Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Estudios de Seguridad Internacional

La inteligencia europea frente a las amenazas híbridas en el periodo 2014-2026

Trabajo fin de estudio presentado por:	Luis Rodríguez Trejo
Tipo de trabajo:	Revisión sistemática
Director/a:	Pedro Trujillo Álvarez
Fecha:	21/07/2026

Resumen

El marco de seguridad europeo ha sufrido una profunda transformación desde la anexión rusa de Crimea en 2014, lo que ha evidenciado una asimetría entre las crecientes amenazas híbridas y la capacidad de respuesta comunitaria. Este trabajo analiza la evolución de la inteligencia europea frente a estos desafíos durante el periodo 2014-2026, empleando una revisión sistemática cualitativa basada en la metodología PRISMA 2020 adaptada.

El estudio aborda primero el mapa actual de amenazas (Rusia, flanco sur y China) para examinar después la respuesta institucional, materializada en estructuras como la SIAC y el EU INTCEN. Seguidamente, se diagnostican sus carencias estructurales: ausencia de medios de obtención propios, dependencia de la voluntad estatal y la limitación del artículo 4.2 del TUE, así como la dicotomía entre soberanía e integración. Finalmente, al requerir la centralización una reforma de los Tratados, el trabajo concluye que la solución realista es la integración funcional de capacidades.

Palabras clave: amenazas híbridas, inteligencia, seguridad europea, zona gris, cooperación internacional.

Abstract

The European security framework has undergone a deep transformation since Russia's annexation of Crimea in 2014, revealing an imbalance between growing hybrid threats and the EU's capacity to respond. This Master's thesis analyses the evolution of European intelligence in the face of these challenges during the period 2014–2026, using a qualitative systematic review based on the adapted PRISMA 2020 methodology.

The study first examines the current threat landscape (Russia, the southern flank and China) before turning to the institutional response, as embodied in structures such as the SIAC and EU INTCEN. It then identifies structural shortcomings: the lack of independent intelligence-gathering capabilities, dependence on national will, the limitations of Article 4.2 of the TEU, and the dichotomy between sovereignty and integration. Finally, as centralisation would require a reform of the Treaties, the study concludes that the realistic solution is the functional integration of capabilities.

Keywords: hybrid threats, intelligence, European security, grey zone, international cooperation.

Índice de contenidos

1. Introducción 8
1.1. Justificación del tema elegido 8
1.2. Problema y finalidad del trabajo 9
1.3. Preguntas y objetivos 9
1.3.1. Preguntas de investigación 9
1.3.2. Objetivos de investigación 10
1.4. Metodología 10
1.5. Caracterización del conjunto de fuentes incluido en la revisión 16
2. Marco teórico 20
2.1. Concepto y evolución de las amenazas híbridas 20
2.1.1. La superación de las taxonomías convencionales 21
2.1.2. El concepto de la guerra híbrida 22
2.1.3. La zona gris y la dimensión cognitiva 24
2.2. El papel de la inteligencia frente a las amenazas híbridas 25
3. Desarrollo 28
3.1. Los retos para la seguridad europea: el escenario actual 29
3.1.1. Rusia y sus *proxies* 29
3.1.2. El flanco sur: el Magreb y el Sahel 33
3.1.3. China: influencia estratégica y la diplomacia de la sonrisa 37
3.2. La respuesta de la inteligencia: capacidades y acciones 39
3.2.1. Del marco común de 2016 a la Comunicación conjunta de 2018 40
3.2.2. Capacidades comunitarias: la SIAC, el EU INTCEN y la Célula de fusión 41
3.2.3. La consolidación de la doctrina (2022-2026) 43
3.2.4. Cooperación UE-OTAN y el Hybrid CoE 44

3.3. Desafíos y carencias del modelo europeo 46
3.4. Propuestas y líneas de acción 48
3.4.1. La asimetría entre amenaza y respuesta 49
3.4.2. ¿Una Agencia Europea de Inteligencia? Propuestas oficiales y académicas 50
3.4.3. La integración de capacidades como propuesta realista 52
3.5. Discusión de la evidencia revisada 55
3.5.1. Concentración geográfica y sesgos del corpus analizado 55
3.5.2. Convergencias y divergencias doctrinales 56
3.5.3. Límites metodológicos y fiabilidad de las fuentes seleccionadas 56
3.5.4. Vigencia de las fuentes en el escenario estratégico de 2026 57
4. Conclusiones 58
Referencias bibliográficas 61
Bibliografía básica 61
Bibliografía complementaria 64
Legislación citada 66
Fuentes hemerográficas 66
Listado de abreviaturas 67

Índice de figuras

Figura 1 - Diagrama de flujo del proceso de selección de fuentes (PRISMA 2020 adaptado). 16

Índice de tablas

Tabla 1 - Criterios de inclusión y exclusión. 12

Tabla 2 - Fuentes consultadas y resultados obtenidos. 14

Tabla 3 - Caracterización del corpus según PRISMA adaptado. 19

Tabla 4 - Síntesis comparativa de las amenazas híbridas a la seguridad europea. 39

1. Introducción

El presente Trabajo de Fin de Máster estudia la respuesta europea en materia de inteligencia frente a las amenazas híbridas más reseñables. Esta sección justifica la elección de este tema, presenta la problemática derivada y plantea una serie de cuestiones y objetivos a los que se dará respuesta a lo largo de todo el documento. Posteriormente, explica la metodología empleada en la selección del corpus sometido a análisis y cierra con la caracterización del conjunto de fuentes resultante.

1.1.Justificación del tema elegido

Los cambios de la última década en el panorama geopolítico global y sus implicaciones para la seguridad del viejo continente han tenido un gran impacto en el proyecto de la Unión Europea. Tras la aparente estabilidad que sobrevino a nivel global con la caída del Muro de Berlín y la desintegración de la URSS, el nuevo milenio ha traído consigo un amplio catálogo de actores, amenazas y riesgos para la seguridad, en muchos casos desconocidos hasta la fecha.

En un escenario internacional marcado por lo que Dezcallar (2022) define como un profundo "desasosiego" geopolítico, la Unión Europea se enfrenta a una realidad donde la línea que separa el conflicto armado de la paz se ha difuminado hasta hacerse, en muchos casos, difícilmente distinguible. Como señala Sánchez Herráez (2021), el retorno a los conceptos clásicos de la guerra se hace necesario para comprender que las amenazas híbridas, pese a la ineludible innovación que comportan, no dejan de ser la lucha por imponer la voluntad frente al adversario –y mantener la soberanía– que siempre ha sido la guerra.

Este estudio parte de la consideración de que, tras los sucesos de 2014 en Crimea y la actual inestabilidad en los flancos este y sur, la seguridad europea ya no puede garantizarse únicamente mediante capacidades militares convencionales, sino que, en este escenario, la inteligencia y la cooperación adquieren un papel protagonista. Esto nos lleva a resaltar la importancia del esfuerzo comunitario en materia de seguridad y defensa y, más concretamente, al necesario análisis acerca de cómo la inteligencia debe adaptarse a la "zona gris" (Aznar Fernández-Montesinos, 2023), donde actores estatales y no estatales operan por debajo del umbral del conflicto armado para desestabilizar las instituciones democráticas europeas.

1.2. Problema y finalidad del trabajo

La cuestión central que busca abordar este trabajo es la asimetría entre la creciente sofisticación de las amenazas híbridas y la fragmentación de la respuesta de inteligencia europea. Aunque la literatura académica ha avanzado significativamente en el estudio y la definición de los conceptos de "guerra híbrida" y "actor híbrido" (Quiñones de la Iglesia, 2020), en la práctica, la respuesta ante tales amenazas sigue dependiendo en gran medida de la capacidad individual de los Estados, en tanto que la implementación efectiva de una arquitectura de inteligencia común está lejos de ser una realidad. Autores como Díaz-Caneja ya advertían en 2014 de la necesidad de superar los recelos en la compartición de información para crear una verdadera Política Europea de Inteligencia, en línea con el esfuerzo integrador impulsado en otros ámbitos de la Unión.

La finalidad de esta revisión sistemática es, por tanto, sintetizar las soluciones existentes -desde el refuerzo del EU INTCEN hasta el papel del analista en la era digital (Páramo, 2022)- para evaluar su viabilidad frente a los retos actuales de seguridad. Se busca determinar si el modelo europeo actual basado en dependencias funcionales es resiliente o si requiere una transformación estructural hacia una Agencia Europea de Inteligencia, tal como proponen las corrientes más integracionistas.

1.3. Preguntas y objetivos

Partiendo de la problemática expuesta en los apartados previos acerca de las vulnerabilidades y retos que presentan las amenazas híbridas para la seguridad europea, este trabajo busca analizar la asimetría entre dichas amenazas y las capacidades existentes en materia de inteligencia a nivel europeo, así como sus causas y posibles alternativas.

1.3.1. Preguntas de investigación

Para llevar a cabo el análisis planteado bajo el epígrafe anterior, se plantean cuatro preguntas de investigación a las que se intenta dar respuesta a lo largo del documento, a saber:

- **PI 1**: ¿Cómo afectan las actuales estrategias híbridas a la estabilidad institucional y la seguridad en Europa?
- **PI 2**: ¿Qué papel desempeñan los mecanismos de inteligencia actuales, tanto a nivel nacional como de la Unión Europea, en la lucha contra estas amenazas?

- **PI 3**: ¿En qué medida las reticencias de los Estados miembros a ceder soberanía y la falta de integración política limitan la respuesta en materia de seguridad frente a actores como Rusia, China u otros no estatales?
- **PI 4**: ¿Existen alternativas de colaboración en inteligencia que permitan superar la fragmentación actual y resulten aceptables para los Estados miembros en relación con la cesión o mantenimiento de la soberanía en este ámbito?

1.3.2. Objetivos de investigación

El objetivo general de este estudio es analizar el papel de la inteligencia en la detección y respuesta ante las amenazas híbridas. Asimismo, se busca evaluar los desafíos que dichas amenazas suponen para la seguridad y la estabilidad europeas en el actual escenario geopolítico.

Este objetivo general se concreta en los siguientes objetivos específicos, que buscan dar respuesta a las preguntas definidas en el apartado anterior:

- **OE 1**: Identificar y categorizar las amenazas híbridas a las que se enfrenta Europa, analizando el impacto de la desinformación y las acciones por debajo del umbral del conflicto armado (zona gris) en la sociedad y las instituciones.
- **OE 2**: Evaluar la arquitectura y las capacidades de la inteligencia europea frente a dichas amenazas, con especial foco en las agencias de los Estados miembros, el EU INTCEN y la cooperación con la OTAN.
- **OE 3**: Examinar los retos y obstáculos para lograr esos objetivos; en especial en lo relacionado con la cooperación, la autonomía estratégica y la disyuntiva entre la preservación de la soberanía y el esfuerzo integrador.
- **OE 4**: Valorar las soluciones o líneas de acción propuestas en los ámbitos oficial y académico y su adecuación a las necesidades. Viabilidad de un modelo de inteligencia europeo más integrado.

1.4. Metodología

El presente trabajo de fin de estudios se enmarca en la modalidad de revisión sistemática de carácter cualitativo. Su objetivo es analizar la evidencia académica e institucional existente hasta la fecha sobre la evolución de las amenazas híbridas y la respuesta de los servicios de inteligencia de la Unión Europea.

Con el objetivo de sistematizar en la medida de lo posible el trabajo realizado, se han seguido las directrices de reporte de PRISMA 2020 (Page et al., 2021), adaptadas a las ciencias sociales (Petticrew y Roberts, 2006; Tricco et al., 2018). Se ha tomado esta decisión debido a las características de las fuentes empleadas: se trata de evidencia cualitativa, heterogénea y apoyada en literatura gris e institucional; una revisión ortodoxa según PRISMA 2020 excluiría un número sensible de referencias de interés. De este modo, se busca dar una respuesta lo más completa y adecuada posible a las preguntas de investigación planteadas en el apartado 1.3.1.

Se describe a continuación la metodología empleada para garantizar el rigor del estudio:

1. Fuentes de información. Repositorios académicos e institucionales, siendo los más relevantes los siguientes:
    - Bases de datos académicas: Scopus como base primaria, Dialnet como base secundaria especializada en literatura en español. Google Scholar se desechó por su falta de precisión, lo que producía resultados de búsqueda demasiado amplios y fuera del ámbito de interés.
    - Repositorios institucionales: Instituto Español de Estudios Estratégicos, Real Instituto Elcano.
    - Búsqueda dirigida: Documentación oficial de la Comisión Europea, el Servicio Europeo de Acción Exterior (SEAE) y el EU INTCEN. También se ha realizado rastreo de citas.
2. Estrategias de búsqueda: Para la búsqueda de documentación, especialmente en bases de datos académicas, se han utilizado diferentes términos de búsqueda, enlazados mediante los operadores booleanos *AND* y *OR*, a saber: "amenazas híbridas" AND "unión europea", "hybrid threats" AND ("europe" OR "EU" OR "European"), ("inteligencia" OR "servicios de inteligencia") AND "amenazas híbridas" AND ("seguridad europea" OR "Unión Europea"), ("intelligence sharing" OR "intelligence services") AND "hybrid threats" AND "European security".

3. Criterios de inclusión y exclusión, establecidos para acotar el objeto de estudio, recogidos en la siguiente tabla:

	Criterio de inclusión	Criterio de exclusión
Ámbito temporal	Publicación entre 2014 (Crisis de Crimea como punto de inflexión) y la actualidad.	Publicaciones anteriores a 2014.
Ámbito geográfico	Europa y áreas de interés.	Cualquier ámbito distinto del anterior.
Temática	Inteligencia frente a amenazas híbridas.	Otros temas o interpretaciones, por ejemplo, amenazas clásicas.
Idiomas	Español e inglés.	Cualquier idioma distinto de los dos anteriores.
Tipología documental	Artículos de revistas científicas revisadas, libros de autores de reconocido prestigio, informes técnicos de *think tanks* de referencia y publicaciones académicas.	Artículos de prensa no especializada o blogs de opinión sin respaldo académico.

Tabla 1 - *Criterios de inclusión y exclusión.*
Fuente: elaboración propia.

Cabe señalar que la restricción temporal fijada a partir de 2014 rige únicamente para la selección de la literatura objeto de la revisión sistemática, no siendo óbice para la inclusión puntual de obras teóricas fundacionales de fecha anterior (como los postulados originarios de Hoffman) a efectos exclusivos de conformar el marco conceptual y la evolución doctrinal del término.

La siguiente tabla condensa los resultados de búsqueda obtenidos tras la aplicación de la metodología empleada en los puntos anteriores:

Tipo de fuente	Fuente	Fecha de consulta	Cadena de búsqueda	Filtros aplicados	Resultados brutos (n)
Base de datos	Dialnet	24/03/2026	"amenazas hibridas" AND ("Europa" OR "UE" OR "Unión Europea")	Intervalo temporal: 2014-2026. Idiomas: español e inglés. Textos completos.	35
Base de datos	Dialnet	24/03/2026	"hybrid threats" AND ("europe" OR "EU" OR "European")	Intervalo temporal: 2014-2026. Idiomas: español e inglés. Textos completos.	27
Base de datos	Dialnet	26/03/2026	("inteligencia" OR "servicios de inteligencia") AND ("amenazas híbridas" or "híbridas") AND ("seguridad europea" OR "Unión Europea")	Intervalo temporal: 2014-2026. Idiomas: español e inglés. Textos completos.	0
Base de datos	Dialnet	26/03/2026	("intelligence sharing" OR "intelligence services") AND "hybrid threats" AND "European security"	Intervalo temporal: 2014-2026. Idiomas: español e inglés. Textos completos.	0
Base de datos	Dialnet	26/03/2026	"intelligence" AND "hybrid" AND "Europe"	Intervalo temporal: 2014-2026. Idiomas: español e inglés. Textos completos.	60
Base de datos	Scopus	26/03/2026	TITLE-ABS-KEY ("hybrid threat*" AND ("European Union" OR "European security" OR Europe* OR EU)) AND (LIMIT-TO (SUBJAREA , "SOCI")) AND PUBYEAR > 2013 AND (EXCLUDE (DOCTYPE , "bk"))	Intervalo temporal: 2014-2026. Idiomas: español e inglés. Textos completos.	137
Base de datos	Scopus	26/03/2026	TITLE-ABS-KEY (("hybrid threat*" OR "grey zone") AND intelligence AND ("European Union" OR Europe* OR EU)) AND PUBYEAR > 2013 AND (LIMIT-TO (SUBJAREA , "SOCI")) AND (LIMIT-TO (OA , "all")) AND (LIMIT-TO (LANGUAGE , "Spanish") OR LIMIT-TO (LANGUAGE , "English")) AND (EXCLUDE (DOCTYPE , "bk"))	Intervalo temporal: 2014-2026. Idiomas: español e inglés. Textos completos.	9

Tipo de fuente	Fuente	Fecha de consulta	Cadena de búsqueda	Filtros aplicados	Resultados brutos (n)
Fuente institucional	IEEE	29/03/2026	("inteligencia" OR "servicios de inteligencia") AND "amenazas híbridas" AND ("seguridad europea" OR "Unión Europea")	-	69
Fuente institucional	Real Instituto Elcano	29/03/2026	"amenazas híbridas" AND "unión europea"	Intervalo temporal: 2014-2026.	29
Fuente institucional	Real Instituto Elcano	29/03/2026	"inteligencia" and "híbrida"	Intervalo temporal: 2014-2026.	75
Fuente institucional	Real Instituto Elcano	29/03/2026	"inteligencia" and "seguridad europea"	Intervalo temporal: 2014-2026.	56
Búsqueda dirigida	EUR-Lex / Comisión Europea / Consejo	05/04/2026	(documentos oficiales citados en el trabajo)	Intervalo temporal: 2014-2026.	7
Búsqueda dirigida	SEAE / EEAS	05/04/2026	(informes FIMI y documentación oficial)	Intervalo temporal: 2014-2026.	3
Búsqueda dirigida	Búsqueda inversa (referencias)	05/04/2026	(rastreo de citas en obras incluidas)	Intervalo temporal: 2014-2026.	4
				TOTAL identificados (brutos)	**511**

Tabla 2 - *Fuentes consultadas y resultados obtenidos.*
Fuente: elaboración propia.

