

02/2026

08/10/2026

Juan Carlos Fernández Cela and José
Fuentes García

Economic and financial intelligence in Spain's 2026 National Security Strategy: from risk awareness to a permanent state capability

Economic and financial intelligence in Spain's 2026 National Security Strategy: from risk awareness to a permanent state capability

Abstract:

The review of Spain's National Security Strategy offers Spain the opportunity to correct a discontinuity. Economic and financial risks have been recognised for years, yet they have still not been consolidated into a cross-cutting, stable and assessable capability within the National Security System. This article proposes the explicit incorporation of economic intelligence (EI) and financial intelligence (FININT) as distinct but analytically convergent functions. EI identifies dependencies, positions of control and vulnerabilities affecting supply chains, technology, investment, debt, infrastructure and contracts. It also supports the protection and projection of strategic economic interests. FININT reconstructs ownership, assets, intermediaries, payments, guarantees and financing circuits relevant to national security. Their integration would make it possible to develop a national picture of strategic exposure and strengthen anticipatory capacity. The article revisits Spain's earlier Economic Intelligence System and proposes its gradual development through a decentralised model combining political direction, common intelligence products, variable-geometry cooperation, secure communications, public-private collaboration and legal safeguards. The purpose is to strengthen the State's decision-making autonomy without turning all economic activity into a matter of national security.

Keywords:

National Security Strategy; economic intelligence; financial intelligence; FININT; economic security; economic coercion; strategic dependencies; critical infrastructure.

How to cite this document:

FERNÁNDEZ CELA, Juan Carlos and FUENTES GARCÍA, José. *Economic and financial intelligence in Spain's 2026 national security strategy: from risk awareness to a permanent state capability*. Framework paper. IEEE 02/2026.

***NOTE:** The ideas contained in the *Framework Papers* are the responsibility of their authors and do not necessarily reflect the views of the IEEE or the Ministry of Defense.

Introduction. An architectural gap

The forthcoming National Security Strategy (*Estrategia de Seguridad Nacional*, ESN) is being drafted in an environment in which security, the economy and technology form a single arena of competition. The procedure approved by the National Security Council on 24 April 2025 requires an analysis of the strategic environment, the specification of risks and threats, the definition of lines of action and the optimisation of existing resources. It also provides for the participation of all ministerial departments, the National Intelligence Centre, the autonomous communities and experts drawn from the public, private and scientific sectors¹.

The agreement does more than set out the procedure. Its recitals emphasise the reinforcement of deterrence and defence, the development of industrial capabilities, comprehensive crisis management, early warning and the secure integration of information. They also identify the economy and technology as vectors of geopolitical influence. This framework offers a concrete channel for incorporating economic intelligence and financial intelligence as distinct and convergent capabilities, rather than as a terminological addition to the catalogue of risks².

Spain also has a clear precedent. The 2011 Spanish Security Strategy proposed the development of an Economic Intelligence System (*Sistema de Inteligencia Económica*, SIE), in cooperation with the private sector, in order to obtain and analyse economic, financial and corporate information relevant to security. The 2013 ESN maintained that orientation. The 2017 and 2021 strategies broadened their treatment of economic security, investment, critical supply chains and technology, although the SIE formula lost continuity and no recognisable cross-cutting function was consolidated³. The present

1 Orden PJC/521/2025, de 23 de mayo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 24 de abril de 2025, por el que se aprueba el procedimiento para la elaboración de la nueva Estrategia de Seguridad Nacional [Order publishing the National Security Council Agreement of 24 April 2025 approving the procedure for drafting the new National Security Strategy]. Boletín Oficial del Estado (BOE) no. 126, 26 May 2025.

<https://www.boe.es/eli/es/o/2025/05/23/pjc521>

2 Orden PJC/521/2025, de 23 de mayo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 24 de abril de 2025, por el que se aprueba el procedimiento para la elaboración de la nueva Estrategia de Seguridad Nacional [Order publishing the National Security Council Agreement of 24 April 2025 approving the procedure for drafting the new National Security Strategy]. Boletín Oficial del Estado (BOE) no. 126, 26 May 2025.

<https://www.boe.es/eli/es/o/2025/05/23/pjc521>

3 Government of Spain, *Estrategia Española de Seguridad*. Una responsabilidad de todos (2011); *Estrategia de Seguridad Nacional* 2013; *Estrategia de Seguridad Nacional* 2017; *Estrategia de Seguridad Nacional* 2021.

<https://www.lamoncloa.gob.es/serviciosdeprensa/paginas/postit/EstrategiaEspanolaDeSeguridad.aspx>;

<https://www.dsn.gob.es/es/actualidad/sala-de-prensa/estrategia-seguridad-nacional-2021>. Instituto Español de Estudios Estratégicos (2016), *El sistema de inteligencia económica en España*, Working Paper DIEEEET07-2016.

<https://www.defensa.gob.es/ceseden/-/el-sistema-de-inteligencia-economica-en-espa%C3%B1a>

problem arises from that distance between the identification of risk and the organisation of a permanent capability.

