engagement where appropriate, to define the response to specific scenarios. Once the anticipated situation arises, the relevant capabilities can then be activated and operate according to a predefined sequence of actions and responses, without requiring a separate ad hoc decision by the competent authority for every planned action.

The analysis shows that the principal added value of the National Security System lies not in creating new powers, but in providing an institutional architecture capable of integrating existing capabilities through stable cooperation and governance mechanisms designed to strengthen resilience.

PORTUGAL. Lei n.º 53/2008, de 29 de agosto, Lei de Segurança Interna. https://diariodarepublica.pt/dr/detalhe/lei/53-2008-453479; PORTUGAL. Lei Orgânica n.º 1-B/2009, de 7 de julho, Lei de Defesa Nacional. https://diariodarepublica.pt/dr/legislacao-consolidada/declaracao-rectificacao/2009-67356360

[49] UK MINISTRY OF DEFENCE. *UK Operations: the Defence Contribution to Resilience (JDP 02)*. https://www.gov.uk/government/publications/operations-in-the-uk-a-joint-doctrine-publication

[50] MACASKILL, Ewen. «Critical threat level: who made the decision and what does it mean?». The Guardian, 23 de mayo de 2017. https://www.theguardian.com/politics/2017/may/23/raise-terror-level-critical-5000-troops-streets-operation-temperer

[51] UNITED STATES CODE. 18 U.S.C. § 1385, Use of Army, Navy, Marine Corps, Air Force, and Space Force as posse comitatus (Posse Comitatus Act). https://uscode.house.gov/us/usc/119-120/t18/s1385/

[52] ASSOCIATED PRESS. (2025, 28 de octubre). «US launches strikes on 4 alleged drug-running boats in the eastern Pacific, killing 14». Associated Press. https://apnews.com/article/8f9f65dd67c0bc55b6dd70b109df0216

Conclusions

The evolution of the strategic environment does not require a change in the existing division of responsibilities between defence and internal security. Rather, it requires assessing whether existing capabilities can be integrated effectively when a threat exceeds the boundaries of a single area of activity. The analysis indicates that the main points of friction lie in turning compartmentalised information into shared knowledge, anticipating developments, activating capabilities in a timely manner, and coordinating responses among organisations with different decision-making chains.

The analysis of Spain's legal framework indicates that the current system provides sufficient instruments to coordinate responses to these challenges. Organic Law 5/2005 on National Defence and Law 36/2015 on National Security preserve the existing distribution of powers while providing mechanisms for cooperation and coordination when required by the nature of a threat. The main limitations stem not from a lack of legal instruments, but from difficulties in implementing them in practice, achieving interoperability between organisations, and establishing stable procedures for coordinated action, while avoiding parallel structures and unnecessary duplication.

Finally, this paper highlights the value of further comparative research into Western models for the functional integration of defence and security, as well as an evaluation of the governance mechanisms used by other States to address hybrid threats. Ultimately, the challenge is not necessarily to acquire more capabilities, but to use existing ones more effectively and efficiently. This requires a shared understanding of the responsibilities and capabilities of the different actors, stable cooperation procedures where necessary, and—where the nature of the threat permits—pre-planned mechanisms that enable an immediate response according to predetermined action–reaction sequences. Such mechanisms could reduce the need for separate ad hoc decisions in each situation, while remaining within the framework of established powers and authorisations. System effectiveness will depend to a large extent on the ability to anticipate threats, translate information into timely decisions, and activate and coordinate available capabilities swiftly. This requires moving beyond compartmentalised

approaches and promoting complementarity, so that the State's response remains proportionate to the threat and makes efficient use of public resources.

Luis Jiménez Ortega,
Lieutenant Colonel (CIM) DEM; D.S.P.