Sobre este primer conjunto de resultados, se ha realizado un proceso de selección para obtener un subconjunto del mismo que se ajustase a las necesidades del estudio. El flujo ha sido el descrito a continuación. En primer lugar, se han eliminado 50 registros duplicados que aparecían en varias búsquedas, quedando 461. A continuación, se ha realizado un cribado por título y resumen, excluyendo aquellos documentos que no tenían relación con los temas de interés para este Trabajo de Fin de Máster. Se han excluido 336 registros, quedando 125. De los 125 registros restantes, 28 no estaban disponibles a texto completo, bien por requerir suscripción o por tratarse de publicaciones impresas. Tras ello, quedaron 97 documentos. De los 97 documentos resultantes del punto anterior, se ha realizado una evaluación de su texto completo, lo que ha permitido descartar 55 por los siguientes motivos:

- 4 de ellos estaban fuera del rango temporal definido.
- 37 no se adecuaban totalmente a la temática o el enfoque del Trabajo. Particularmente, un número significativo de ellos trataba amenazas clásicas o tenía un enfoque eminentemente militar, alejado del ámbito de la inteligencia.

- 12 documentos analizaban ámbitos geográficos distintos del delimitado.
- 2 documentos estaban en ruso.

Finalmente, se ha incluido un total de 42 documentos para realizar, mediante un proceso de síntesis narrativa o temática cualitativa, un análisis de su contenido, estructurándolo en cuatro ejes: la evolución conceptual de las amenazas híbridas, la arquitectura actual de la inteligencia europea, las capacidades y carencias de dicha arquitectura, y las propuestas de reforma o integración existentes. La figura 1 sintetiza el flujo descrito en el párrafo anterior.

No conviene terminar este apartado sin reconocer las limitaciones propias del método de análisis elegido. En primer lugar, la búsqueda no es completamente exhaustiva al excluir a Google Scholar del recuento y no contar con más buscadores como *Web of Science*. Además, el componente dirigido introduce necesariamente un sesgo mínimo por parte del autor. Por otro lado, no se ha realizado revisión cruzada ni doble cribado y la restricción idiomática limita la perspectiva de análisis a la de los autores occidentales de referencia. Con todo, se ha procurado mantener el rigor anteriormente descrito durante todo el análisis.

Por último, en un tema como el analizado, de marcada actualidad, el autor ha considerado oportuno incluir algunas referencias contrastadas a prensa de reputación probada para respaldar algunos acontecimientos recientes.

El corpus final objeto de análisis queda integrado por los 42 documentos mencionados. A ellos se añaden, en el aparato de referencias y al margen del recuento sistemático, las guías metodológicas del propio método PRISMA, las obras teóricas fundacionales anteriores al marco temporal —incorporadas conforme al criterio ya expuesto—, la legislación citada y las referencias de prensa contrastada empleadas como anclaje de actualidad.

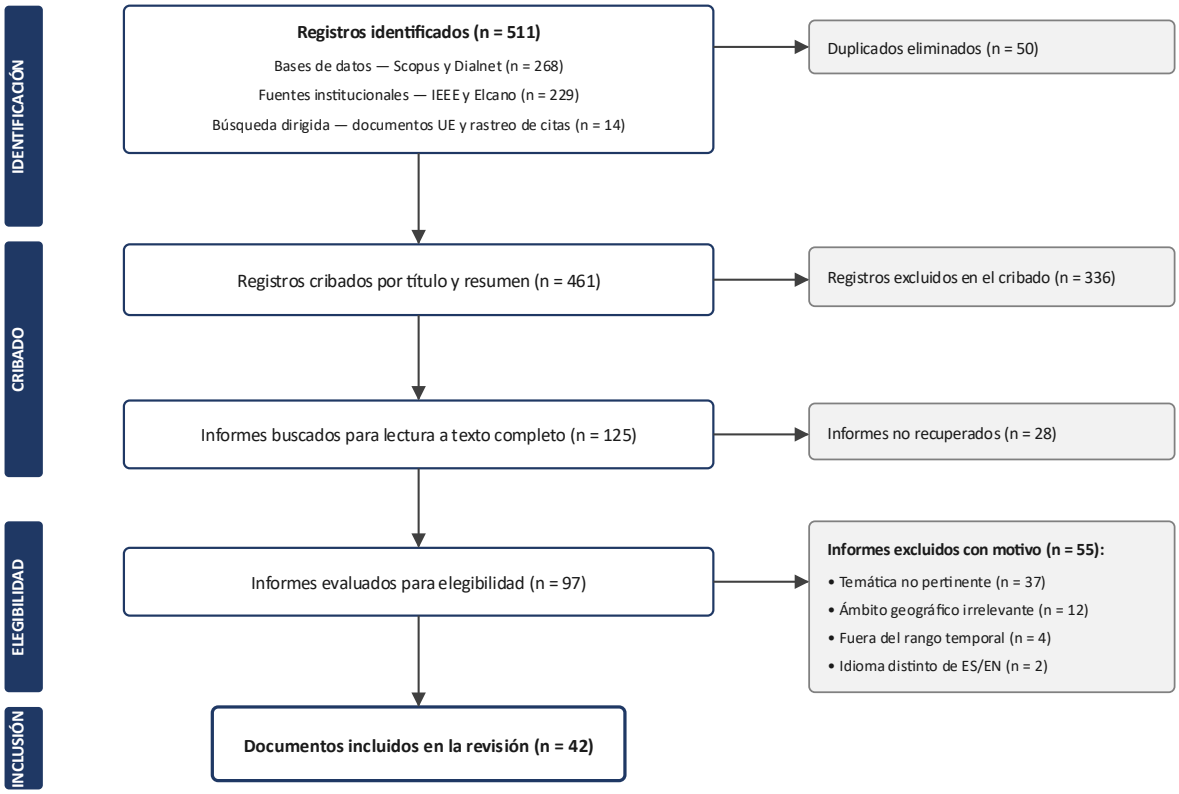


Figura 1 - *Diagrama de flujo del proceso de selección de fuentes (PRISMA 2020 adaptado).*
Fuente: elaboración propia.

1.5. Caracterización del conjunto de fuentes incluido en la revisión

Una vez aplicado el proceso de selección descrito, resulta pertinente caracterizar el conjunto de documentos incluidos antes de proceder a su análisis. Estas fuentes se enumeran en la tabla 3.

Referencia (APA 7)	Tipología	Idioma	Periodo	Geografía	Eje temático
Anagnostakis, D.(2025)	Académico	Inglés	2022-2026	Transversal	Arquitectura comunitaria
Arco Escriche, I. (2026)	Institucional	Español	2022-2026	China	Amenazas
Aznar Fernández-Montesinos, F. (2023)	Académico	Español	2022-2026	Transversal	Evolución conceptual
Barras Tejudo, R. y García Cantalapiedra, D. J. (2020)	Institucional	Español	2019-2021	Flanco sur	Amenazas

Referencia (APA 7)	Tipología	Idioma	Periodo	Geografía	Eje temático
Benedicto, M. Á. (2025)	Académico	Español	2022-2026	Transversal	Arquitectura comunitaria
Borghoff, U. M., Berger, L., y Fischer, F. (2024)	Académico	Inglés	2022-2026	Transversal	Propuestas
Camarero Orive, A. (2026)	Institucional	Español	2022-2026	Transversal	Amenazas
Colom Piella, G. (2019)	Institucional	Español	2019-2021	Transversal	Evolución conceptual
Colom Piella, G. (2023)	Académico	Español	2022-2026	Rusia	Amenazas
Colom Piella, G. (2026)	Institucional	Español	2022-2026	Transversal	Evolución conceptual
Dezcallar, J. (2022)	Libro / memoria	Español	2022-2026	Transversal	Evolución conceptual
Díaz-Caneja, J. M. (2014)	Institucional	Español	2014-2018	Transversal	Arquitectura comunitaria
Fägersten, B. (2016)	Institucional	Inglés	2014-2018	Transversal	Carencias / propuestas
Forti, M. (2023)	Académico	Inglés	2022-2026	Transversal	Amenazas
Freedman, J., Gjørv, G. H., y Razakamaharavo, V. T. (2021)	Académico	Español	2019-2021	Transversal	Evolución conceptual
Geri, M. (2024)	Académico	Inglés	2022-2026	Rusia	Amenazas
Giannopoulos, G., Smith, H., y Theocharidou, M., (Eds.) (2021)	Institucional	Inglés	2019-2021	Transversal	Evolución conceptual
González López, D. (2024)	Académico	Español	2022-2026	Transversal	Propuestas

Referencia (APA 7)	Tipología	Idioma	Periodo	Geografía	Eje temático
Molina Urosa, M., Lafuente Capó, J., Lopera Rodríguez, M., Ruiz Sancho, L., Terrés Pueyo, G., y García Hernández, P. (2026)	Institucional	Español	2022-2026	Rusia	Amenazas
Navarro Paredes, Á. (2026)	Institucional	Español	2022-2026	Transversal	Propuestas
Niinistö, S. (2024)	Institucional	Inglés	2022-2026	Transversal	Carencias / propuestas
Nilsson, N., Weissmann, M., y Palmertz, B. (2026)	Académico	Inglés	2022-2026	Transversal	Evolución conceptual
Páramo, A. (2022)	Institucional	Español	2022-2026	Transversal	Evolución conceptual
Quiñones de la Iglesia, F. J. (2020)	Institucional	Español	2019-2021	Transversal	Evolución conceptual
Rodríguez, Á. y Solé, J. (2025)	Institucional	Inglés	2022-2026	Flanco sur	Amenazas
Sánchez Herráez, P. (2021)	Institucional	Español	2019-2021	Transversal	Evolución conceptual
Sánchez Peláez, L. (2021)	Tesis doctoral	Español	2019-2021	Transversal	Arquitectura comunitaria
Sansó-Rubert Pascual, D. (2025)	Académico	Español	2022-2026	Flanco sur	Amenazas
Terrero Carrobles, J. J. (2025)	Institucional	Español	2022-2026	Rusia	Amenazas
Trujillo Álvarez, P. (2024)	Académico	Español	2022-2026	Transversal	Evolución conceptual
Tuinier, D. H. (2025)	Tesis doctoral	Inglés	2022-2026	Transversal	Carencias / propuestas
Weissmann, M. (2023)	Académico	Inglés	2022-2026	China	Amenazas

Referencia (APA 7)	Tipología	Idioma	Periodo	Geografía	Eje temático
Comisión Europea (2020)	Institucional	Español	2019-2021	Transversal	Arquitectura comunitaria
Comisión Europea y Alta Representante (2016)	Institucional	Español	2014-2018	Transversal	Arquitectura comunitaria
Comisión Europea y Alta Representante (2018)	Institucional	Español	2019-2021	Transversal	Arquitectura comunitaria
Consejo de la Unión Europea (2022a)	Institucional	Español	2022-2026	Transversal	Arquitectura comunitaria
Consejo de la Unión Europea (2022b)	Institucional	Español	2022-2026	Transversal	Arquitectura comunitaria
Consejo de la Unión Europea (2026)	Institucional	Español	2022-2026	Transversal	Arquitectura comunitaria
Servicio Europeo de Acción Exterior (2015)	Institucional	Inglés	2014-2018	Transversal	Arquitectura comunitaria
Servicio Europeo de Acción Exterior (2025)	Institucional	Inglés	2022-2026	Transversal	Arquitectura comunitaria
Servicio Europeo de Acción Exterior (2026)	Institucional	Inglés	2022-2026	Transversal	Arquitectura comunitaria
Unión Europea y Organización del Tratado del Atlántico Norte (2023)	Institucional	Inglés	2022-2026	Transversal	Arquitectura comunitaria

Tabla 3 - *Caracterización del corpus según PRISMA adaptado.*
Fuente: elaboración propia.

A título meramente ilustrativo, los datos numéricos más llamativos son los siguientes: aproximadamente el 60% de los documentos tienen origen institucional, mientras que un 30% son artículos académicos. Por otro lado, por ámbito temporal, casi el 70% de ellos fueron publicados a partir de 2022. Los siguientes párrafos profundizan en estas cuestiones.

La distribución temporal y tipológica merece, por presentar números más rotundos, ser analizada en primer lugar. Como se ha señalado, las fuentes analizadas se concentran en el

periodo 2022-2026 y hay un predominio notable de las institucionales sobre las académicas. En opinión del autor, esto se debe a que la reflexión sobre inteligencia y amenazas híbridas es un campo reactivo y en construcción, impulsado más por la respuesta institucional a los acontecimientos recientes que por la existencia de tradición académica. En cuanto al periodo temporal, es probable que la invasión de Ucrania de 2022 haya propiciado un incremento de las publicaciones, tanto académicas como institucionales. Así, hay que reseñar que los documentos orientados a políticas europeas tienen más peso que los que realizan análisis teórico, lo que ha condicionado el particular marco teórico de este Trabajo.

La anexión de Crimea en 2014 y la posterior invasión de Ucrania en 2022 son, precisamente, los eventos que justifican que, de entre los documentos que se ciñen a un ámbito geográfico concreto, los dedicados a Rusia tengan un mayor peso, lo que explica una mayor proliferación de literatura acerca de esta amenaza. La distribución la completan, por orden, el flanco sur y China. La mayor parte del corpus, no obstante, es transversal en lo geográfico, pues corresponde al análisis del actor de inteligencia atípico que es la Unión Europea y a las respuestas que está ofreciendo.

Terminada esta somera caracterización de las fuentes, el documento continúa con la conceptualización necesaria en el ámbito de estudio.

2. Marco teórico

Como paso previo a la revisión del estado de la cuestión, y entendiendo que la complejidad del tema objeto de estudio requiere de la definición de un marco conceptual sobre el que basar cualquier análisis posterior, se dedican los siguientes apartados a dos cuestiones fundamentales. La primera de ellas es la definición, en sentido amplio, de las amenazas híbridas; la segunda, la adaptación de la inteligencia para hacer frente a dichas amenazas.

2.1. Concepto y evolución de las amenazas híbridas

La comprensión de los desafíos actuales para la seguridad europea exige la superación de los esquemas de análisis concebidos durante la Guerra Fría y que seguían constituyendo el marco de referencia hasta los primeros años del presente siglo. En este sentido, el denominador común que la literatura especializada coincide en señalar como rasgo definitorio del

panorama estratégico actual es, de manera muy simplificada, la difuminación de las fronteras tradicionales del conflicto.

2.1.1. La superación de las taxonomías convencionales

El estudio de la guerra se ha apoyado durante siglos en un repertorio de distinciones binarias —guerra y paz, combatiente y civil, fuerza regular y fuerza irregular, actor estatal y actor no estatal, frente interior y frente exterior— que ordenaban tanto el análisis del fenómeno bélico como la respuesta jurídica e institucional ante él. Ese armazón conceptual, heredado en buena medida del orden westfaliano y depurado por la tradición clausewitziana, presupone unos umbrales nítidos: un momento identificable en que se transita de la paz a la guerra y categorías estancas que permiten clasificar a los contendientes y aplicarles el marco correspondiente. La premisa de este trabajo, que es también el punto de partida de cualquier aproximación a las amenazas híbridas, es que ese enfoque ha perdido buena parte de su capacidad descriptiva; no porque haya dejado de existir, sino porque el adversario contemporáneo opera, precisamente, en las costuras que esas categorías dejan al descubierto.