This trajectory is relevant for a further reason. The 2011 reference did not envisage an isolated agency, but a system built together with the private sector and oriented towards improving the decisions of the State. That approach anticipated two features that are now central: decisive knowledge is distributed, and economic security requires continuity beyond any single crisis. The proposal lost institutional visibility, but the environment has evolved in ways that have made it increasingly necessary. Sanctions, competition over critical technologies, investment screening and supply-chain vulnerability have increased the number of public decisions that require an integrated assessment. The 2025 National Security Annual Report confirms the growing importance of economic, technological and supply-related risks⁴.

Discontinuity is not equivalent to an absence of capabilities. Spain has intelligence bodies, supervisory authorities, sectoral regulators, law enforcement agencies, investment screening and export control bodies, administrative registers and private operators that produce high-value information. Sepblac acts as Spain's Financial Intelligence Unit within the specific legal framework for the prevention of money laundering and terrorist financing⁵. Other bodies analyse competition, markets, investment, solvency, infrastructure, foreign trade, hybrid threats or technology protection. The weakness lies in the absence of a common product — at least at the unclassified level — capable of relating those partial representations when an economic exposure may affect national security.

This institutional map may change if the reform given first-round approval by the Council of Ministers on 28 July 2026 is completed. The draft bill would create the National Financial Integrity Authority (Autoridad Nacional de Integridad Financiera, ANIFI) as an independent administrative authority, base it on the existing structure of the Fund for Orderly Bank Restructuring (Fondo de Reestructuración Ordenada Bancaria, FROB) and bring together within it Financial Intelligence Unit, supervisory and inspection functions, sanctioning powers, international financial sanctions and the prevention of proliferation

4 Departamento de Seguridad Nacional, Informe Anual de Seguridad Nacional 2025 (2026) [National Security Annual Report 2025]. <https://www.dsn.gob.es/es/actualidad/sala-de-prensa/IASN2025>

5 Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo; Ley Orgánica 9/2022, de 28 de julio; Sepblac, Financial Intelligence Unit and organisational structure. <https://www.sepblac.es/es/sobre-el-sepblac/organizacion/estructura-organizativa/>

financing. It would also act as Spain's interlocutor with AMLA⁶. The proposal reinforces institutional specialisation, but it is not equivalent to the SIE advocated in this article. Its proposed remit is sectoral and legally circumscribed, whereas the ESN needs to relate financial exposures to industrial, technological, investment-related, contractual and territorial dependencies. Should it eventually be established, ANIFI could act as a specialised node within the system, without absorbing strategic coordination or blurring the separation between financial intelligence, supervision, inspection and criminal investigation.

Economic security, economic intelligence and financial intelligence occupy different levels. Economic security defines the political objective of preserving functions, capabilities and room for manoeuvre. EI and FININT produce the intelligence needed to support that objective. Industrial policy, investment screening, financial supervision, trade policy and criminal prosecution operate through their own legal instruments. Maintaining this distinction avoids attributing regulatory or interventionist functions to intelligence, and allows its contribution to concentrate on anticipation, contextualisation and the assessment of alternatives.

For the purposes of this article, economic intelligence is understood as a systematic function of collection, analysis, protection and dissemination of information relevant to strategic economic decisions. It comprises the protection of critical assets and capabilities, the detection of opportunities and threats, and support for the projection of national interests. Its effectiveness depends on coordinated interaction between public administration, business, universities and technology centres. FININT is used here in a functional sense to designate the analysis of flows, assets, ownership structures, intermediaries, payments, guarantees and financial mechanisms relevant to security. This usage does not make FININT synonymous with the activity of a Financial Intelligence Unit, nor does it alter the legal competences of the bodies that produce the information within the National Security System⁷. In this context, neither should it be reduced to money laundering and terrorist financing. It helps identify who exercises control and track

6 Government of Spain, Council of Ministers (2026), "Reforma integral del marco de prevención del blanqueo de capitales y la financiación del terrorismo" [Comprehensive reform of the AML/CFT framework], [Council of Ministers record \(referencia\) of 28 July 2026](#).

<https://www.lamoncloa.gob.es/consejodeministros/referencias/paginas/2026/20260728-referencia-rueda-de-prensa-ministros.aspx>

7 Ley 36/2015, de 28 de septiembre, de Seguridad Nacional [National Security Act].

<https://www.boe.es/eli/es/l/2015/09/28/36>

the activation of financial positions relevant to sanctions, proliferation, interference or evasion.

The two functions examine different dimensions of the same structure. EI makes it possible to locate dependencies, positions of control, critical knowledge and substitution options. FININT helps to establish who finances, guarantees, acts as intermediary, collects or benefits, and how state, corporate and criminal actors are connected. Their convergence can answer questions that usually remain fragmented: which national function is at stake, on which asset or supplier it depends, where control is concentrated, what forms of opacity obscure it, which actor can exploit the vulnerability, through which channel and with what effect on Spain's freedom of action.

It would therefore be appropriate for the new ESN to recognise EI and FININT as cross-cutting capabilities, define the products they must contribute to the decision cycle and mandate subsequent institutional development. That development may revive the SIE concept, provided it is configured as a federated and gradual system rather than as the absorption of competences already assigned. The strategy must set political direction, objectives and deadlines; the implementing instrument will have to specify authorities, membership, access rules, communications, resources and safeguards.