Conviene matizar, no obstante, que la novedad es relativa. Como recuerda Sánchez Herráez (2021), resulta difícil no identificar elementos "híbridos", en distinto grado, en la mayoría de los conflictos de cierta magnitud del pasado: la Segunda Guerra Mundial, paradigma aparente del enfrentamiento convencional, combinó fuerzas regulares e irregulares, campañas intensísimas de propaganda y desinformación y el recurso deliberado al terror sobre la población, del mismo modo que las guerras de desintegración de Yugoslavia exhibieron ya, de forma notoria, ese entrelazamiento de planos. Lo verdaderamente nuevo no es la combinación de medios, sino su amplificación: la globalización, la hiperconectividad y la digitalización han multiplicado el alcance y la eficacia de unas prácticas tan antiguas como el propio conflicto, hasta el punto de que la literatura habla ya, sin metáforas, de una zona crepuscular entre la guerra y la paz (Giannopoulos et al., 2021).

A este respecto, la transformación decisiva no afecta solo a la naturaleza de la guerra, sino también, y es esto lo que más desafía a las clasificaciones heredadas, a la naturaleza de la paz. Cada vez con mayor frecuencia, la situación no es de guerra declarada ni de paz efectiva, sino de un espacio intermedio entre ambas (la llamada zona gris), de límites difusos, poblado de paradojas y de ambigüedad calculada, en el que la duda sobre cómo responder forma parte

fundamental del propio diseño de la agresión (Sánchez Herráez, 2021). De hecho, esa ambigüedad no es un efecto colateral, sino un instrumento: el actor hostil manipula deliberadamente los umbrales de detección, dificulta la atribución y explota la dificultad de los Estados democráticos para activar sus mecanismos de respuesta ante acciones que, aisladamente consideradas, pueden no ser siquiera ilícitas (Giannopoulos et al., 2021).

La propia proliferación terminológica es, en sí misma, síntoma de esa "crisis" taxonómica. En las últimas décadas se han acuñado etiquetas tan diversas como guerra de cuarta generación, nuevas guerras, guerra asimétrica, guerra compuesta, guerra no lineal o actividad en la zona gris, algunas de raíz occidental y otras de procedencia rusa o china; pero todas ellas con la pretensión de designar un fenómeno que se resiste a la clasificación (Giannopoulos et al., 2021). Esta acumulación de términos no es sólo una cuestión académica: revela que ninguna de las categorías al uso captura por sí sola un objeto cuya seña de identidad es, justamente, difuminar las dicotomías sobre las que se construyó el pensamiento estratégico moderno.

Cabe señalar, sin embargo, un riesgo que conviene no perder de vista. El afán por encajar cada situación en una categoría exacta, a fin de aplicarle la "receta" correspondiente del manual o algoritmo, supone en buena medida una vuelta al álgebra de la acción que Clausewitz reprochaba a sus contemporáneos (Sánchez Herráez, 2021). Así pues, más que una nueva taxonomía cerrada, lo que la superación de las categorías convencionales reclama es un marco analítico flexible, capaz de cartografiar relaciones —actores, instrumentos, dominios, fases— sin la pretensión de fijar fronteras estancas. Es sobre ese presupuesto sobre el que se asienta el concepto de guerra híbrida que se aborda a continuación.

2.1.2. El concepto de la guerra híbrida

La formulación canónica del concepto de "guerra híbrida" se debe a Hoffman (2007), quien sostuvo que la letalidad de esta forma de conflicto no reside simplemente en el empleo aislado de distintas "maneras de hacer la guerra", sino en su convergencia simultánea. Conforme a esta definición, la guerra híbrida es aquella que incorpora y coordina en un mismo espacio de batalla capacidades convencionales, formaciones irregulares, actos de terror o coerción e incluso el desorden criminal, con el propósito de alcanzar una sinergia operativa que ninguno de esos elementos lograría por separado. En su planteamiento inicial, Hoffman tenía presentes sobre todo a los actores no estatales capaces de combinar lo táctico y lo operacional con una sofisticación hasta entonces reservada a los ejércitos regulares.

La constatación empírica de este modelo teórico no tardó en materializarse. El conflicto del Líbano de 2006 se erigió en el caso paradigmático de esa fusión de métodos cinéticos y no cinéticos. Allí, Hizbulá demostró la capacidad de operar como una insurgencia tecnológicamente avanzada: el empleo de misiles guiados y de medios de inteligencia de señales (SIGINT) se entrelazó con una cuidada gestión de la narrativa informativa. De aquella experiencia la literatura posterior extrajo una lección que excede el plano estrictamente militar, y sobre la que se volverá más adelante: en el entorno contemporáneo, la gestión de la percepción puede resultar tan decisiva como el control del terreno físico, si no más.

Ahora bien, la idea acuñada por Hoffman, de raíz eminentemente militar, pronto se reveló insuficiente para abarcar un fenómeno que desbordaba el campo de batalla. De ahí que la literatura institucional, y en particular el modelo conceptual del Joint Research Centre y el Hybrid CoE, optara por reservar el término “guerra híbrida” para una modalidad concreta de actividad y emplear “amenaza híbrida” como concepto paraguas, más amplio, que engloba la interferencia, la influencia, las operaciones, las campañas y la propia guerra (Giannopoulos et al., 2021). A diferencia de las amenazas tradicionales, las híbridas así entendidas operan en la zona gris entre la paz y la guerra (cuyo análisis se aborda en el apartado siguiente) y se sirven de la apertura misma de los procesos democráticos para comprometer los valores que los sustentan.

Lo que confiere carácter híbrido a una acción no es, por tanto, ningún medio aislado, sino la intencionalidad maliciosa que la anima, que Giannopoulos et al. (2021) caracterizan mediante los rasgos siguientes:

- Sincronización de múltiples herramientas, en principio no militares, para generar efectos lineales y no lineales.
- Creación de ambigüedad, mediante el encubrimiento y la negación plausible, y ocultación de la intención real.
- Manipulación deliberada de los umbrales de detección y respuesta, con el fin de permanecer por debajo de ellos y no desencadenar la reacción del adversario.
- Explotación de las fisuras de la sociedad democrática y de los conflictos entre jurisdicciones.

- Recurso frecuente a elementos de distracción, de modo que la acción se ejecuta en un lugar mientras el objetivo real se sitúa en otro.

Sobre esa base, el modelo se articula en torno a cuatro pilares —actores, instrumentos, dominios y fases— cuya interrelación permite reconstruir la lógica de una campaña híbrida. En cuanto a los dominios, la publicación identifica trece áreas en las que las amenazas pueden materializarse: infraestructura, ciberespacio, espacio ultraterrestre, economía, defensa, cultura, sociedad, administración pública, ámbito jurídico, inteligencia, diplomacia, política e información (Giannopoulos et al., 2021). Conviene señalar, por último, una precisión de orden analítico: un ataque dirigido contra un dominio determinado persigue a menudo, por efecto cascada, un objetivo situado en otro distinto, lo que dificulta tanto su detección como la correcta atribución de su propósito.

2.1.3. La zona gris y la dimensión cognitiva

Si bien el planteamiento inicial de Hoffman (2007) ponía el acento en el campo de batalla táctico, la evolución del conflicto en la última década ha desplazado su centro de gravedad hacia las dimensiones no físicas. A este respecto, el modelo conceptual propuesto por el Centro de Excelencia para la Lucha contra las Amenazas Híbridas (Giannopoulos et al., 2021) constata que la amenaza contemporánea se dirige, primordialmente, contra la estabilidad institucional y la cohesión de las sociedades democráticas.

En consecuencia, el análisis debe incardinarse en el concepto de "zona gris" (Aznar Fernández-Montesinos, 2023). Este constructo teórico define el espacio de rivalidad situado entre la paz y el conflicto armado abierto, donde actores estatales emplean la coerción económica, el *lawfare*, la instrumentalización de flujos migratorios o el ciberespacio para alterar el *statu quo* geopolítico. Su particularidad —y, por tanto, la dificultad para hacerle frente— radica en que esta ambigüedad calculada (Colom Piella, 2019) permite a dichos actores operar por debajo del umbral que desencadenaría una respuesta militar convencional por parte de la Alianza Atlántica o la Unión Europea.

Para comprender la vulnerabilidad de las democracias liberales ante este fenómeno de la zona gris, resulta especialmente útil recuperar la tradicional tríada clausewitziana —Política, Ejército y Ciudadanía— y observar su evolución en el complejo ecosistema del siglo XXI (Trujillo Álvarez, 2024). Habida cuenta de la superioridad militar convencional de Occidente,

los actores revisionistas dirigen hoy su esfuerzo hacia el vértice de la ciudadanía. Mediante operaciones de Manipulación de la Información e Injerencia Extranjera (FIMI, por sus siglas en inglés), actores como Rusia o China buscan incrementar la polarización social y minar la credibilidad institucional, fracturando así el centro de proyección del poder del Estado sin necesidad de recurrir al *hard power* (Servicio Europeo de Acción Exterior, 2026).

La principal materialización de este asedio al vértice ciudadano se produce en el dominio cognitivo. Las actividades de desinformación, lejos de operar como meros vectores de distracción táctica, atacan directamente la identidad colectiva (Freedman et al., 2021). De este modo, el entorno híbrido configura un escenario donde la distinción entre el estado de paz y el de guerra se ha diluido, exigiendo una adaptación perentoria de la respuesta occidental a este fenómeno.

2.2.El papel de la inteligencia frente a las amenazas híbridas

La mutación del entorno estratégico descrita en el epígrafe anterior hace necesaria una revisión ineludible del papel tradicional de los servicios dedicados a hacer frente a este fenómeno. Durante décadas, el ciclo de inteligencia clásico ha operado bajo un paradigma de raíz westfaliana, orientado de manera casi exclusiva a calibrar las capacidades militares convencionales y las intenciones políticas de actores estatales soberanos en un contexto nítido de paz o guerra. Sin embargo, la zona gris contemporánea quiebra esta lógica binaria al configurarse, como advierte Colom Piella (2026), no como un mero espacio intermedio de hostilidad de baja intensidad, sino como un verdadero régimen de escalada. A este respecto, Nilsson et al. (2026) denominan a estas amenazas "problemas perversos" (*wicked problems*) por diseño estratégico: el agresor estructura sus acciones de forma intencionadamente ambigua para difuminar la distinción entre paz y guerra, operando por debajo de los umbrales de detección y respuesta del objetivo. En consecuencia, las herramientas tradicionales de obtención y análisis resultan insuficientes cuando el adversario no busca la destrucción cinética, sino la parálisis estratégica del decisor mediante la explotación de sus propias vulnerabilidades institucionales.

Ante este escenario de ambigüedad calculada, la función primordial de la inteligencia se desplaza necesariamente desde la gestión de la certeza hacia la gestión de la incertidumbre. La doctrina tradicional, habituada a reaccionar ante indicadores de despliegue militar

observables, resulta ineficaz cuando las acciones híbridas se ejecutan de manera dispersa y diluida en el tiempo. Por ello, cobra un protagonismo central la capacidad de anticipación mediante la alerta temprana. Como señala Navarro Paredes (2026), hacer frente a la "hibridez estratégica" exige el diseño y la adopción de modelos predictivos tempranos que permitan identificar las anomalías en dominios no militares antes de que estas devengan en una crisis abierta o en un daño irreversible para la seguridad nacional. La inteligencia, por tanto, debe verse reforzada como un mecanismo de detección precoz de la intencionalidad hostil.

Es importante subrayar que el núcleo de la efectividad de las estrategias híbridas reside en la negación plausible y el encubrimiento de la autoría. Así, Giannopoulos et al. (2021) destacan que el actor hostil manipula deliberadamente los umbrales de detección y fragmenta sus acciones a través de intermediarios (*proxies*) o de herramientas en apariencia inocuas (como transacciones económicas o campañas de opinión) para evitar la autoría directa. En este sentido, la atribución se convierte en el principal desafío político y técnico para los servicios de inteligencia. Colom Piella (2026) subraya que retrasar o imposibilitar dicha atribución es un fin en sí mismo para el agresor, ya que la falta de pruebas concluyentes bloquea el consenso político necesario para activar mecanismos de defensa colectiva o imponer sanciones jurídicas. Desentrañar esta opacidad exige un esfuerzo analítico superior, capaz de conectar indicios inconexos para demostrar la intencionalidad maliciosa que subyace a una campaña coordinada.

Habida cuenta de que las amenazas híbridas se despliegan simultáneamente a lo largo de los trece dominios identificados por la literatura institucional —que abarcan desde el ciberespacio y la economía hasta la administración pública y la cultura—, la inteligencia actual no puede continuar compartimentada en estructuras estancas. El análisis contemporáneo requiere una profunda integración de la inteligencia civil y la militar y una aproximación integral que supere la dicotomía entre seguridad interior y exterior. Asimismo, este entorno hiperconectado obliga a modificar el peso de las disciplinas de obtención. Si bien el secreto de Estado sigue existiendo, la mayor parte de los vectores de interferencia híbrida (como las operaciones FIMI o los ciberataques contra infraestructuras críticas) operan en entornos públicos o redes abiertas.

Por consiguiente, la explotación sistemática de fuentes abiertas (OSINT, por sus siglas en inglés) pasa de ser un complemento secundario a constituir la base fundamental sobre la que

construir el conocimiento estratégico, combinándose con la inteligencia de señales (SIGINT) y la de fuentes humanas (HUMINT). Esta realidad impulsa un cambio conceptual hacia la "coproducción" de inteligencia. Nilsson et al. (2026) subrayan que el conocimiento ya no es monopolio exclusivo del Estado, sino una práctica interactiva que requiere nutrirse del sector privado y de la sociedad civil, como demuestran organizaciones como Bellingcat en la identificación de operaciones hostiles o los actores corporativos en la atribución de ciberataques.

Esta transición hacia un entorno saturado de información replantea por completo el perfil y las competencias de la figura del analista. El reto ya no es la escasez de datos, sino la intoxicación y el volumen masivo de los mismos, un fenómeno exponencialmente multiplicado por la irrupción de la Inteligencia Artificial generativa. Siguiendo los planteamientos de Páramo (2022), el analista de última generación debe actuar en simbiosis con las herramientas tecnológicas, empleando la automatización y el procesamiento de datos masivos no para delegar el juicio crítico, sino para cribar el ruido informativo. La función del analista se desplaza, así, hacia la deconstrucción de narrativas complejas y operaciones de desinformación, un cometido donde el factor humano, la comprensión del contexto cultural y el sesgo analítico siguen siendo determinantes frente al determinismo tecnológico (Páramo, 2022).

Por otro lado, la inteligencia asume un papel central en la comunicación estratégica del Estado para contrarrestar la desinformación y disuadir al agresor. Casos recientes, como la rápida desclasificación de información durante la investigación del incidente Skripal en 2018 o la publicación sistemática de inteligencia por parte de Estados Unidos y el Reino Unido en los meses previos a la invasión rusa de Ucrania en 2022, evidencian cómo el uso público y previsor de la inteligencia permite a las democracias disputar la narrativa, arrebatar la iniciativa al adversario y preparar a la opinión pública frente a crisis inminentes.

Como conclusión a este apartado, la inteligencia en el siglo XXI constituye una herramienta fundamental de defensa de las democracias liberales ante las agresiones asimétricas. Lejos de limitarse a la mera recolección de secretos, el analista afronta hoy el reto de desentrañar una ambigüedad deliberada; frente a un volumen masivo de datos, su función primordial se desplaza hacia la generación de una alerta temprana que permita a los decisores políticos romper la inercia y recuperar la iniciativa estratégica. Para operativizar esta función en el

contexto actual, Nilsson et al. (2026) proponen el *Intelligence Analysis Interaction Model*, el cual ilustra que este flujo de conocimiento e información debe estructurarse de forma bidireccional entre las agencias y los diversos actores sociales.

El principal "cuello de botella" de este modelo radica en la capacidad de la inteligencia para agregar análisis complejos y diseminarlos de manera adaptada hacia receptores que escapan al perfil del consumidor tradicional de inteligencia (el decisor político), tales como operadores de infraestructuras críticas, instituciones académicas o gobiernos locales. Contrarrestar las amenazas híbridas exige, por tanto, un verdadero enfoque de "toda la sociedad" (*whole-of-society approach*), donde la comunidad de inteligencia actúe no solo como un escudo gubernamental, sino como un elemento habilitador y catalizador que dote a la sociedad civil del conocimiento contrastado necesario para salvaguardar la cohesión social y la credibilidad institucional. No obstante, el análisis crítico exigible hace necesario tratar las contrapartidas de este enfoque. Y es que, por un lado, no resulta difícil concebir que la cultura del secreto propia de los servicios de inteligencia respecto a la sociedad civil pueda generar tensiones a la hora de concretar este planteamiento; por otra parte, se corre el riesgo de trasladar a la sociedad civil una carga de verificación que no le corresponde[1].

Una vez delimitadas estas necesidades conceptuales, resulta preceptivo examinar en qué medida la arquitectura institucional y los mecanismos de cooperación vigentes en el seno de la Unión Europea están capacitados para dar cumplimiento a estas exigencias doctrinales.

3. Desarrollo

A lo largo de las siguientes páginas, se analiza la problemática presentada en la primera sección del documento. Para ello, se realiza un recorrido que empieza con el diagnóstico del escenario actual, para estudiar a continuación la respuesta existente, sus límites y sus alternativas, terminando con una ponderación del conjunto de fuentes seleccionadas.

[1] El debate acerca del control estatal de la información excede el ámbito de este trabajo, por lo que no se ha ahondado en esta cuestión.

3.1. Los retos para la seguridad europea: el escenario actual

Como se anunciaba en el párrafo anterior, este desarrollo comienza con la determinación de las tres amenazas prioritarias para la seguridad europea en el ámbito híbrido: las acciones rusas, orquestadas cuidadosamente; la amenaza difusa y multiactor del flanco sur; la progresiva influencia china. El apartado cierra con una tabla que sintetiza las particularidades de los tres actores citados.

3.1.1. Rusia y sus *proxies*

Rusia se ha consolidado en la última década como el adversario híbrido por excelencia y la principal amenaza que emplea métodos no convencionales para la seguridad de Europa. En la práctica, la estrategia de Moscú representa la puesta en práctica de los conceptos fundamentales del marco teórico de la zona gris: el despliegue de un repertorio sincronizado y persistente de instrumentos estatales y no estatales, concebido para operar por debajo del umbral que desencadenaría una respuesta armada convencional u obligaría a la activación de mecanismos de defensa colectiva. En esta evolución, el inicio de la invasión a gran escala de Ucrania en 2022 supuso un punto de inflexión significativo, marcando la transición de Moscú hacia una mayor osadía y agresividad en sus operaciones encubiertas en territorio europeo. Según Colom Piella (2026), esta aproximación desdibuja intencionadamente el umbral del conflicto mediante una coerción acumulativa que busca paralizar la toma de decisiones occidental. Asimismo, esta amalgama táctica ejemplifica con exactitud el modelo conceptual trazado por Giannopoulos et al. (2021), en el que la amenaza híbrida se define por la sincronización de múltiples dominios para generar ambigüedad y explotar las vulnerabilidades democráticas. En términos clausewitzianos, estas acciones conforman un ataque dirigido específicamente contra el vértice de la ciudadanía.

La dimensión cognitiva: FIMI y desinformación

La dimensión cognitiva constituye una de las principales líneas de acción de la estrategia híbrida rusa y un vector al que Moscú destina una cantidad considerable de recursos. A través de operaciones FIMI, Rusia dirige su esfuerzo hacia la injerencia en los procesos electorales, el fomento deliberado de la polarización en las sociedades europeas y el ataque directo a la cohesión social. Tal y como advierte el informe del Servicio Europeo de Acción Exterior (2026), el aparato ruso orienta sus tácticas a fracturar el centro de gravedad de las democracias

liberales minando la credibilidad institucional. Esta manipulación sostenida de la identidad y la estabilidad encuentra su respaldo analítico en Freedman et al. (2021), quienes la identifican como una amenaza central para la seguridad contemporánea.

Al analizar la doctrina subyacente a esta ofensiva cognitiva, resulta conveniente tomar con cautela y rigor analítico la frecuentemente citada "doctrina Gerasimov". Gran parte de la literatura especializada contemporánea ha desmontado el mito de que el famoso artículo publicado por Valery Gerasimov en 2013 constituyera un manual estratégico ofensivo de Rusia. Al contrario, el texto original describía la praxis híbrida que Moscú atribuía a las potencias occidentales en el marco de las llamadas "Revoluciones de Colores". Como señala con acierto Colom Piella (2023) al diseccionar el pensamiento militar ruso, comprender este sesgo perceptivo es vital: Moscú no concibe inicialmente sus operaciones en la zona gris como una agresión unilateral, sino como una defensa activa y preventiva frente a lo que percibe como un asedio subversivo de Occidente.

El reto fundamental de detección que plantean las operaciones FIMI no radica en la escasez o el secretismo de la información, sino en la intoxicación y el volumen masivo de datos que saturan el dominio cognitivo. Al operar en entornos públicos, redes abiertas y a través de herramientas comunicativas en apariencia inocuas, el actor hostil manipula deliberadamente los umbrales de detección. De este modo, la amenaza se diluye entre el flujo de información cotidiana, difuminando la línea que separa una campaña orquestada de injerencia extranjera del libre ejercicio de la opinión ciudadana. Este escenario exige que el analista de inteligencia desplace su foco hacia la deconstrucción de narrativas complejas y el cribado del ruido informativo para detectar la intencionalidad maliciosa subyacente.

Coerción e instrumentalización de la migración y la energía

El segundo bloque de actuación rusa se fundamenta en la coerción y la instrumentalización táctica, un ámbito en el que la participación de sus aliados o *proxies* resulta determinante. Un ejemplo empírico palmario de esta dinámica fue la crisis migratoria desatada entre 2021 y 2022 en la frontera oriental de la Unión Europea, donde Bielorrusia operó como un Estado-instrumento al servicio de una estrategia de presión coercitiva. La facilitación de flujos migratorios irregulares hacia Lituania, Letonia y Polonia fue diseñada para tensionar los marcos legales de asilo y las capacidades de recepción europeas, un fenómeno ampliamente documentado por Forti (2023).

En paralelo, la instrumentalización de los suministros energéticos se vislumbra como otra herramienta coercitiva impulsada con frecuencia por el Kremlin, cuyo uso se ha intensificado tras las sanciones impuestas por la guerra en 2022. Rusia ha explotado el suministro de gas como un arma geopolítica para fracturar el consenso político de la Unión Europea. Siguiendo a Geri (2024), esta faceta de la guerra híbrida en el sector energético ilustra una constante metodológica: el actor hostil identifica una dependencia estructural o una vulnerabilidad legal y ejerce una presión significativa sobre ella, pero manteniéndose siempre un paso por detrás de la confrontación bélica directa.

En este ámbito, los principales retos para la comunidad de inteligencia son la atribución de un acto específicamente concebido para preservar la negación plausible de su autor y la detección de la manipulación del discurso dirigido a la sociedad. Al instrumentalizar actores interpuestos (*proxies* como Bielorrusia) o enmascarar la presión bajo aparentes disputas comerciales o crisis humanitarias, el agresor crea una zona de ambigüedad calculada. En este sentido, retrasar o imposibilitar la atribución no es una cuestión casual, sino un fin estratégico en sí mismo para el actor hostil. Al carecer de pruebas concluyentes y unívocas sobre la autoría y la intencionalidad, se paraliza la toma de decisiones occidental y se bloquea el consenso político indispensable para activar mecanismos de defensa colectiva o imponer un régimen de sanciones.

La acción física y clandestina: sabotaje y espionaje

En el extremo más tangible del espectro híbrido se sitúan las acciones físicas y clandestinas, cuya frecuencia e intensidad han experimentado un incremento constatable tras el inicio del conflicto en Ucrania en 2022. La interferencia dirigida contra infraestructuras críticas europeas ilustra una evolución hacia métodos de mayor repercusión física dentro de una estrategia de influencia y coacción en la que las acciones deliberadas se diluyen y entremezclan con sucesos fortuitos o sin pruebas sobre su autoría. Los incidentes registrados en el mar Báltico y otras regiones de Europa del Norte entre 2024 y 2025 —tales como los cortes en cables submarinos de telecomunicaciones y energía, las perturbaciones recurrentes en las señales de posicionamiento GPS que afectan a la aviación civil, o los incendios de origen no esclarecido en instalaciones logísticas e industriales de carácter estratégico— configuran un patrón de disrupción directa en sectores clave para el funcionamiento de los Estados afectados.

Como ejemplos más reseñables, relacionados principalmente con las telecomunicaciones y la energía, conviene rescatar los casos de las explosiones de los gasoductos Nord Stream 1 y 2 en 2022 (cuya autoría sigue sin esclarecerse a día de hoy, tras sospechas iniciales que apuntaban a Rusia y que posteriormente tornaron hacia actores ucranianos) o el corte de cinco cables submarinos —entre ellos, la interconexión EstLink 2—, en esta ocasión por parte del petrolero *Eagle S*, vinculado a la flota fantasma rusa. Sin embargo, incluso en este segundo episodio, en el que el grado de certeza es mayor, las limitaciones de la jurisdicción finlandesa impiden conclusiones claras y determinar si hubo intencionalidad (de hecho, la falta de jurisdicción resultó en el archivo de la causa, archivo que ha sido recurrido por la fiscalía); aunque la presencia de equipos de contraespionaje durante los siete meses necesarios para su reparación refuerza la tesis de que se trató de un acto intencionado (Molina Urosa et al., 2026).

Como defienden estos mismos autores en su estudio sobre la vulnerabilidad estructural y la competición geopolítica en el espacio marítimo del Báltico, la eficacia de estas acciones no reside en su potencial destructivo absoluto, sino en su origen y su diseño: la viabilidad de plantear un sabotaje deliberado de tal manera que pueda ser razonablemente interpretado como un accidente marítimo, un fallo técnico casual o un impacto ambiental común (por ejemplo, el arrastre de un ancla o redes de pesca). Esta calculada ambigüedad en el origen del daño es la que sostiene la negación plausible por parte del actor hostil y bloquea los mecanismos normativos e institucionales de atribución. Al dilatar la obtención de una certeza probatoria, se ralentiza o paraliza la adopción de contramedidas políticas, legales o de defensa colectiva, lo que constituye la esencia misma de la actividad en la zona gris y el caso paradigmático del reto analítico que estas agresiones plantean a los servicios de inteligencia.

A esta amenaza a las infraestructuras se añade la metamorfosis que ha experimentado el aparato de espionaje ruso en Europa tras la ola de expulsiones masivas de diplomáticos y agentes encubiertos en 2022. Al perder sus redes de inteligencia tradicionales, Moscú se ha visto forzado a reinventar su *modus operandi*. Tal y como documenta Terrero Carrobles (2025), esta adaptación se ha materializado en el uso intensivo de aplicaciones de mensajería (como Telegram) para el reclutamiento de ciudadanos europeos de bajo perfil, empleados como “agentes desechables” para labores de vigilancia o pequeños sabotajes. Esta táctica

descentralizada abarata los costes operativos, diluye el rastro de atribución y satura los servicios de contrainteligencia occidentales.

La necesidad de una visión de conjunto

En definitiva, la gravedad del desafío que plantea Rusia no radica en el impacto aislado de cada una de estas herramientas —desde un ciberataque hasta el corte de un gasoducto o la amplificación de una noticia falsa—, sino en el carácter sinérgico del conjunto. Es la orquestación de estas piezas soterradas y negables lo que otorga el carácter particular de esta amenaza para la seguridad europea. Y aquí radica precisamente la dificultad: tener la capacidad de detectar el conjunto más allá de sus piezas aisladas. Al explotar las fronteras entre lo civil y lo militar, y entre la seguridad interior y exterior, este repertorio híbrido impone la necesidad de superar los enfoques analíticos tradicionales, apuntando hacia el rediseño de la arquitectura de respuesta que se analizará en el próximo apartado.

3.1.2. El flanco sur: el Magreb y el Sahel

La región comprendida por los países situados al sur de Europa, cruzando el mar Mediterráneo, a la que es frecuente referirse como el "flanco sur", presenta una amenaza de naturaleza difusa y multiactor (en contraste con la orquestación rusa), que se sitúa en la intersección de dos realidades: la del Magreb, un vecino que mantiene una relación tensa con la Unión, y la del Sahel, una región periférica que se desmorona. No se trata, en este caso, de una campaña orquestada, sino de una zona de vulnerabilidad estructural que afrontan sobre todo los socios meridionales de la UE, con España en primera línea.

Para abordar los retos vinculados a esta área geográfica, se hace necesario dejar atrás el concepto MENA (*Middle East and North Africa*) acuñado por Estados Unidos en los años noventa y adoptar, como proponen Barras Tejudo y García Cantalapiedra (2020), la idea del "Gran Magreb", que se abordará más adelante; además de reconocer la importancia que tiene para la Unión Europea una región tan aparentemente remota como inestable: el Sahel, donde la simbiosis de amenazas ya conocidas adquiere una dimensión inédita. Por otro lado, la Estrategia de Seguridad Nacional española de 2021 ya asume el impacto de las amenazas provenientes de esta región, pero resulta imprescindible su incorporación a la agenda europea, algo que se consiguió parcialmente en 2022 con la inclusión del "flanco sur" en el nuevo Concepto Estratégico de la OTAN (Sansó-Rubert Pascual, 2025), pero que no se ha

trasladado formalmente al ámbito comunitario. Esto conduce a un análisis fuertemente condicionado por la perspectiva española, pero no debe olvidarse que las amenazas para la seguridad del país ibérico lo son para toda la Unión.

Marruecos, el "vecino incómodo"

El primer gran reto para la seguridad comunitaria no proviene de ningún adversario, sino de un socio revisionista —Rabat— que, como parte de su doctrina del "Gran Marruecos", cuestiona la soberanía española sobre las plazas de Ceuta y Melilla. Sin ánimo de entrar en debates jurídicos (totalmente fuera del ámbito de este trabajo), las Ciudades Autónomas tienen un valor geoestratégico fundamental para el control del Mar Mediterráneo y la gestión de las fronteras de la Unión Europea. Para Marruecos es, además, una cuestión de identidad nacional, lo que ha generado tensiones con España. Aquí, la principal amenaza para la seguridad europea la constituye, como señalan Rodríguez y Solé (2025), la instrumentalización de los flujos migratorios, siendo el episodio más representativo de este fenómeno el ocurrido en 2021, cuando 12 000 personas intentaron cruzar irregularmente la frontera con Ceuta. Los riesgos derivados de este tipo de acciones son variados, desde el desafío a la seguridad fronteriza hasta la generación de inestabilidad política y social en España, pasando por el cuestionamiento del modelo fronterizo y el respeto a los derechos humanos ante la opinión pública internacional. También pueden incluirse aquí, atendiendo a Sansó-Rubert Pascual (2025), otras medidas de presión como los cierres unilaterales de puestos fronterizos (con gran impacto para la economía local), la retirada de personal diplomático, la concesión de prospecciones en aguas en disputa, o el recurso sistemático al *lawfare* en relación con el contencioso del Sáhara Occidental y la manipulación del relato. Sin embargo, todas ellas son acciones plenamente justificables desde el lado marroquí y difícilmente imputables a una estrategia deliberada desde el punto de vista diplomático: es complicado acreditar la manipulación por parte de Marruecos de los flujos migratorios. En cuanto al resto de acciones, si bien en conjunto pueden esconder una determinada intencionalidad, no vulneran ninguna norma internacional.

La complejidad de la situación se ve acrecentada por las alianzas de uno y otro lado (Sansó-Rubert Pascual, 2025): la aplicación del artículo 5 de la OTAN queda claramente excluida por lo dispuesto en el artículo 6, pero lo recogido en el artículo 4 abre la puerta a una respuesta aliada. Por su parte, el Tratado de Lisboa fundamenta la defensa europea común. Sin embargo,

Marruecos mantiene alianzas estratégicas con Estados Unidos, Francia e Israel, lo que debilita la posición española y, en última instancia, la del conjunto de la Unión Europea.

Así pues, el reto de inteligencia está en la capacidad de anticipar flujos migratorios orquestados e interpretar la señalización coercitiva de un país que, formalmente, es un socio, no un enemigo. Todo ello en un contexto de debilidad en el seno de la Unión Europea, lastrada por sus divisiones internas. Frente a ella, un Marruecos con respaldo internacional que lleva a cabo acciones por debajo del umbral del conflicto armado que, por sí solas, es complicado categorizar como actos hostiles deliberados, pero que, en conjunto, configuran una presión deliberada.

Gibraltar y los *choke points*

El otro punto que enfrenta riesgos reseñables desde la perspectiva europea es el Estrecho de Gibraltar. Como señala Camarero Orive (2026), este accidente geográfico entre el océano Atlántico y el mar Mediterráneo soporta el paso de más de 120 000 buques anuales, constituyendo uno de los principales *choke points* mundiales. Se trata además de un espacio fuertemente militarizado, en el que confluyen la Base Naval de Rota y la presencia militar británica en el Peñón de Gibraltar. A esto debe añadirse que España importa más del 60% de su energía por vía marítima, lo que, unido a su capacidad de regasificación (más del 30% del total de la Unión Europea), pone de relieve el impacto que supondría la materialización de cualquier amenaza en este ámbito.