The decisive question is one of command and control. A system needs approved priorities, information requirements, designated producers, integration procedures, a political decision-maker and a feedback loop that makes it possible to know whether the analysis changed a decision. Without that chain, coordination is reduced to the occasional exchange of data. With it, individual bodies can retain their autonomy and produce a common picture without transferring case files, duplicating databases or altering legal custody.

The limit matters equally. Inflation, productivity, competition or foreign investment may raise serious problems without thereby amounting to a national security risk. Intervention is justified when there is a combination of concentration, difficulty of substitution, opacity, capacity for exploitation and an effect of sufficient magnitude to compromise essential functions, technological autonomy, sustainment, defence, energy, telecommunications, external action or social resilience. A rigorous ESN must broaden its capacity for observation while maintaining a precise delimitation of its object.

Why interdependence requires an integrated capability

From efficiency to the strategic use of interdependence

For several decades, interdependence was analysed above all as a source of efficiency, specialisation and cost reduction. The sanctions associated with the war in Ukraine, the technological dispute between the United States and China, export restrictions, pressure on energy and raw materials, and the regionalisation of supply chains have revealed its strategic dimension. Economic networks distribute benefits, but they also create capacities for observation, exclusion and conditioning. Farrell and Newman termed the ability to extract information from central nodes the panopticon effect, and the ability to deny access to those nodes the chokepoint effect⁸.

Spain participates intensively in European and global networks without directly controlling most of their central nodes. A realistic response is to understand Spain's own position, critical concentrations and substitution costs. EI identifies dependencies and options; FININT reveals financing, beneficiaries and channels of pressure. This reading avoids both the promise of absolute autonomy and the passive acceptance of exposures that can in fact be reduced.

Nor can Spain's position be measured solely by the volume of imports or exports. Two trade relationships of similar size may produce very different vulnerabilities if one depends on a single supplier, a revocable licence, an external financing currency or a digital service with no immediate substitute. Intelligence must identify those points of asymmetry and estimate how long the country would need to replace them. The key variable is response capacity, not the mere existence of interdependence.

Coercion can operate without a formal sanction

Economic coercion comprises sanctions, export controls and investment restrictions, but it can also take less visible forms. Regulatory delays, the withdrawal of financing, pressure on suppliers, technology licensing, discriminatory pricing, litigation, the enforcement of security interests or coordinated moves against confidence in an asset can alter decisions without an easily attributable public directive. Such action is often

⁸ Farrell, H. and Newman, A. L. (2019), "Weaponized Interdependence: How Global Economic Networks Shape State Coercion", *International Security*, 44(1), pp. 42–79. https://doi.org/10.1162/isec_a_00351

dispersed across public authorities, banks, funds, insurers, state-owned enterprises, logistics operators and interposed entities.

Strategic analysis must reconstruct the architecture that makes pressure possible. The formal nationality of a company or the physical location of an infrastructure provide insufficient information when ownership, operational control, financing and contractual jurisdiction are located in different countries. The geography of economic power is expressed in rights, dependencies and intermediary positions, as well as in material assets.

Early warning requires the observation of signals that, taken separately, may appear unremarkable. Simultaneous changes in credit conditions, concentrated purchasing of a component, coordinated litigation, rising insurance premiums, opaque corporate transactions or regulatory pressure on a logistics route may form a pattern. EI supplies the sectoral and geopolitical context; FININT helps to verify links, sequences and beneficiaries. Integration reduces the time needed to distinguish a market disturbance from deliberate action.

Technology, knowledge and data as security assets

Technological competition has shifted the focus from the final product towards the ecosystem that sustains it. Capital, specialised personnel, intellectual property, manufacturing, software, data, cloud services, minerals, machinery and standards form chains whose interruption can neutralise an entire capability. The 2023 European Economic Security Strategy organises assessment around supply chains, infrastructure, technological security and economic coercion, applying criteria of proportionality and precision⁹. The initial assessment of critical technologies prioritised advanced semiconductors, artificial intelligence, quantum technologies and biotechnology¹⁰.

EI must distinguish which capabilities have no substitute, which companies concentrate knowledge, which contracts allow it to be transferred and which dependencies turn a commercial disruption into a loss of autonomy. In defence, this reading connects the industrial and technological base with sustainment. Ammunition, spare parts,

⁹ European Commission and High Representative (2023), Joint Communication on a European Economic Security Strategy, JOIN(2023) 20 final, 20 June 2023.

¹⁰ European Commission (2023), Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, C(2023) 6689 final, 3 October 2023.

consumables, software, licences, technical data, maintenance and second- or third-tier suppliers may constitute more significant chokepoints than the main platform. The analysis must translate exposure into operational consequences: which capability ceases to be available, for how long and with what alternatives.

Research security is part of the same problem. Knowledge transfers may occur through acquisitions, investment in start-ups, staff recruitment, remote access to data, joint projects or dependence on equipment and platforms. An effective policy must differentiate legitimate collaboration from links that create exposure involving sensitive technologies. The response requires intelligible guidance for researchers and companies, proportionate assessment and consultation channels, in addition to formal controls.

Critical infrastructure also has a financial and contractual architecture

Ports, energy networks, data centres, submarine cables, satellites, payment systems and logistics nodes are not controlled through direct ownership alone. Concessions, secured debt, veto rights, operating contracts, shareholder agreements, insurance, guarantees and jurisdiction clauses distribute decision-making capacity among actors located in different countries. The material geography of an infrastructure and the legal and financial geography of its control rarely coincide completely.