Tampoco conviene olvidar que, como ya se ha señalado con respecto al Mar Báltico, por el estrecho de Gibraltar discurren cables de comunicaciones, interconexiones eléctricas y gasoductos. Mediante el empleo de las mismas técnicas descritas por Molina Urosa et al. (2026) en lo referido a interferencias y la manipulación de señales GPS y AIS, una flota fantasma escondida en el constante tráfico marítimo del Estrecho tiene una nada desdeñable ventana de oportunidad para llevar a cabo acciones de gran impacto y difícilmente atribuibles.

La clave en este caso es la anticipación: cómo distinguir la actividad hostil, leer las señales hostiles de un socio, prever oleadas migratorias dirigidas, atribuir a un determinado buque una acción concreta o, simplemente, cómo identificar qué buques forman parte de una flota fantasma, son cuestiones que requieren propuestas audaces. Es decir, la capacidad de alerta temprana.

La inestabilidad del Sahel

Para completar este apartado, se dedicarán unas líneas al caso del Sahel, la región comprendida (atendiendo al G5 del Sahel) por Burkina Faso, Chad, Mali, Mauritania y Níger, además de otras zonas situadas entre el desierto del Sáhara y la sabana sudanesa. Tal y como señalan Barras Tejudo y García Cantalapiedra (2020), esta área geográfica se caracteriza por su estructura anárquica, su inestabilidad, la porosidad de sus fronteras, la debilidad de sus Estados y la institucionalización de la corrupción. Este panorama proporciona el caldo de cultivo perfecto para la simbiosis entre grupos terroristas —como Al Qaeda del Magreb Islámico (AQMI), el Estado Islámico del Gran Sáhara o Boko Haram— y la delincuencia transnacional dedicada al tráfico de drogas (provenientes de América del Sur a través de África Occidental) y de personas (provenientes del Cuerno de África). De este modo, los grupos terroristas obtienen financiación mediante los tráficos ilícitos y, a su vez, las organizaciones criminales transnacionales se benefician del control del territorio por parte de estos grupos.

En este contexto, tras la finalización de las misiones europeas y la salida de las tropas francesas de Mali, el grupo Wagner reconvertido en Africa Corps se ha erigido en garante de la seguridad regional, al tiempo que permite a Rusia afianzar su presencia en el continente africano e influir en la estabilidad del Sahel con el objetivo de dividir y debilitar la respuesta europea. El desafío para la comunidad de inteligencia, en este caso, viene de la propia dificultad de la anticipación a los acontecimientos en una región vasta, anárquica, de fronteras permeables y en la que, en muchas ocasiones, el Estado ocupa un papel residual. Además, la ausencia de infraestructura y comunicaciones dificulta enormemente tanto la recolección de información sobre el terreno como el recurso a fuentes como OSINT o SIGINT.

La debilidad europea en materia de inteligencia y diplomacia

La Unión Europea está aún en proceso de adaptar su doctrina y asumir el marco del "Gran Magreb" para abordar las particularidades de la zona norte de África-Sahel-África Occidental de manera diferenciada a Oriente Medio. Además, es imperativo recuperar la aproximación integral y firme, por parte de toda la Unión, que decayó tras la pandemia del SARS-CoV-2 y el *brexit*, pues las acciones estatales individuales adolecen de falta de credibilidad y alcance. El objetivo último en materia de inteligencia es conseguir la capacidad de predecir y anticipar la descomposición de los Estados saheliano para atajar la inestabilidad que ello genera y

detectar la infiltración rusa que comienza por la presencia del Africa Corps pero que tiene su continuación en inversiones que responden a los intereses de Moscú.

Este "flanco sur" pone a prueba una capacidad de inteligencia distinta a la del teatro ruso: anticipación y monitorización frente a atribución. Adicionalmente, su carácter transfronterizo y multiactor, así como las relaciones bilaterales existentes al margen de la Unión Europea, tensionan la arquitectura comunitaria y limitan su respuesta. Superar esta cuestión requiere una respuesta conjunta en materia de diplomacia, defensa e inteligencia, como se abordará más adelante.

3.1.3. China: influencia estratégica y la diplomacia de la sonrisa

Si la estrategia rusa se caracteriza por su naturaleza marcadamente disruptiva, el despliegue de la República Popular China en la zona gris responde a una estrategia de influencia progresiva y estructural. Pekín prioriza una aproximación a largo plazo orientada a generar dependencia económica y tecnológica, evitando superar los umbrales de alerta que desencadenarían una respuesta abierta por parte de sus adversarios.

Doctrina y dominio cognitivo: las "tres guerras" y FIMI

Las operaciones de influencia chinas se sustentan sobre la doctrina militar de las "tres guerras" (guerra de la opinión pública, guerra psicológica y guerra legal o *lawfare*). Como analiza Arco Escriche (2026), esta aproximación teórica ha evolucionado, dando forma a operaciones de dominio cognitivo que buscan moldear el entorno de decisión del adversario sin recurrir a la coerción directa. Aunque estas tácticas se han perfeccionado operativamente en el contexto territorial de Taiwán, su lógica es perfectamente extrapolable al escenario europeo. A través de campañas FIMI, China opera para contrarrestar el escrutinio sobre sus políticas internas e imponer narrativas favorables a sus intereses geopolíticos. En este sentido, el Servicio Europeo de Acción Exterior (2026) documenta cómo las redes de información alineadas con Pekín orientan sus esfuerzos hacia la promoción de la autocensura, la amplificación de la polarización existente y la alteración paulatina de la opinión pública europea.

Influencia y dependencias europeas: de los Balcanes al Báltico

En la dimensión geoeconómica, China aprovecha su músculo financiero y comercial para tejer una red de dependencias en el continente. Un vector fundamental en esta dinámica ha sido la Iniciativa de la Franja y la Ruta (BRI, por sus siglas en inglés). Weissmann (2023) detalla cómo

Pekín ha aprovechado las necesidades de desarrollo en los Balcanes Occidentales —región que constituye el "patio interior" estratégico de Europa— para consolidar su presencia, con Serbia como eje principal. La provisión de financiación para infraestructuras, exenta de las condicionalidades democráticas o de Estado de derecho exigidas por la Unión Europea, permite a China asentar un alineamiento diplomático a largo plazo y dificultar la cohesión regional europea, aprovechando que la realidad socioeconómica de estos países los hace más proclives a aceptar una financiación que no exija contraprestaciones liberales o democráticas.

Esta expansión económica se entrelaza con el control de infraestructuras críticas y tecnológicas, una práctica que se ha dado en denominar "diplomacia del cable" (Molina Urosa et al., 2026). El interés estratégico chino en el despliegue de cables submarinos de telecomunicaciones y en la gestión de redes logísticas marítimas ilustra la doble naturaleza de sus inversiones comerciales. Los recientes incidentes en el mar Báltico ponen de manifiesto la vulnerabilidad estructural que se deriva de esta presencia. Incluso en supuestos de afectación física a infraestructuras en los que se ven involucrados buques mercantes chinos, la complejidad del derecho marítimo comercial proporciona un amplio margen para la negación plausible, lo que dificulta enormemente los procesos de atribución legal y política.

La inteligencia frente a la influencia ilícita

La singularidad de la estrategia china plantea un desafío analítico sustancialmente distinto para los servicios de inteligencia europeos. Frente a un adversario ruso que explota la clandestinidad y el sabotaje directo o las amenazas multiactor del Gran Magreb, la dificultad de hacer frente a la estrategia de Pekín radica en la dificultad de detectar y evaluar una influencia que progresa a través de cauces aparentemente legales, comerciales y diplomáticos.

El esfuerzo de la inteligencia debe orientarse a discernir en qué punto exacto una legítima inversión extranjera directa, un acuerdo de cooperación académica o una concesión portuaria dejan de ser transacciones de mutuo beneficio para convertirse en instrumentos de coerción estratégica o de transferencia de tecnología sensible. Esta realidad obliga a la comunidad de inteligencia a integrar plenamente la dimensión de la seguridad económica en su ciclo analítico, monitorizando la vulnerabilidad de las cadenas de suministro y el flujo de capitales para poder proporcionar una alerta temprana efectiva frente a la erosión silenciosa de la autonomía estratégica europea.

Foco	Naturaleza de la amenaza	Instrumentos principales	Reto para la inteligencia
Rusia y sus *proxies*	Disruptiva y orquestada: campaña coordinada bajo el umbral del conflicto armado, diseñada para preservar la negación plausible de su autor.	Operaciones FIMI y desinformación; coerción mediante *proxies* (instrumentalización migratoria desde Bielorrusia); coerción energética; sabotaje de infraestructuras críticas (Nord Stream, EstLink 2, flota fantasma); reconversión del aparato de espionaje tras las expulsiones de 2022.	Atribución de actos concebidos para la negación; detección de la manipulación en entornos abiertos saturados de datos; lectura de acciones aisladas como piezas de una campaña coordinada.
Flanco sur (Magreb y Sahel)	Difusa y multiactor, protagonizada en parte por un socio revisionista (Rabat) y agravada por la inestabilidad saheliana; carácter transfronterizo.	Instrumentalización de flujos migratorios; *lawfare* (Sáhara Occidental); presión sobre Ceuta y Melilla; dependencia de interconexiones energéticas y de comunicaciones (estrecho de Gibraltar); penetración rusa vía Africa Corps; delincuencia transnacional.	Anticipación y monitorización: interpretar la señalización coercitiva de un socio formal, prever oleadas migratorias dirigidas y cubrir un espacio transfronterizo con relaciones bilaterales delicadas.
China	Influencia progresiva y estructural, de apariencia no coercitiva y horizonte de largo plazo, articulada sobre la doctrina de las "tres guerras".	Poderío geoeconómico (BRI); control de infraestructuras críticas y tecnológicas ("diplomacia del cable"); participaciones portuarias; influencia sobre los Balcanes Occidentales; guerra de la opinión pública, psicológica y legal.	Detección de una erosión silenciosa ejercida mediante instrumentos formalmente legales; evaluación de dependencias acumulativas cuyo efecto solo resulta visible a largo plazo; neutralización del escrutinio por parte del actor.

Tabla 4 - *Síntesis comparativa de las amenazas híbridas a la seguridad europea.*
Fuente: elaboración propia.

3.2. La respuesta de la inteligencia: capacidades y acciones

La Unión Europea carece, a día de hoy, de una capacidad de inteligencia propia e independiente: la función de inteligencia recae, en su mayor parte, sobre los Estados miembros. No obstante, la evolución de las amenazas descritas en epígrafes anteriores ha traído consigo el convencimiento (al menos, entre las autoridades comunitarias) de la necesidad de un esfuerzo integrador, a imagen de lo que sucede en otros ámbitos de la Unión.

Este apartado analiza el germen de la respuesta de la inteligencia europea, sus capacidades y límites, la doctrina actual y la importancia de la cooperación en esta materia, tanto en el seno de la UE como con aliados externos.

3.2.1. Del marco común de 2016 a la Comunicación conjunta de 2018

La anexión rusa de Crimea en 2014 transformó el panorama geopolítico europeo y dinamitó por completo el marco de seguridad existente hasta esa fecha. La respuesta inicial de la Unión Europea tuvo un carácter reactivo y declarativo, en línea con la idiosincrasia comunitaria, proponiendo en 2016 un "marco común" para la lucha contra las amenazas híbridas. Mediante la Comunicación Conjunta al Parlamento Europeo y al Consejo JOIN(2016) 18 final (Comisión Europea y Alta Representante, 2016) se establecieron 22 medidas orientadas a aumentar la concienciación, reforzar la resiliencia y mejorar la respuesta ante las crisis y se identificó como principal debilidad en este ámbito la falta de información fusionada. Para remediarlo, la propuesta más destacable fue la creación de una "Célula de fusión de la UE contra las amenazas híbridas", cuyo estudio se abordará más adelante. Además, se invitó a los Estados miembros a identificar vulnerabilidades mediante estudios de riesgos híbridos, a mejorar la comunicación estratégica y a crear un Centro de Excelencia para la lucha contra las amenazas híbridas.

Por lo demás, este Marco enfatizó la protección de infraestructuras críticas —con especial mención a la diversificación de fuentes y rutas energéticas y a la protección del espacio ultraterrestre—, el aseguramiento de los sistemas financieros, la ciberseguridad y la vigilancia de la salud pública para prevenir amenazas NRBQ. En otro orden de cosas, la Comunicación subrayó la necesidad de aumentar la cooperación con la OTAN y terceros países y remarcó la amenaza que suponen la radicalización y el extremismo violento. El espíritu de la Comunicación queda reflejado en tres de las palabras más usadas a lo largo de la misma: prevención, resiliencia y cooperación.

La cooperación en materia de inteligencia era, precisamente, la reclamación que dos años antes planteara Díaz-Caneja (2014), quien abogaba por establecer un marco de cooperación e intercambio de información realista para los Estados y los servicios de inteligencia, así como crear una estructura que coordinase dichos servicios. Es decir, reconociendo que los Estados miembros nunca renunciarían a una capacidad propia de inteligencia, la propuesta era abordar una política europea en ese ámbito para posibilitar una respuesta conjunta y eficaz.

En 2018, tras el ataque con agente neurotóxico en Salisbury, la Unión Europea reafirmó su compromiso con la lucha y la resiliencia frente a las amenazas híbridas en la Comunicación Conjunta al Parlamento Europeo y al Consejo JOIN(2018) 16 final (Comisión Europea y Alta Representante, 2018). Esta Comunicación daba un mayor peso a la lucha contra la desinformación y ratificaba la importancia de la ciberseguridad y la defensa NRBQ, la necesidad de mejorar la comunicación estratégica y volvía a poner el foco sobre la resiliencia. Como novedad, dedicaba un apartado a la contrainteligencia y reconocía la inteligencia como eje transversal, capacidad que, sin embargo, no ha dejado de enfrentarse a diversos factores que se analizarán más adelante. A nivel de capacidades, el mayor avance fue la inclusión de estas cuestiones en el ámbito de competencias de la ya citada Célula de fusión.

3.2.2. Capacidades comunitarias: la SIAC, el EU INTCEN y la Célula de fusión

Abordar las capacidades de la Unión Europea en materia de inteligencia exige reconocer, desde el primer momento, los límites de las mismas. No se trata de cuestiones presupuestarias u operativas, sino que forman parte de su propia concepción: la Capacidad Única de Análisis de Inteligencia (y por extensión todo lo que de ella depende) se circunscribe al análisis y fusión de información, dependiendo de los Estados miembros para el proceso de obtención. Como se analizará más adelante, esta circunstancia condiciona por completo el alcance de la inteligencia europea.

Esta Capacidad Única de Análisis de Inteligencia (SIAC por sus siglas en inglés) es el mecanismo de fusión que integra la inteligencia civil (EU INTCEN) y la militar (Dirección de Inteligencia del Estado Mayor de la Unión Europea, EMUE INT). La Célula de fusión contra Amenazas Híbridas, ya mencionada, se encuadra en el EU INTCEN. En cuanto a la Dirección de Inteligencia, que se encarga de la dimensión militar y se encuentra ligada a las operaciones de la PCSD, excede el objeto de este trabajo, centrado en la respuesta a las amenazas híbridas. Por otro lado, el hecho de que la Célula de fusión dependa del EU INTCEN permite apreciar una cuestión significativa, y es que la Unión Europea concibe la amenaza híbrida como un asunto de resiliencia civil que afecta a toda la sociedad, no como un dominio exclusivamente militar. Se desgranan a continuación las capacidades presentadas.

La SIAC nació en 2007 con el objetivo de integrar las inteligencias civil y militar de la Unión (Servicio Europeo de Acción Exterior, 2015), permitiendo fusionar ambas perspectivas para generar evaluaciones estratégicas conjuntas y alertas tempranas sin llegar a formar un servicio

de inteligencia. Todas las evaluaciones de inteligencia puestas a disposición de los Estados miembros y del Alto Representante son elaboradas conjuntamente bajo el paraguas de la SIAC. Trabaja estrechamente con el Centro de Satélites de la Unión Europea (SatCen), ubicado en la localidad española de Torrejón de Ardoz.

El EU INTCEN está vinculado, desde su origen, a la Política Europea de Seguridad y Defensa. Creado en 2002 como EU Situation Centre (EU SITCEN), fue la respuesta del entonces Alto Representante, Javier Solana, para dotar a la Unión de cierta capacidad de análisis de inteligencia (Servicio Europeo de Acción Exterior, 2015). En 2012, tras su integración el año anterior en el Servicio Europeo de Acción Exterior, adquirió su denominación actual. Las misiones del EU INTCEN pueden sintetizarse en evaluaciones de inteligencia, informes de inteligencia y evaluaciones de amenazas. Este organismo se estructura en dos Divisiones: la de Análisis (INTCEN.1) y la de Apoyo e Investigación de Fuentes Abiertas (INTCEN.2), lo que refuerza la idea de que la misión principal del EU INTCEN es el análisis y la integración de información. De este modo, las posibilidades de obtención de información de la SIAC se limitan a las fuentes abiertas, la inteligencia de imágenes geoespaciales (proporcionada por el SatCen) y los canales diplomáticos.