EI identifies the critical function, the assets and the alternatives. FININT traces financing, guarantees, payments and beneficial ownership. The objective is to identify those contracts and structures in which a concentration of rights may constrain the continuity of an essential function. This dimension remains largely invisible in general strategies, even though it determines who can block, replace, accelerate or raise the cost of a response.

Contractual analysis must address termination rights, change of control, enforcement of security interests, step-in rights, licences, maintenance, data access and dispute resolution. No clause in isolation demonstrates a vulnerability; risk emerges when several of them concentrate decision-making capacity in an external actor and the alternatives require timescales incompatible with the continuity of the service. The assessment must connect the contract with actual operations and with crisis scenarios.

Debt, investment and exposure in third countries

Spain's security also depends on spaces beyond its borders. Infrastructure financing, sovereign debt, loans to state-owned enterprises and guarantees over strategic assets may alter the decision-making capacity of countries relevant to energy, communications, maritime routes, raw materials or regional stability. Risk appears when the financial structure concentrates rights, reduces alternatives, facilitates the appropriation of rents or makes it possible to condition sovereign decisions.

The analysis of strategic debt must go beyond macroeconomic aggregates and examine creditors, currency, maturities, guarantees, associated contracts, jurisdiction, refinancing and the connection with physical assets. The same logic applies to foreign investment. A beneficial transaction may generate a dependency that is difficult to reverse if it affects dual-use technology, data, maintenance or irreplaceable infrastructure. Intelligence makes it possible to distinguish among cases and avoids turning the foreign origin of capital into a presumption of threat.

For Spain, this external assessment has both a preventive and a foreign-policy dimension. It makes it possible to anticipate how a debt crisis, a problematic concession or a refinancing may affect relevant partners, and also to guide cooperation, alternative financing and economic diplomacy. EI is not confined to protecting the domestic market. It also helps to project interests, identify opportunities and sustain economic relations that reduce vulnerabilities, both Spain's own and those of its partners.

Distinct threats that share financial infrastructure

Terrorism, proliferation, organised crime, sanctions evasion, corruption, cyberattacks and influence operations operate according to different logics, yet they frequently use the same companies, service providers, payment platforms, trade networks and jurisdictions. Crypto-assets, tokenised assets¹¹ and decentralised finance add speed and fragmentation, although they remain connected to entities, currencies and services of the traditional financial system.

¹¹ Tokenised assets: digital representations of assets or rights over them through tokens, typically recorded and transferred on distributed-ledger infrastructures.

FININT makes it possible to reconstruct those connections. At the strategic level, its contribution can take the form of aggregate assessments of trends, actors, circumvention methods and sectoral exposure, produced and shared through legally established channels. The new European architecture against money laundering and terrorist financing, with AMLA and reinforced coordination among Financial Intelligence Units, will increase the need for interoperability in accordance with the applicable international standards¹². Such cooperation must respect the purpose, classification and restrictions specific to each source.

Functional separation protects the legitimacy of the system. Information obtained for supervision, intelligence, criminal investigation or regulatory compliance responds to different legal bases and purposes. Strategic integration does not authorise indiscriminate circulation. It can rest on aggregate products, indicators, typologies and alerts produced by the competent authority. This solution allows relevant insights to reach the political level without altering the nature or purpose of the source or transferring unnecessary personal data.

Private companies within the effective security perimeter

A large share of critical capabilities is owned or operated by companies in telecommunications, energy, banking, logistics, cloud services, data, defence, insurance, auditing, payments and transport. The State needs their knowledge, while retaining responsibility for defining the national interest. Cooperation must allow the administration to share threats, priorities and typologies, and companies to contribute early signals concerning suppliers, acquisitions, pressures, defaults, regulatory changes and strategic opportunities.

Two recurring shortcomings reduce the value of that relationship. The first is occasional cooperation, activated once the crisis is already visible. The second is the ceremonial forum without continuity or feedback. A useful SIE requires access levels, secure communications, regular exchanges, designated officers, products and verifiable results.

12 Regulation (EU) 2024/1620 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism; Regulation (EU) 2024/1624; Directive (EU) 2024/1640. Financial Action Task Force, The FATF Recommendations, Recommendation 29, updated version. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>; Egmont Group of Financial Intelligence Units, Charter. <https://egmontgroup.org/egmont-resources/egmont-group-charter/>

SMEs require specific attention because some of them concentrate essential knowledge or components, yet lack the resources to sustain advanced protection and intelligence capabilities on their own.

Trust cannot be imposed through a generic obligation to share information. Companies need to know the purpose of the exchange, how sensitive information will be handled and what benefit they will obtain. Contextualised alerts, sectoral guidance, points of contact and restricted sessions can generate a reciprocal relationship. The State receives early signals and operators improve their protective capacity.

Comparative models and lessons for Spain

International comparison requires caution. A national security strategy, an economic security policy and an economic and financial intelligence structure are different instruments. The European Union sets much of the legal framework that Spain must apply; France combines central direction with territorial deployment; Germany articulates economic protection through existing capabilities; Japan has translated economic security priorities into legislative instruments; the United Kingdom and the United States integrate security, business and finance with particular intensity; Canada offers useful experience in research security. No model can be transferred automatically.