La creación de la Célula de fusión de la UE contra amenazas híbridas (Comisión Europea y Alta Representante, 2016) es la respuesta orgánica específica al fenómeno que estudia este trabajo. Su función es recibir, analizar y compartir información clasificada y de dominio público sobre las amenazas híbridas, información procedente del SEAE, la Comisión y los Estados miembros. El objetivo último de esta Célula es alimentar los procesos de decisión estratégicos en el seno de la Unión y su efectividad depende en gran medida de que los Estados miembros compartan información, por lo que desde la Comisión y la Alta Representante se invita encarecidamente a crear puntos nacionales de contacto con la Célula, invitación que sería reiterada en la Comunicación Conjunta de la Comisión Europea y la Alta Representante (2018), que además apuesta por dotar de más recursos a la Célula de fusión, algo que también se reitera en la Brújula Estratégica para la Seguridad y la Defensa (Consejo de la Unión Europea, 2022b).

Resulta por tanto evidente que el grueso de la capacidad de inteligencia de la Unión Europea frente a las amenazas híbridas es en realidad una capa de análisis, integración y coordinación que depende profundamente de las diferentes capacidades de obtención de los Estados

miembros y del SEAE. Esto no es óbice para que la Unión reconozca la importancia de las amenazas híbridas, como atestiguan los títulos de las Comunicaciones Conjuntas analizadas, que ponen el foco sin ambages en esta problemática.

3.2.3. La consolidación de la doctrina (2022-2026)

La invasión a gran escala de Ucrania en 2022 sirvió como catalizador para la política de seguridad comunitaria, forzando un tránsito desde el enfoque fundamentalmente declarativo y preventivo de años anteriores hacia una arquitectura dotada de instrumentos de respuesta. Este punto de inflexión quedó plasmado en la Brújula Estratégica para la Seguridad y la Defensa (Consejo de la Unión Europea, 2022b), documento que actuó como base doctrinal al reconocer explícitamente la urgencia de dotar a la Unión de un repertorio de medidas tangibles para contrarrestar las agresiones en la zona gris.

El paso de "declarar" a "dotarse de herramientas de respuesta" se materializó mediante el diseño de "cajas de herramientas" (*toolboxes*) orientadas a centralizar, coordinar y escalar las acciones europeas. El primer pilar de esta nueva arquitectura fue la aprobación del marco para una respuesta coordinada a las campañas híbridas, conocido como *Hybrid Toolbox* (Consejo de la Unión Europea, 2022a). Este instrumento fue concebido para aglutinar medidas diplomáticas, económicas y de ciberseguridad, proporcionando a los decisores europeos opciones de respuesta frente a actores hostiles. En paralelo, y dada la primacía del dominio cognitivo en las estrategias de adversarios como Rusia o China, se impulsó la *FIMI Toolbox*. Como señala Benedicto (2025), este andamiaje institucional ha permitido a la Unión organizar una defensa más sistematizada frente a la desinformación. Apoyado en la labor analítica del Servicio Europeo de Acción Exterior (2026), este marco dota a Europa de mecanismos para la imposición de costes (sanciones y medidas restrictivas) a quienes dirigen la manipulación informativa.

La última consolidación de este proceso evolutivo se produce con las Conclusiones del Consejo sobre el desarrollo de la capacidad de la Unión Europea para luchar contra las amenazas híbridas (Consejo de la Unión Europea, 2026). Sin embargo, desde una perspectiva analítica en el ámbito de la inteligencia, resulta imprescindible introducir un matiz crítico sobre la verdadera naturaleza de estos avances: si bien representan un salto cualitativo innegable en la maduración de la doctrina comunitaria, estas iniciativas continúan siendo, en su mayor parte, marcos procedimentales. De hecho, el informe de 2025 sobre la implementación de la

Brújula Estratégica (Servicio Europeo de Acción Exterior, 2025) reconoce que es necesario un mayor esfuerzo para alcanzar una capacidad suficiente. Por otro lado, la efectividad real de la *Hybrid Toolbox* y la *FIMI Toolbox* adolece de una dependencia estructural ineludible. La Unión Europea ha logrado construir y sistematizar las "cajas de herramientas" operativas, pero las capacidades de inteligencia de base —indispensables para la detección temprana y la atribución a actores concretos— que deben desencadenar el uso de dichas herramientas siguen perteneciendo casi en exclusiva a los Estados miembros.

3.2.4. Cooperación UE-OTAN y el Hybrid CoE

La seguridad europea ha estado tradicionalmente vinculada a la OTAN desde la fundación de la Organización transatlántica. La cooperación con la Alianza, así como la dicotomía seguridad efectiva frente a dependencia estratégica no son, pues, cuestiones ajenas al ámbito de la lucha contra las amenazas híbridas. Antes al contrario, ejemplifican a la perfección algunas de las aristas en las relaciones UE-OTAN, si bien, como se verá, también han permitido construir sinergias de gran valor cuando se han identificado correctamente las fortalezas y debilidades de una y otra organización.

Históricamente, las relaciones entre la Unión Europea y la OTAN han estado marcadas por tensiones políticas, la búsqueda de la autonomía de la Unión Europea y la llamada "fatiga institucional". Hasta mediados de la pasada década, la cooperación era rudimentaria, informal y a bajo nivel, limitada por el bloqueo político a nivel macro (principalmente debido a la disputa entre Turquía y Chipre). La Declaración Conjunta de Varsovia en 2016 supuso un punto de inflexión, dando paso a una cooperación sostenida en áreas técnicas específicas.

Desde entonces, y como destaca Anagnostakis (2025), esa cooperación se ha estrechado, pero también ha dado lugar a lo que denomina "solapamiento funcional", fruto de la combinación del solapamiento institucional con la dependencia de recursos. Algo que, si bien genera un riesgo de duplicidad, también ha derivado en una sólida cooperación funcional. Esta superación del solapamiento por la cooperación se debe a dos factores estructurales: la crisis exógena (la anexión de Crimea por parte de Rusia en 2014, precedida de los ciberataques a Estonia en 2007, y la expansión del Estado Islámico) y la interdependencia y asimetría de recursos. Este último factor se explica por las dificultades de ambas organizaciones para hacer frente, por sí solas, a unas amenazas híbridas que operan por debajo del umbral del conflicto militar abierto: la OTAN —esencialmente militar—, reconoció su dependencia de la "caja de

herramientas" civiles, regulatorias y financieras de la UE, así como de su influencia en regiones vulnerables como los Balcanes o los países de la Asociación Oriental; por su parte la Unión se beneficia de la dimensión transatlántica y la robustez estratégica de la OTAN. De este modo, disminuyeron el riesgo de disputas territoriales institucionales y el temor de pérdida de autonomía.

Esta cooperación se ha venido estrechando en los últimos años, como muestran las sucesivas declaraciones conjuntas de 2018 y 2023, siendo esta última la que reviste mayor interés. En primer lugar, se firmó tras la invasión a gran escala de Ucrania en 2022 y fue la respuesta a la "instrumentalización de la energía" por parte de Rusia, poniendo el foco en las amenazas híbridas, la resiliencia y la protección de infraestructuras críticas. De hecho, al día siguiente de esta firma, se constituyó la *Task Force* para la resiliencia de las infraestructuras críticas (Molina Urosa et al., 2026), reforzando la colaboración en ese ámbito. Y, como último elemento de interés, fue la primera declaración conjunta en la que se mencionaba a China como actor de interés para ambas organizaciones. Sin embargo, revisando el texto original de la declaración (Unión Europea y Organización del Tratado del Atlántico Norte [UE y OTAN], 2023) puede apreciarse que la declaración tiene, valga la redundancia, un carácter eminentemente declarativo, destacando varios casos de éxito en materia de cooperación, pero sin presentar avances claros en la delimitación de responsabilidades y el reparto de tareas, conque el solapamiento, al menos aparentemente, persiste.

Mención especial merece el *Hybrid CoE* –Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas– propuesto en la Comunicación Conjunta al Parlamento Europeo y al Consejo JOIN(2016) 18 final (Comisión Europea y Alta Representante, 2016), en la que, de hecho, se menciona a los centros de excelencia de la OTAN como modelo para su creación. La Comunicación dedica además un apartado completo a resaltar la importancia de la cooperación entre la Unión Europea y la OTAN. En cuanto al *Hybrid CoE* en sí mismo, nació al año siguiente como un centro internacional independiente en el que participan ambas organizaciones, siendo su papel el de un nodo de conocimiento, doctrina, formación y ejercicios. Es decir, se trata de un foro de conocimiento compartido de alto nivel político y técnico, como evidencian publicaciones como la de Giannopoulos et al. (2021). Pero ello también conduce de vuelta a la reflexión ya deslizada en varias ocasiones a lo largo de este apartado: no es una capacidad operativa conjunta.

Con todo, la colaboración institucional permite extender el alcance y superar el que tendrían ambas organizaciones por separado, pero suma el reto de la coordinación: mandatos solapados, estructuras paralelas, límites políticos y dependencia de la voluntad de ambas organizaciones y, en última instancia, de los Estados. La cooperación es real, pero desigual, solapada y pendiente aún de concreción en el ámbito operativo.

3.3. Desafíos y carencias del modelo europeo

La arquitectura de inteligencia de la Unión Europea no adolece de fallos de ejecución, sino que está limitada por su propio diseño. Evaluar las capacidades de la UE bajo los mismos parámetros que los de un Estado nación supone ignorar que Bruselas es, por definición, un actor de inteligencia atípico. En su configuración actual, la Capacidad Única de Análisis de Inteligencia (SIAC) opera bajo ciertas restricciones; es, como su propio nombre indica, una capacidad de análisis de alto nivel, pero funciona, en esencia, como un "analista sin ojos propios". A pesar de haber evolucionado desde una pequeña célula de evaluación hasta convertirse en un centro de fusión de todas las fuentes, la Unión carece de medios soberanos de obtención directa. Al no disponer de redes propias de inteligencia humana (HUMINT), capacidades autónomas de interceptación de señales (SIGINT) o constelaciones exclusivas de satélites militares de observación (las capacidades del SatCen son limitadas y dependen en gran medida de imágenes proporcionadas por terceros), el sistema se encuentra limitado por la ausencia de una capacidad de obtención. La Unión Europea no recolecta información en el terreno; su función primordial es *fusionar* la información de fuentes abiertas (OSINT) con aquellos productos elaborados que las capitales deciden, en función de sus intereses, compartir con Bruselas.

Esta limitación técnica originaria conduce inexorablemente al segundo gran inconveniente del sistema: la volatilidad de la contribución voluntaria. La brecha de inteligencia europea no se explica únicamente por carencias materiales, sino por el realismo político que rige el comportamiento de los Estados miembros. Como describe Fägersten (2016), la cooperación europea en este ámbito se topa con cuatro obstáculos profundamente arraigados en la cultura estatal. En primer lugar, predomina una lógica de suma cero: los servicios nacionales perciben la inteligencia como una divisa soberana, encontrando mayor valor estratégico, político e incluso comercial en retener información exclusiva (o compartirla estrictamente a nivel bilateral) que en volcarla en un fondo común europeo.

A esta reticencia se suman las asimetrías de poder. Los Estados con grandes capacidades y tradición en inteligencia (como Francia o Alemania) tienden a moldear las dinámicas de cooperación a su medida, generando recelos entre los Estados más pequeños y perpetuando la existencia de clubes dentro del club. En tercer lugar, existen intereses burocráticos, que evidencian que las agencias nacionales protegen sus prerrogativas y desconfían de la creación de supraestructuras que puedan diluir su influencia o amenazar las redes profesionales preexistentes. Por último, Fägersten (2016) subraya la falta de infraestructuras cooperativas sólidas, esto es, la ausencia de una cultura compartida y de un nivel suficiente de confianza interpersonal e institucional a escala continental, un déficit que imposibilita la homogeneidad en el análisis de amenazas.

Lejos de mitigarse mediante la integración, estas fricciones estatales se ven amplificadas por una crónica fragmentación institucional. El ecosistema de inteligencia de la UE no es un monolito, sino un conjunto segregado de parcelas funcionales que operan, a menudo, de espaldas unas de otras. El Centro de Inteligencia y Situación de la UE (INTCEN) nutre a la Política Exterior y de Seguridad Común (PESC), Europol se circunscribe a la aplicación de la ley y la seguridad interior y el Centro de Satélites (SatCen) provee inteligencia geoespacial bajo demanda. Por su parte, foros como el Club de Berna y su Grupo Contraterrorista (CTG) operan al margen del marco institucional de la Unión Europea, restringiendo la cooperación operativa en materia de inteligencia a los canales intergubernamentales en detrimento del ecosistema comunitario.

Esta multiplicidad de nodos genera duplicidades orgánicas y fricciones burocráticas constantes. Una disfunción que quedó patente a finales de 2025 en el choque político entre la presidenta de la Comisión, Ursula von der Leyen, y la Alta Representante, Kaja Kallas (Foy, 2025). Las tensiones en torno a quién debía liderar la centralización del análisis de inteligencia (la Comisión con su enfoque tecnocrático y transversal, o el Servicio Europeo de Acción Exterior reivindicando su competencia sobre la inteligencia diplomática) ilustraron cómo las rivalidades institucionales lastran la agilidad de la UE. Este tipo de solapamientos internos, sumados a la compleja interoperabilidad con actores externos como la OTAN, configuran un entramado de seguridad denso, pero lento y poco eficiente ante la naturaleza difusa de las amenazas híbridas actuales.

Atendiendo a los argumentos de Fägersten (2016), construir estructuras supranacionales de inteligencia desde arriba, sin asentar previamente una base política, legal y técnica sólida, supone trasladar las expectativas de seguridad al nivel de la UE, sin dotarla de las herramientas coercitivas ni operativas para cumplirlas.

Sin embargo, esta acumulación de disfunciones (el déficit operativo, el recelo conductual y el laberinto institucional) no deja de estar respaldada por el límite fundamental de la integración: la delimitación de competencias de los Tratados. Cualquier intento de consolidar una agencia centralizada al estilo de un servicio federal choca con el Artículo 4.2 del Tratado de la Unión Europea (TUE), que estipula literalmente que "la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro". Es en este precepto donde encuentra su límite, hoy por hoy, la viabilidad de la centralización plena de la inteligencia comunitaria. Este límite supone una cuestión no menor, pues su principal arista, la carencia de herramientas comunitarias de obtención es especialmente onerosa en el campo híbrido, porque la atribución y la detección de campañas que operan por debajo del umbral del conflicto abierto exigen una fusión multifuente (HUMINT, SIGINT) que la Unión no es capaz de proporcionar.

Por otra parte, como señala Tuinier (2025), la cooperación entre servicios nacionales exige un elevado nivel de confianza entre autoridades que el marco jurídico actual no puede forzar por decreto. Por su parte, Niinistö (2024) advierte de que la cooperación informal vigente carece de base jurídica en la UE y no puede apoyar directamente la toma de decisiones; por otro lado, el servicio pleno que propone –a largo plazo– debe hacerse sin emular a los servicios nacionales ni interferir en su prerrogativa sobre la seguridad nacional. Y es que, mientras los Tratados mantengan la seguridad nacional como competencia exclusiva de los Estados, el techo estructural de la inteligencia europea permanecerá. Cabe preguntarse hasta qué punto es posible una mayor integración sin reforma previa de los Tratados y en qué condiciones los Estados miembros estarían dispuestos a ello.

3.4. Propuestas y líneas de acción

Tras las cuestiones tratadas a lo largo de las secciones precedentes, se hace necesario ahora abordar el debate existente acerca de las propuestas que hay sobre la mesa para dotar a la Unión Europea de un conjunto de herramientas de inteligencia que permita hacer frente, de manera eficaz, a las amenazas a la seguridad comunitaria.

En este punto, es conveniente recordar que el presente Trabajo constituye una revisión sistemática del estado de la cuestión, por lo que las alternativas planteadas provienen de los ámbitos académico y oficial, no del parecer del autor.

3.4.1. La asimetría entre amenaza y respuesta

A lo largo del análisis realizado, se ha puesto de manifiesto (en algunas ocasiones de modo más patente que en otras) la desigualdad entre los adversarios de la Unión Europea y las capacidades en inteligencia de esta última. Si los primeros actúan de manera coordinada –especialmente en el caso de China y Rusia–, con campañas híbridas, negables y por debajo del umbral del conflicto abierto (Giannopoulos et al., 2021), la Unión responde con una capacidad de análisis y fusión pero sin herramientas de obtención autónomas, dependiente de la contribución voluntaria de los Estados, diseminada entre órganos diversos y acotada por el artículo 4.2 del Tratado de la Unión Europea como señalan los ya analizados Tuinier (2025) y Fägersten (2016).

Esta asimetría, no obstante, no es cuantitativa, sino estructural. No es una cuestión de falta de recursos, sino de diseño. Y no cabe pensar que sea algo accidental, porque si bien el citado artículo 4.2 del TUE establece que la seguridad nacional es competencia exclusiva de los Estados y pone coto, por tanto, a la inteligencia comunitaria, los artículos 71 a 73 del Tratado de Funcionamiento de la Unión Europea (TFUE) se dedican al Espacio de Libertad, Seguridad y Justicia, en cuyo marco se inscribe la cooperación en materia de seguridad interior, articulada en instrumentos como la Estrategia para una Unión de la Seguridad (Comisión Europea, 2020). Esta cooperación tiene lugar bajo la coordinación de órganos como el Comité Permanente de Cooperación Operativa en materia de Seguridad Interior (COSI) —artículo 71 TFUE—, aunque preservando en todo caso —artículos 72 y 73— la responsabilidad última de los Estados sobre su propia seguridad, extremo que se retomará al valorar la vía de la integración pragmática.

Esta cuestión estructural condiciona, empero, la respuesta comunitaria. Mientras el adversario actúa como sujeto único, la Unión provee una capa de coordinación a los contribuyentes soberanos, que cooperan en función de sus intereses particulares, conque la solución no puede ser únicamente un incremento en el personal o el presupuesto para la inteligencia comunitaria. Así, incluso considerando el debate actual en el que se halla inmersa la Unión Europea acerca de la integración de diferentes ámbitos, cualquier propuesta con una

mínima posibilidad de prosperar en el campo de la inteligencia debe plantearse desde la perspectiva de la restricción soberana, no contra ella. Esto conduce necesariamente a cuestionar si la piedra angular de la comunidad de inteligencia europea debe ser un organismo autónomo o, por el contrario, un espacio que propicie la cooperación y la compartición de información entre Estados.

3.4.2. ¿Una Agencia Europea de Inteligencia? Propuestas oficiales y académicas

Ante el panorama descrito a lo largo de este Trabajo, analizado ya por múltiples autores, varios de ellos han plasmado sus propuestas. En este apartado se aborda la propuesta maximalista: la creación de una suerte de "Agencia Europea de Inteligencia", idea recurrente que ya analizaba Fägersten (2016).

No cabe duda de que este planteamiento es atractivo, ya que, sobre el papel, soluciona el problema de la asimetría frente a las amenazas ya enumeradas: un servicio único, con plenas capacidades a lo largo de todo el ciclo de inteligencia, medios propios, independiente de la voluntad y las contribuciones de los Estados miembros y el mandato claro de proporcionar inteligencia al servicio del conjunto de la Unión Europea. Un sujeto único frente a una amenaza única –entendida como una amenaza al conjunto de la Unión–.

Sin embargo, Fägersten (2016) advierte de los motivos por los cuales una "CIA europea" es un modelo difícil de llevar a la práctica en el día de hoy. En primer lugar, por el sesgo de autoselección, ya que las propuestas en esta línea suelen proceder de actores con capacidades de inteligencia débiles o limitadas (como Estados pequeños o la propia Comisión Europea), que buscan en el planteamiento común soluciones a sus carencias particulares. Por otro lado, no parece probable que los servicios nacionales estén dispuestos a sustituir las relaciones bilaterales, basadas en la confianza labrada a lo largo de años o décadas, por la compartición de información con una nueva agencia centralizada que, a la larga, podría acabar reemplazándolos. Finalmente, está la cuestión competencial, ya mencionada, que tiene su techo en los Tratados: una construcción "de arriba hacia abajo", con el marco actual, podría crear expectativas que la UE no puede cumplir legal, política ni técnicamente. La Unión Europea es un actor de inteligencia atípico y, como tal, no es posible reproducir modelos ya existentes que no tienen en cuenta las particularidades comunitarias.

A todo ello se añade otro factor, señalado por González López (2024): los Estados no terminan de percibir las amenazas desde una perspectiva europea, sino que lo hacen desde una perspectiva nacional; de este modo, a los Estados del este les preocupa la amenaza rusa, mientras que los del sur consideran que sus principales riesgos provienen del Magreb o el Sahel. Así, resulta complicado concebir que estén dispuestos a renunciar a esta capacidad soberana en favor de un servicio central que no les proporcione la garantía de que *su* amenaza va a ser considerada prioritaria.

Este mismo autor (González López, 2024), por otra parte, propone lo que bautiza como "División de Inteligencia contra el Terrorismo y el Blanqueo de Capitales", un organismo independiente que no sustituiría a los servicios nacionales, sino que los complementaría en dos áreas críticas: el terrorismo y el blanqueo de capitales. Esta División, con capacidades completas a lo largo de todo el ciclo de inteligencia, estaría sometida al control del Parlamento Europeo mediante comisiones específicas y su director estaría nombrado por el Parlamento Europeo a propuesta unánime del Consejo Europeo. Sin embargo, pese a la intención subrayada de delimitar el ámbito de actuación, esta propuesta sigue encontrándose con los problemas ya mencionados: soberanía, competencias y confianza.

En el apartado institucional, resulta inevitable revisar la propuesta de Niinistö (2024). El expresidente finlandés, en su calidad de asesor especial de la presidencia de la Comisión propone una evolución del modelo actual basada en dos líneas de acción. La primera de ellas es la evolución de las capacidades actuales, centrándose en la SIAC, mediante la implementación de los pasos acordados en la Brújula Estratégica. Además, aboga por formalizar el intercambio de datos entre la SIAC y otros organismos comunitarios, lo que a su vez otorgaría cierta capacidad de contraespionaje. Pero posiblemente la línea de mayor interés sea la propuesta de creación de un servicio de cooperación de inteligencia completo a nivel comunitario que responda a necesidades estratégicas y operativas, complementario a los servicios nacionales y sin duplicar tareas asumidas por estos. En ese sentido, el informe es bastante explícito al aseverar que este servicio no debe emular las tareas de las organizaciones nacionales de inteligencia de los Estados miembros, especialmente en lo que respecta a la obtención de inteligencia.

Para concluir este apartado, es preciso recurrir a fuentes hemerográficas para ilustrar la propuesta institucional más reciente: el ya mencionado anuncio de noviembre de 2025 de

Ursula von der Leyen (Foy, 2025). La mandataria propuso la creación de una nueva unidad de inteligencia dependiente de la Secretaría General de la Comisión, que se nutriría de personal de inteligencia de los Estados miembros. Diversas voces han mostrado su reticencia al respecto ante el riesgo de duplicidades y solapamientos con el EU INTCEN, hasta el punto de que la Alta Representante, Kaja Kallas, ha rechazado públicamente esta posibilidad (Wax, 2025), apelando al citado riesgo de duplicidad. Finalmente, en febrero de 2026 (Roussi y Barigazzi, 2026) la presidenta de la Comisión rebajó el plan inicial ante la resistencia de los Estados miembros y del propio SEAE: la célula quedará previsiblemente reducida a una "unidad de seguridad", dejando la compartición de inteligencia en el INTCEN.

Así las cosas, la creación de una Agencia Europea de Inteligencia no parece, hoy por hoy, una posibilidad que pueda ponerse en práctica. A las limitaciones de los Tratados hay que añadir las inherentes disfuncionalidades que, muy probablemente, se verían agravadas por las reticencias de los Estados miembros. El siguiente apartado analiza la integración de capacidades como vía para mitigar la asimetría de la inteligencia comunitaria frente a las amenazas híbridas analizadas, pero dentro del marco vigente.

3.4.3. La integración de capacidades como propuesta realista

La formulación de una propuesta realista para la inteligencia europea hace necesario, en primer lugar, un reenfoque conceptual: el objetivo no es quebrar o vencer el techo soberano que imponen los Tratados, sino operar productivamente bajo él. Frente a los recurrentes y poco factibles llamamientos a crear agencias de inteligencia supranacionales —una suerte de CIA europea que centralice la capacidad de inteligencia—, la viabilidad pasa por profundizar en aquellos ámbitos en los que la Unión sí tiene margen de actuación y ya genera un valor añadido. Esto implica apostar por el análisis, la fusión de la información, la Inteligencia de Fuentes Abiertas (OSINT), la explotación de imágenes a través del Centro de Satélites de la UE (SatCen) y la coordinación estratégica. Como principio fundamental, este modelo asume que el impulsor de la cooperación no es la coerción jurídica ni los mandatos verticales, sino el fortalecimiento de una "infraestructura blanda" —compuesta de confianza, cultura común y rutinas compartidas— que gobierne y estimule la compartición voluntaria de información entre los Estados miembros.

El argumento a favor de priorizar y financiar esta infraestructura blanda se asienta sobre bases doctrinales y empíricas. Fägersten (2016) ya recomendaba construir confianza mediante la

formación y la socialización, argumentando que los componentes de los servicios de inteligencia nacionales se beneficiarían notablemente de aprender los hábitos del trabajo multilateral en etapas tempranas de sus carreras institucionales, forjando así confianza y comprensión estructural. En esta misma línea de investigación, Tuinier (2025) demuestra empíricamente que, en un área tan sensible, la cooperación descansa genuinamente sobre las relaciones sociales y la confianza interpersonal, no sobre la obligación jurídica. De ahí se deduce que invertir de forma decidida en dicha confianza constituye, de hecho, la principal motivación hacia la cooperación voluntaria.

Para calibrar el ritmo, el alcance y la profundidad esperables de esta integración, resulta aconsejable recurrir al ya citado COSI. Como se ha analizado, incluso en el ámbito de la seguridad interior, donde los Tratados sí conceden a la Unión una competencia compartida explícita (artículo 71 TFUE), la integración se ha construido con notable cautela. Su evolución ha sido marcadamente gradual, de raíz intergubernamental y carente de una ejecución operativa propia: el COSI coordina acciones, pero no ostenta mando directo, consolidando una trayectoria histórica de respeto a las prerrogativas nacionales operativas (Sánchez Peláez, 2021). La inferencia lógica por comparación con el ámbito de estudio de este Trabajo se impone por sí sola: si en un terreno jurídicamente compartido los avances son tan parsimoniosos y repletos de cautelas, en el terreno reservado por excelencia a la soberanía nacional —la inteligencia forma parte de la seguridad nacional amparada en el artículo 4.2 TUE— solo cabe esperar el desarrollo de una vía aún más liviana. Esto es, una arquitectura de inteligencia no operativa y sin prerrogativas de captación de fuentes humanas.

Esta lógica limitativa se concreta, por ejemplo, en el Colegio de Inteligencia en Europa (ICE). Concebido como una plataforma intergubernamental y no operativa, el ICE tiene como misión primordial forjar esa necesaria cultura estratégica común. Su diseño institucional sortea la restricción del artículo 4.2 del TUE precisamente porque, desde su concepción, renuncia a intervenir en la obtención o en el intercambio operativo de inteligencia. Tal y como señala Tuinier (2025), el ICE opera como una plataforma para cultivar lazos y fomentar una cultura común, y no como un mero lugar de “intercambio de sellos”. Por su parte, Borghoff et al. (2024) ahondan en el detalle descriptivo de esta entidad y destacan su vocación formativa marcadamente interna. No obstante, conviene remarcar lo ya mencionado anteriormente: el ICE, si bien integra cultura, lenguaje y confianza, no aporta capacidades materiales de

obtención. Se erige, por tanto, en una pieza estrictamente necesaria del engranaje, pero en ningún caso suficiente.

El paquete de medidas realista debe extenderse, en consecuencia, más allá del marco del ICE, focalizándose en aquellos nichos donde la UE sí obtiene resultados tangibles. En primer término, requiere el refuerzo de la Capacidad Única de Análisis de Inteligencia (SIAC), avanzando en la línea del enfoque paso a paso propuesto recientemente por Niinistö (2024) para transitar de forma gradual hacia un servicio de cooperación plenamente desarrollado, que potencie la Célula de Fusión Híbrida ya existente y los procesos estructurados de intercambio de datos. Estos esfuerzos se alinean directamente con los compromisos reflejados en el informe de implementación del SEAE (2025). En segundo lugar, exige el desarrollo expansivo de la OSINT y de la capacidad geoespacial del SatCen, cuyo nicho indiscutido de competencia en inteligencia de imágenes debe complementarse progresivamente con servicios gubernamentales propios de observación de la Tierra. Finalmente, asume como una virtud operativa el "minilateralismo" (Fägersten, 2016), es decir, el avance conjunto de pequeñas coaliciones de Estados con intereses comunes concretos. El eje vertebrador de este paquete realista puede resumirse acudiendo a la clásica disyuntiva *potestas-auctoritas*: la Unión no aspira —ni puede aspirar hoy— a construir una capacidad soberana de obtención por métodos coercitivos sobre los Estados miembros, sino a consolidar una autoridad analítica y de coordinación de referencia para el club comunitario.

Con todo, es preceptivo reconocer la limitación fundamental de esta propuesta. Este modelo de integración pragmática no resuelve la asimetría estructural ni la tensión competencial descrita en el apartado 3.4.1, sino que se limita a mitigarla en sus efectos cotidianos. Las competencias exclusivas de obtención y acción directa permanecen bajo la soberanía nacional; la actuación comunitaria busca la optimización dentro de los márgenes que otorgan los Tratados.

En definitiva, este modelo pragmático de inteligencia es viable precisamente porque respeta el principio de soberanía de los Estados miembros, pero su horizonte final queda ineludiblemente fijado por ese mismo techo soberano. Que esta arquitectura analítica y de coordinación pueda llegar a materializarse a corto y medio plazo depende de una voluntad política que —como evidenció con claridad el episodio del pasado mes de noviembre— sigue siendo volátil y condicional. Queda abierto, por tanto, un interrogante estructural: está por

ver si la presión del actual panorama de amenazas terminará por vencer las reticencias históricas y mover esa voluntad, o si, por el contrario, la asimetría descrita se consolidará como un rasgo estructural persistente del proceso europeo. Las claves para dilucidar el desenlace de esta encrucijada entre seguridad colectiva y reserva de soberanía son las que articulan las conclusiones del presente Trabajo, presentadas tras la discusión de la evidencia revisada.

3.5. Discusión de la evidencia revisada

La naturaleza cualitativa de esta revisión sistemática hace necesario un ejercicio crítico de ponderación sobre el corpus documental seleccionado. A continuación, se evalúan los sesgos epistémicos del material analizado, las líneas de consenso y disenso entre los autores, las limitaciones de fiabilidad de ciertas fuentes y la vigencia del marco teórico frente al acelerado escenario geopolítico actual.

3.5.1. Concentración geográfica y sesgos del corpus analizado

El análisis sistemático de la literatura apunta a una asimetría en la distribución de los focos de atención y las metodologías empleadas. Lo más reseñable es que existe un sesgo geográfico significativo hacia las dinámicas del flanco este, ya adelantado en la caracterización del corpus. Mientras que las acciones rusas (operaciones FIMI, sabotajes en el Báltico y coerción energética) acaparan la mayor parte de la producción académica y predictiva analizada, el flanco sur (Magreb y Sahel) y el vector tecnológico chino reciben una atención considerablemente más fragmentada o tangencial. Esto puede generar una percepción distorsionada de que la "hibridez" es un patrimonio metodológico casi exclusivo de Moscú, invisibilizando la progresión silenciosa y estructural de Pekín o los desafíos multiactor del norte de África.

Por otra parte, el conjunto de fuentes analizado adolece de una escasez de trabajos empíricos de campo. La literatura es minuciosa en el apartado teórico (como la discusión sobre la zona gris o la tríada clausewitziana), pero son escasos los estudios que miden de forma cuantitativa o empírica el impacto real de estas amenazas en la ciudadanía.

En lo relativo al bloque de capacidades de la Unión Europea (SIAC, EU INTCEN, Célula de Fusión Híbrida), la evidencia analizada se nutre de forma predominante de fuentes oficiales y documentos de alta política (como las Comunicaciones Conjuntas de la Comisión y las

Conclusiones del Consejo). Esta dependencia de la literatura gris institucional —de nuevo, descrita en el apartado 1.5.— tiende a reflejar marcos procedimentales e intenciones normativas óptimas, soslayando en ocasiones las fricciones burocráticas cotidianas y los fallos operativos reales de las agencias.