The European Union provides the common framework. Its Economic Security Strategy organises action around the promotion of competitiveness, protection against risks and cooperation with partners. Investment screening, the Anti-Coercion Instrument, the assessment of critical technologies, the resilience of essential entities and the AML/CFT package form an expanding ecosystem¹³. For Spain the consequence is direct: a national capability must produce assessments compatible with the European architecture and, at the same time, identify its own exposures, which are not always visible in an EU-level aggregation.

The European architecture is composed of elements with different mandates. Within the European External Action Service, the European Union Intelligence and Situation Centre (EU INTCEN) produces analysis for European decision-making on the basis of

13 European Commission and High Representative (2023), Joint Communication on a European Economic Security Strategy, JOIN(2023) 20 final, 20 June 2023. Regulation (EU) 2024/1620; Regulation (EU) 2024/1624; Directive (EU) 2024/1640. Regulation (EU) 2023/2675 on the protection of the Union and its Member States from economic coercion by third countries.

contributions from Member States, delegations, missions, satellite imagery and open sources¹⁴. OLAF conducts administrative investigations into fraud, corruption and other conduct affecting the financial interests of the Union¹⁵. The EUIPO hosts the European Observatory on Infringements of Intellectual Property Rights, a network that generates knowledge, disseminates good practice and supports the enforcement of intellectual property rights¹⁶. Its information is relevant to the protection of technology, trademarks and other intangible assets, but the Observatory is not a financial intelligence unit.

Within Europol, the European Financial and Economic Crime Centre (EFECC) concentrates operational support and analytical capabilities on economic and financial crime. It hosts the secretariat of the Europol Financial Intelligence Public Private Partnership (EFIPPP), which Europol describes as the first transnational information-sharing mechanism established in the field of the fight against money laundering and terrorist financing¹⁷. Financial Intelligence Units, for their part, exchange financial intelligence within their own legal framework, and AMLA is assuming European coordination and supervisory functions. Treating these entities as sources, producers or specialised partners is useful; presenting them as a single European economic intelligence or FININT community would obscure differences of mandate, purpose and access that Spain must respect when designing its interoperability.

Japan shows how a framework document can be translated into instruments. The 2022 National Security Strategy and the Economic Security Promotion Act establish mechanisms covering critical supplies, essential infrastructure, sensitive technologies and patents¹⁸. The transferable lesson does not derive from cultural features that are difficult to compare, but from the continuity between doctrine, legislation, designated authorities and timetable.

14 European External Action Service and European Union Military Staff, "Single Intelligence Analysis Capacity: ensuring strategic situational awareness", Impetus, no. 28.

https://www.eeas.europa.eu/sites/default/files/documents/eums_impetus_28_final_web.pdf

15 European Anti-Fraud Office (OLAF), "What we do". https://anti-fraud.ec.europa.eu/about-us/what-we-do_en

16 Regulation (EU) No 386/2012 entrusting the EUIPO with tasks related to the enforcement of intellectual property rights; EUIPO, European Observatory on Infringements of Intellectual Property Rights.

<https://www.euipo.europa.eu/en/observatory>

17 Europol, European Financial and Economic Crime Centre (EFECC); Europol Financial Intelligence Public Private Partnership (EFIPPP). <https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-ececc>; <https://www.europol.europa.eu/media-press/newsroom/news/financial-institutions-and-law-enforcement-enhance-their-cooperation>

18 Government of Japan (2022), National Security Strategy of Japan, 16 December 2022.

https://www.mod.go.jp/en/d_policy/basis/index.html; Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures, Act No. 43 of 2022.

<https://www.japaneselawtranslation.go.jp/en/laws/view/4716/en>

Germany offers a different path. Its 2023 National Security Strategy adopted the notion of integrated security, and the National Economic Protection Strategy approved in March 2026 develops the protection of companies, research, innovation and value chains against physical, digital and hybrid threats¹⁹. This case demonstrates that existing capabilities can be coordinated without necessarily creating a large new organisation, provided that a mandate, a relationship with companies and implementation measures are in place.

France contributes stable administrative experience. SISSE designs and coordinates economic security policy and maintains a territorial network of delegates under the authority of the regional prefects²⁰. Its value for Spain lies in combining central direction, detection close to the asset and support for companies. The French territorial structure is not transferable, but the underlying idea is: acquisitions, the loss of a supplier or pressure on technology centres are usually detected earlier in the business and industrial environment than at the administration's headquarters.

The United Kingdom and the United States illustrate the strategic usefulness of financial information. The British integrated review connects resilience, coercion and the relationship with the private sector, while the UK Financial Intelligence Unit analyses and disseminates suspicious activity reports within its legal framework²¹. In the United States, the Treasury integrates sanctions, intelligence and the protection of financial integrity; its Office of Intelligence and Analysis forms part of the intelligence community. The 2025 National Security Strategy again places economic security at the foundation of national security²². The institutional scale of both countries is not transferable, but the regular connection between financial analysis and strategic decision-making is.

19 Federal Government of Germany (2023), National Security Strategy. <https://www.bundesregierung.de/breg-de/aktuelles/national-security-strategy-2196356>; Federal Government of Germany (2026), Nationale Wirtschaftsschutzstrategie, approved on 18 March 2026. <https://www.bundesregierung.de/breg-de/aktuelles/kabinett-wirtschaftsschutz-2412548>

20 Direction générale des Entreprises, Service de l'information stratégique et de la sécurité économiques (SISSE) and DISSE territorial network. <https://www.entreprises.gouv.fr/service-de-linformation-strategique-et-de-la-securite-economiques-sisse>

21 Government of the United Kingdom (2023), Integrated Review Refresh 2023. <https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world>; National Crime Agency, UK Financial Intelligence Unit. <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/ukfiu>

22 The White House (2025), National Security Strategy. <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>; U.S. Department of the Treasury, Office of Terrorism and Financial Intelligence. <https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence>; Office of Intelligence and Analysis. <https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence/oia>

Canada is particularly useful with regard to the protection of knowledge. The Canadian Security Intelligence Service (CSIS) has developed public guidance for companies, researchers and investors, and takes part in the implementation of research security policies. The policy on research in sensitive technologies and affiliations of concern establishes targeted controls over federal funding, and the Secure Innovation initiative disseminates mitigation guidance against economic espionage²³. The lesson for Spain is to combine protection, training and dialogue with universities and companies without closing off legitimate scientific cooperation.

These cases also reveal two institutional paths. France makes a coordinating centre and a territorial network visible. Germany distributes responsibility among existing structures and reinforces a culture of protection in companies and research. Japan links strategy and legislation; Canada emphasises prevention and public guidance; the United Kingdom and the United States connect financial data with security decisions. Spain could combine elements of these paths: recognisable political direction, federated execution, territorial capacity and a stable interface with the business and industrial base.

Table 1. Comparative models and lessons for Spain

Actor	Strategic framing	Main mechanism	Lesson for Spain
European Union	Economic Security Strategy and AML/CFT framework	Risk assessment, critical technology, investment, anti-coercion and AMLA	Align the national capability with the European system while retaining a specific reading of Spain's exposure
Japan	Economic security within the 2022 National Security Strategy	Act covering supplies, infrastructure, patents and technology	Link doctrine, instruments, designated authorities and timetable
Germany	Integrated security and the 2026 economic protection strategy	Protection of companies, R&D and value chains	Coordinate existing capabilities through assessable technical development
France	Stable administrative policy on economic security	Central SISSE and territorial DISSE network	Combine political direction with detection close to companies and assets
United Kingdom	Integrated review, resilience and the fight against illicit finance	Public-private interface and UKFIU	Separate functions and ensure common products and stable channels
United States	Economic security as a dimension of national security	Treasury, sanctions and strategic financial intelligence	Connect financial analysis with foreign policy and security

²³ Canadian Security Intelligence Service, Public Report 2024. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2024.html>; Government of Canada, Policy on Sensitive Technology Research and Affiliations of Concern. <https://ised-isde.canada.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/policy-sensitive-technology-research-and-affiliations-concern>; Five Eyes Secure Innovation initiative. <https://www.canada.ca/en/security-intelligence-service/news/2024/10/five-eyes-intelligence-partners-launch-shared-security-advice-initiative-for-tech-companies-researchers-and-investors.html>

Actor	Strategic framing	Main mechanism	Lesson for Spain
Canada	Protection of innovation and research	Public guidance, STRAC policy and Secure Innovation	Extend training and protection to universities, investors and technology SMEs

Source: Authors' analysis based on the strategies and official sources cited.

The comparative examination makes it possible to identify five recurrent features. First, a recognisable political mandate. Second, a node or procedure capable of integrating information without erasing responsibilities. Third, a stable relationship with companies, universities and technology centres. Fourth, products that turn analysis into decisions on investment, technology, sanctions, asset protection or crisis response. Fifth, separation between strategic intelligence, supervision, criminal investigation and business support. The main conclusion is institutional: capabilities weaken when coordination depends on personal relationships and disappears from public assessment.

Proposals for the 2026 National Security Strategy

In light of the above, it seems reasonable to think that the ESN should establish doctrine, priorities, governance and implementation requirements. It does not need to describe a complete organisational chart, but it should avoid a generic formula that could, once again, postpone implementation. The following seven lines of action would turn the recognition of EI and FININT into an assessable capability.

Express recognition and gradual development of an SIE

The strategy should name economic intelligence and financial intelligence as cross-cutting capabilities supporting anticipation, prevention, crisis management and strategic decision-making. It should also revive the concept of an Economic Intelligence System, understood as a federated framework for integrating products and not as a new authority with indiscriminate access to information. This formulation acknowledges the approach first introduced in 2011 and corrects the subsequent loss of continuity.

The ESN can mandate an implementation plan with a defined deadline. An initial planning cell should inventory capabilities, specify products, identify gaps, propose coordination rules and compare organisational alternatives. The final design would be adopted after consulting the competent bodies, major operators, strategic SMEs, universities and

technology centres. This gradual development reduces the risk of creating a nominal structure without doctrine or resources.

The system should be guided by six principles: political direction at the appropriate level, with effective command and control; distributed competences and clear responsibilities; public–public and public–private participation; variable geometry based on need-to-know; secure communications; and a common methodology with traceability. The Interministerial Regulatory Board on Foreign Trade in Defence and Dual-Use Material (JIMDDU) offers a limited but useful analogy. It demonstrates that an interministerial body can assess transactions from different perspectives and submit a coordinated position²⁴. Its subject matter, legal regime and decisions are not transferable to the SIE, but its collegiate logic deserves study.

Deployment could be organised in three stages. The first would produce the inventory of capabilities, the conceptual framework and two or three pilot products on priority exposures. The second would test cooperation procedures with operators and universities, including the territorial dimension. The third would evaluate results and propose a stable institutional arrangement. Each stage should close with an explicit decision on continuity, resources and corrections. This would prevent the SIE from once again being reduced to a programmatic declaration.

A national assessment of economic and financial exposure

The main product should be a periodic assessment addressed to the political level, integrating economic, technological, financial, contractual and territorial dependencies. Its unit of analysis would be the chain through which a vulnerability can become a strategic effect. The sequence can be expressed simply: critical function, dependency, concentration, opacity, actor, channel of exploitation, effect and available response.

The assessment must overlay two maps. The first represents dependencies, control rights, technology and chokepoints. The second reconstructs financing, intermediaries, guarantees, payments and beneficiaries. Overlaying them makes it possible to distinguish

²⁴ Real Decreto 679/2014, de 1 de agosto, por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso [Regulation on the control of foreign trade in defence material, other material and dual-use items and technologies].

<https://www.boe.es/buscar/act.php?id=BOE-A-2014-8926>

a manageable dependency from an exploitable vulnerability, and an infrastructure located in Spain from a capability controlled from another jurisdiction.

Indicators should measure concentration, substitutability, replacement time, jurisdictional exposure, corporate control, maturities, guarantees and network centrality. Part of the information will come from open sources and administrative registers; another part will require restricted or classified contributions. The final product must be comparable over time and useful for prioritising decisions.

The assessment should not be limited to describing risks. For each priority exposure it must identify response options, the responsible authority, cost, implementation time and residual risk. Diversification, reserves, contractual modification, alternative financing, knowledge protection, European cooperation or the preparation of a diplomatic response are distinct measures. Linking the diagnosis to alternatives turns the product into genuine decision support.

Technical integration with data governance and human validation

The ESN should require a stable procedure for integrating the assessments produced by the competent bodies. Each entity would retain its competences, the custody of information and responsibility for its own analysis. Integration can rest on indicators, typologies, patterns, scenarios and aggregate assessments. Access to sensitive information would remain within legally established channels.

Technology can improve search, entity resolution, deduplication, scenario comparison and source traceability. Artificial intelligence can assist those tasks where adequate data, secure environments, access controls, decision logging and human validation exist. Its role must be defined as analytical support. Attribution, prioritisation and strategic recommendation continue to require identifiable institutional responsibility. The priority is a common doctrine and a governed data architecture; a platform lacking those conditions would merely automate fragmentation.

Interoperability does not require a central database. It can be built through a shared vocabulary, common identifiers, exposure records, classification criteria and federated query mechanisms. This model reduces unnecessary transfers, allows information to be

updated at its originating body and facilitates audit. Quality will depend on each assertion retaining its source, date, confidence level and validating officer.

Priority missions linked to freedom of action

The strategy should concentrate effort on a limited set of missions. The first is the protection of critical supply chains for defence, energy, health, food, telecommunications and digital transformation. The second is technological and knowledge security, including investment, acquisitions, talent mobility, intellectual property, cloud services and dual-use technologies. The third is the comprehensive protection of critical infrastructure, addressing ownership, financing, operating contracts and jurisdiction.

The fourth mission is the analysis of economic coercion, sanctions and export controls. The fifth covers the financing associated with state, terrorist, criminal and proliferation-related threats, including circumvention mechanisms and logistics networks. The sixth examines financial and contractual exposure in third countries relevant to Spain, with attention to sovereign debt, concessions, guarantees and infrastructure financing. The seventh incorporates these variables into crisis and defence exercises in order to measure time-to-effect, reserves and realistic alternatives.

The annual selection of priorities should combine potential impact, likelihood, urgency, difficulty of substitution and effective capacity to intervene. This filter prevents the system from attempting to cover the entire economy and allows multidisciplinary teams to concentrate on a manageable number of exposures. Priorities must be revised whenever the environment, suppliers, technology or financial positions change.

A stable, territorially informed public-private network

The ESN should mandate a permanent mechanism involving operators in strategic sectors, business associations, financial institutions, insurers, universities and technology centres. Its usefulness will depend on the feedback it provides through declassified alerts, typologies, guidance and consultation channels. Requesting information without sharing context produces formal cooperation and little intelligence.

The network needs differentiated levels. Some exchanges can be open, others restricted, and the most sensitive bilateral. Participation must follow need-to-know and rely on

communications appropriate to the level of classification. Territorial liaison with the autonomous communities and industry clusters is also advisable. The early detection of an acquisition, the disappearance of a supplier or pressure on a technology centre usually occurs close to the asset.

Strategic SMEs must receive specific treatment. Some dominate niches of knowledge, maintenance or components for which no substitute exists, yet their protective capacity is lower than that of large groups. The system should facilitate diagnostics, alert channels, training and access to public guidance without imposing disproportionate burdens.

Nor should business representation rest solely on large umbrella organisations. For certain supply chains it will be necessary to convene specialised suppliers, sectoral associations, insurers, financial institutions or technology centres directly. The variable geometry proposed for the SIE makes it possible to adapt each group to the specific problem and to reduce both conflicts of interest and the unnecessary exposure of sensitive information.

Training and research security

Training is part of the system's infrastructure. The profiles required span intelligence, finance, geography, economics, law, accounting, data, cybersecurity, engineering, trade and sectoral knowledge. The administration needs a common language and shared methods; companies require capabilities to recognise pressure, protect information and communicate relevant signals; and universities must identify risks affecting projects, funding, intellectual property, staff mobility and sensitive collaborations.

The Canadian experience suggests combining public guidance, targeted assessment and support for researchers. Spain could produce sectoral guidance, training modules and consultation procedures for universities and technology centres, preserving scientific openness and avoiding blanket restrictions. Training must extend to executives, security officers, researchers and SMEs. Without a shared culture, the formal architecture will depend on a handful of individuals and will lose continuity.

The training programme should differentiate levels. A basic level would provide economic-security awareness and criteria for identifying warning signs. A professional level would teach the analysis of corporate networks, contracts, supply chains, financing and

technology. An executive level would concentrate on scenarios, decision-making and crisis management. Joint exercises involving the administration, companies and universities would serve to test common language, communications and response times.

Interoperability, resources, evaluation and safeguards

Spain should design this capability within the European Union and in cooperation with NATO and allied partners²⁵. Interoperability requires comparable formats, exercises, the exchange of indicators and joint scenario analysis. Liaison with EU INTCEN, OLAF, the EUIPO and its Observatory, Europol and the EFECC, the EFIPPP, the Financial Intelligence Units and AMLA must be established by function, legal basis and need-to-know. Convergence can produce common assessments, typologies and alerts; it does not justify pooling data custody or circulating data obtained for incompatible purposes.

The mandate must be matched with resources, professional profiles and a reporting obligation. The National Security Annual Report offers a channel for reporting on products delivered, exercises conducted, sectors covered, cooperation and progress in the implementation plan. Indicators must measure improvement in anticipation and response, not merely meetings or volumes of data.

Proportionality, precision, data protection, commercial confidentiality and functional separation are design principles. Economic security must not become an open-ended category or protectionism without assessment. Parliamentary oversight and periodic review must verify that measures respond to defined risks, avoid duplication and produce verifiable improvement.

Evaluation should combine activity and outcome indicators. The number of products, exercises or participants indicates effort, but does not demonstrate usefulness. Detection time, the quality of the alternatives identified, the reduction of critical exposures, the incorporation of alerts into decisions and the degree of implementation of agreed measures must also be measured. A periodic external review can verify that the system retains focus, legality and added value.

²⁵ NATO (2022), NATO 2022 Strategic Concept. <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept>

Conclusions

The incorporation of economic and financial intelligence into the 2026 ESN is justified because markets, contracts, financing, technology, data and supply chains have become channels of power. A strategy that describes that environment without organising the capability to interpret it will maintain the current gap between diagnosis and decision.

Spain is not starting from scratch. It has doctrinal precedents, specialised bodies, supervisory authorities, registries, an intelligence community and an increasingly developed European framework. The gap lies in convergence. What is missing is a stable chain connecting political priorities, analytical products, coordination, response and evaluation. Reviving the SIE as a federated and gradual architecture allows continuity with the proposal begun in 2011 without encroaching on existing competences or rushing into an organisational chart.

The joint contribution of EI and FININT can be summarised in two maps. The first shows where dependencies, control rights, technology and chokepoints are concentrated. The second reveals who finances, intermediates, guarantees, collects and benefits. Overlaid, they make it possible to distinguish between an ordinary economic relationship and a vulnerability open to exploitation.

The institutional dimension must be accompanied by a cultural one. Training within the administration, companies and universities, attention to strategic SMEs and research security are conditions for continuity. So are territorial detection, secure communications and useful feedback for the private actors who cooperate.

The proposed architecture avoids two extremes. The first would be to create a large central structure before defining products, competences and users. The second would be to rely once again on spontaneous coordination among dispersed capabilities. A federated SIE, tested in stages and subject to evaluation, makes it possible to build common direction without destroying specialisation. This architecture should also include centralised political-level direction with genuine command-and-control authority. Variable geometry and need-to-know facilitate the participation of each actor whenever its contribution is pertinent.

The quality of the system will depend less on the volume of data than on its capacity to formulate the right questions, connect sources and provide options in time to act. Technology can accelerate those tasks, but it does not replace doctrine, trust or

responsibility. Useful intelligence culminates in an informed decision and feeds back into the system through evaluation and new requirements.

The opportunity in 2026 is to establish a verifiable mandate. If the ESN recognises these functions, mandates an SIE implementation plan, requires a national exposure assessment, integrates the financial dimension into crisis scenarios and establishes responsible authorities, resources, safeguards and indicators, it will have made substantial progress in reducing the accumulated discontinuity. If it merely reiterates the connection between the economy, technology and security, the diagnosis will be correct but the capability of the State will remain unchanged in an increasingly complex and contested environment.

*Juan Carlos Fernández Cela**
Professor, Complutense University of Madrid (UCM)
*Col. (Ret.) José Fuentes García**
Professor, ESFAS/CESEDEN