3.5.2. Convergencias y divergencias doctrinales

Lejos de presentarse como un bloque monolítico, los autores revisados convergen en el diagnóstico estructural, pero discrepan en las soluciones propuestas. Ciertamente, la mayor parte de la literatura coincide en señalar que la carencia de capacidades autónomas de obtención (HUMINT, SIGINT) conforma el límite estructural de la inteligencia comunitaria. Existe consenso acerca de que la UE analiza información, pero no la obtiene, lo que deja la capacidad de inteligencia comunitaria supeditada a la contribución voluntaria y discrecional de las capitales.

En relación con la cooperación UE-OTAN, autores como Anagnostakis (2025) muestran una postura optimista, argumentando que las crisis exógenas han permitido transitar del solapamiento institucional a una cooperación funcional sólida y asimétrica de mutuo beneficio. Sin embargo, al contrastar esta visión con la del propio texto de la Declaración Conjunta de 2023, se observa que estos avances son eminentemente declarativos, apreciándose una falta de un reparto operativo explícito que perpetúa duplicidades latentes.

El debate sobre el futuro institucional de la inteligencia europea divide al corpus en dos corrientes. Por un lado, se sitúan las propuestas maximalistas que abogan por una Agencia Europea de Inteligencia con competencias plenas o divisiones independientes especializadas. Por otro lado, se observa otra línea más pragmática ejemplificada en los informes de Niinistö (2024) o la tesis de Tuinier (2025); estas publicaciones advierten de que cualquier estructura construida desde arriba sin asentar primero una infraestructura blanda de confianza interpersonal y respeto escrupuloso al artículo 4.2 del TUE generará expectativas imposibles de cumplir.

3.5.3. Límites metodológicos y fiabilidad de las fuentes seleccionadas

El rigor de una revisión sistemática cualitativa hace necesario ponderar con cautela el valor probatorio de los textos incluidos, diferenciando entre su potencia analítica y su precisión en lo que se refiere a la arquitectura institucional.

Ciertos trabajos del corpus poseen un indudable valor en el plano de la propuesta teórica, pero requieren ser manejados con prudencia metodológica al evaluar datos institucionales. Un ejemplo representativo lo componen las aportaciones de González López (2024) y su propuesta de una "División de Inteligencia contra el Terrorismo y el Blanqueo de Capitales". Si bien su enfoque normativo es sugerente para el debate académico, presenta incorrecciones técnicas respecto al funcionamiento de la arquitectura de seguridad interior de la UE y las realidades competenciales del Tratado de Funcionamiento.

Con todo, identificar estas inconsistencias no resta valor la inclusión de estas fuentes, sino que enriquece la revisión, evidenciando que la literatura académica a menudo proyecta soluciones ideales que subestiman la rigidez de la burocracia europea.

3.5.4. Vigencia de las fuentes en el escenario estratégico de 2026

El marco temporal acotado para este TFM (2014-2026) permite al estudio evaluar la evolución del conocimiento estratégico y su adaptación a la realidad cambiante. Así, las fuentes publicadas en 2021 o años anteriores (como los planteamientos iniciales sobre resiliencia de la Comunicación de 2018 o ciertos modelos conceptuales del decenio pasado) partían de un escenario donde la amenaza híbrida se entendía como un fenómeno esencialmente difuso, intangible y de baja intensidad. El inicio de la invasión a gran escala de Ucrania en 2022 y las posteriores acciones físicas clandestinas en el mar Báltico entre 2024 y 2025 (como los incidentes del petrolero *Eagle S*) han hecho necesaria una revisión de esas lecturas protectoras y reactivas.

De este modo, al confrontar la literatura fundacional con la realidad de 2026 se demuestra que, si bien las herramientas físicas se emplean cada vez de manera más directa, los pilares de la intencionalidad maliciosa —la negación plausible, la manipulación de los umbrales de detección descrita por Giannopoulos et al. (2021) o la explotación del vértice ciudadano— siguen siendo plenamente vigentes. Lo que ha mutado no es la naturaleza de la hibridez, sino la tolerancia al riesgo de los agresores, obligando a la Unión Europea a transformar de urgencia sus marcos doctrinales en cajas de herramientas operativas (*toolboxes*).

Esta discusión acerca del corpus revisado, realizada a lo largo de cuatro subapartados, ha proporcionado algunos datos de interés que se incorporan a las conclusiones extraídas del análisis en sí mismo de las fuentes seleccionadas.

4. Conclusiones

A lo largo del presente Trabajo de Fin de Máster se ha estudiado la respuesta de la inteligencia comunitaria europea a las amenazas que han cobrado especial protagonismo en la última década. El principal reto para la Unión proviene de la asimetría entre las acciones híbridas —coordinadas, negables y que actúan por debajo del umbral del conflicto abierto— y esa respuesta de inteligencia, que proporciona capacidades de análisis pero que está estructuralmente limitada. El método empleado para este análisis es el de una revisión sistemática cualitativa, basada en una adaptación de PRISMA 2020, sobre 42 documentos (con apoyos hemerográficos adicionales) y con un alcance temporal que abarca desde 2014 a 2026.

Sobre la base de lo anteriormente descrito, se presentan las siguientes conclusiones:

Primera.- Se han identificado tres fuentes de amenazas principales para el conjunto de la Unión Europea en las que el empleo de estrategias híbridas es reseñable. El primer lugar lo ocupa Rusia, probablemente el actor más sofisticado al que se atribuyen diversas operaciones FIMI, sabotajes y acciones en la zona gris. El flanco sur, conformado por las regiones geográficas del Magreb y el Sahel, supone un reto en cuanto a la necesidad de anticipación y monitorización de amenazas y riesgos tan dispares como la instrumentalización de flujos migratorios, la inestabilidad saheliana o las interconexiones energéticas y de comunicaciones. China cierra esta tríada, expandiendo su influencia de manera lenta pero constante, haciendo uso de su poderío económico y de la denominada en el ámbito del análisis internacional "diplomacia de la sonrisa". Con todo, el rasgo definitorio de estas amenazas no es el uso de cada uno de los instrumentos reseñados, sino su orquestación bajo el umbral del conflicto armado y su dimensión cognitiva.

Segunda.- Como respuesta a este amplio abanico de amenazas, la Unión Europea ha sido capaz de articular, a lo largo de la última década, una capacidad de análisis y fusión de información, materializada en la SIAC, el EU INTCEN y la Célula de Fusión Híbrida, complementadas por el SatCen. Además, la relación con la OTAN ha conseguido superar las tensiones políticas y ha limitado los riesgos de solapamiento, evolucionando hacia una cooperación funcional progresiva, aunque pendiente aún de un reparto explícito de cometidos operativos. No obstante, la atipicidad de la UE como actor de inteligencia resulta en la ausencia de capacidad autónoma de obtención, más allá del ámbito OSINT y de la IMINT

que pueda proporcionar el SatCen. Es decir, la Unión tiene capacidad de "diagnóstico", pero adolece de la imposibilidad de "observar" por sí misma.

Tercera.- Esta carencia de obtención de inteligencia es, precisamente, el principal reto en este ámbito para la Unión, o, si se prefiere, la raíz de las limitaciones estudiadas, pues de ella derivan la dependencia de la contribución voluntaria de los Estados —asentada, a su vez, sobre relaciones de confianza— y la fragmentación institucional. Este inconveniente no deriva, sin embargo, de una escasez de medios, sino de una arquitectura deliberada: el artículo 4.2 del TUE limita las capacidades comunitarias, algo que, como pone de manifiesto el reparto competencial en el ámbito de la seguridad interior, es necesariamente deliberado.

Cuarta.- Así las cosas, la centralización de la inteligencia europea es, al menos, a día de hoy, inviable. Los Tratados actualmente vigentes lo impiden y el riesgo de disfuncionalidad en caso de llevarla a cabo es elevado. Sirva además como muestra de su escasa viabilidad el episodio protagonizado, entre noviembre de 2025 y febrero de 2026, por la presidenta de la Comisión Europea y la Alta Representante de la Unión. En el panorama actual, la vía realista la constituye la integración pragmática de capacidades nacionales y comunitarias, basada en la "infraestructura blanda", el ICE como herramienta para desarrollar la cultura estratégica común, el refuerzo de la SIAC y de las capacidades de obtención existentes —OSINT y SatCen— y la asunción del "minilateralismo" como estrategia ineludible. En opinión del autor, esta aproximación mitiga la asimetría sin resolverla, pero es la mejor opción posible.

Este Trabajo de Fin de Máster pretende ofrecer una síntesis sistemática sobre la materia acotada al periodo de 2014-2026 y realizar un análisis preciso del marco competencial, sin olvidar la actualidad institucional. Para concluir, desde un enfoque más prospectivo, resulta complicado aventurar la dirección que tomará la comunidad de inteligencia europea, pero probablemente resulten significativos —y sirvan, por tanto, de indicadores predictivos— la evolución de la unidad propuesta por Ursula von der Leyen, la trayectoria del ICE, la consecución de una autonomía real en el ámbito GEOINT o los resultados de la Brújula Estratégica más allá de 2026. Todos estos indicadores permitirían hacerse una idea de en qué sentido avanza y qué probabilidades reales de éxito tiene la integración de capacidades. Esta parece ser la vía más realista para dotar a la UE de herramientas para hacer frente a las amenazas híbridas desde el ámbito de la inteligencia, lo que no descarta, en el futuro, que una nueva reforma de los Tratados, impulsada por una cesión o compartición de soberanía de los

Estados miembros, permita la creación de un Servicio de Inteligencia Europeo. Hoy por hoy, no obstante, no es una opción viable y, en cualquier caso, la integración funcional de capacidades es necesaria para el presente y muy aconsejable como paso previo a cualquier proyecto más ambicioso.

Referencias bibliográficas

Bibliografía básica

- Anagnostakis, D. (2025). "Taming the Storm" of Hybridity: The EU-NATO Relationship on Countering Hybrid Threats – From Functional Overlap to Functional Cooperation. *Defence Studies*, *25(3),* 587-611. https://doi.org/10.1080/14702436.2025.2464636
- Arco Escriche, I. (2026). La República Popular de China y la intensificación de su estrategia híbrida en Taiwán: doctrina, prácticas e implicaciones para la Unión Europea. En *Panorama Estratégico* 2026 (pp. 99-119). Instituto Español de Estudios Estratégicos.
- Aznar Fernández-Montesinos, F. (2023). Teoría de la guerra y relato. La zona gris. *Araucaria, 25*(52), 419–441. https://doi.org/10.12795/araucaria.2023.i52.19
- Barras Tejudo, R., y García Cantalapiedra, D. J. (2020). *Hacia un «gran Magreb». La UE, la seguridad europea y el declive del concepto MENA* (Documento de Opinión 59/2020). Instituto Español de Estudios Estratégicos.
- Benedicto, M. Á. (2025). La desinformación como amenaza híbrida: respuestas institucionales de la Unión Europea. *Behavior & Law Journal*, *11(1)*, 32-42. https://doi.org/10.47442/blj.2025.125
- Borghoff, U. M., Berger, L., y Fischer, F. (2024). The Intelligence College in Europe: An effort to create a European intelligence community. *Connections: The Quarterly Journal, 23(1),* 133-143. https://doi.org/10.11610/Connections.23.1.03
- Camarero Orive, A. (2026). Los puertos y la seguridad nacional. Los choke points y la geoestrategia mundial. En *Puertos del Estado y la defensa nacional* (Cuaderno de Estrategia 234, pp. 177-207). Instituto Español de Estudios Estratégicos.
- Colom Piella, G. (2019). *La amenaza híbrida: mitos, leyendas y realidades* (Documento de Opinión 24/2019). Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO24_2019GUICOL-hibrida.pdf
- Colom Piella, G. (2023). Pensamiento militar ruso y suposiciones sobre la zona gris y la guerra en Ucrania. *Revista de Pensamiento Estratégico y Seguridad CISDE, 8(2)*, 91-103.

- Colom Piella, G. (2026). *Desdibujar el umbral: zona gris, atribución y coerción acumulativa* (Documento de Opinión 47/2026). Instituto Español de Estudios Estratégicos. https://www.defensa.gob.es/documents/2073105/3095923/ieee-2026-zona-gris-opinion47.pdf/
- Dezcallar, J. (2022). *Abrazar el mundo*. La Esfera de los Libros.
- Díaz-Caneja, J. M. (2014). *La cooperación de inteligencia en la Unión Europea* (Documento de Opinión 151/2014). Instituto Español de Estudios Estratégicos.
- Fägersten, B. (2016). For EU eyes only? Intelligence and European security (Brief n.º 8). European Union Institute for Security Studies. https://doi.org/10.2815/674916
- Forti, M. (2023). Belarus-sponsored migration movements and the response by Lithuania, Latvia, and Poland: A critical appraisal. *European Papers, 8(1)*, 227-238. https://doi.org/10.15166/2499-8249/648
- Freedman, J., Gjørv, G. H., y Razakamaharavo, V. T. (2021). Identity, stability, Hybrid Threats and Disinformation. *Revista ICONO14*, *19(1),* 38-69. https://doi.org/10.7195/ri14.v19i1.1618.
- Geri, M. (2024). Understanding Russian hybrid warfare against Europe in the energy sector. *Journal of Strategic Security, 17(3)*, 15-34. https://doi.org/10.5038/1944-0472.17.3.2270
- Giannopoulos, G., Smith, H., y Theocharidou, M. (Eds.). (2021). *The landscape of hybrid threats: A conceptual model* (EUR 30585 EN). Publications Office of the European Union. https://doi.org/10.2760/44985
- González López, D. (2024). La integración europea en materia de inteligencia: ¿un servicio de inteligencia europeo? *Studia Humanitatis Journal*, *4(2)*, 1-19. https://doi.org/10.33732/shj.v4i2.113
- Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
- Molina Urosa, M., Lafuente Capó, J., Lopera Rodríguez, M., Ruiz Sancho, L., Terrés Pueyo, G., y García Hernández, P. (2026). *Infraestructura crítica en contexto de guerra híbrida: cables submarinos, competición geopolítica y vulnerabilidad estructural en el mar Báltico*. Instituto Español de Estudios Estratégicos. https://www.defensa.gob.es/ceseden/-/ieee/infraestructura-critica-contexto-guerra-

hibrida-cables-submarinos-competicion-geopolitica-vulnerabilidad-estructural-mar-baltico

- Navarro Paredes, Á. (2026). *La información en la guerra híbrida. Propuesta de un modelo predictivo temprano* (Documento de Opinión 02/2026). Instituto Español de Estudios Estratégicos. https://www.defensa.gob.es/ceseden/-/ieee/informacion-guerra-hibrida-propuesta-modelo-predictivo-temprano
- Niinistö, S. (2024). *Safer together: Strengthening Europe's civilian and military preparedness and readiness*. European Commission. https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en
- Nilsson, N., Weissmann, M., y Palmertz, B. (2026). Hybrid threats and the intelligence community: Priming for a volatile age. *International Journal of Intelligence and CounterIntelligence*, *39(1)*, 109-131. https://doi.org/10.1080/08850607.2024.2435265
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. https://doi.org/10.1136/bmj.n71
- Páramo, A. (2022). El analista de inteligencia de última generación. En F. Arteaga y D. Ríos Insúa (Coords.), *El analista de inteligencia en la era digital* (pp. 21-29). Real Instituto Elcano y Centro Nacional de Inteligencia. https://www.realinstitutoelcano.org/monografias/el-analista-de-inteligencia-en-la-era-digital
- Petticrew, M., y Roberts, H. (2006). *Systematic reviews in the social sciences: A practical guide*. Blackwell Publishing.
- Quiñones de la Iglesia, F. J. (2020). *Una revisión del concepto «guerra híbrida/actor híbrido»* (Documento de Opinión 153/2020). Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO153_2020FRAQUI_guerrahibrida.pdf

- Rodríguez, Á., y Solé, J. (2025). Ceuta and Melilla as a strategic hotspot: A strategic playbook for Spanish policymaking (Natolin Policy Papers Series, vol. 5, n.º 2/2025). College of Europe in Natolin.
- Sánchez Herráez, P. (2021). *Comprender la guerra híbrida... ¿el retorno a los clásicos? (reedición)* (Documento de Análisis 42/2021). Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/docs_analisis/2021/DIEEEA42_2021_PEDSAN_Guerra.pdf
- Sánchez Peláez, L. (2021). *El COSI y el proceso de integración europea en seguridad interior* [Tesis doctoral, Universidad Nacional de Educación a Distancia].
- Sansó-Rubert Pascual, D. (2025). Ceuta y Melilla: ¿casus belli España-Marruecos? *Revista de Estudios en Seguridad Internacional, 11(1)*, 141-159.
- Terrero Carrobles, J. J. (2025). *El cambio de estrategia del espionaje ruso en Europa* (Documento de Opinión 95/2025). Instituto Español de Estudios Estratégicos.
- Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., et al. (2018). PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and explanation. *Annals of Internal Medicine*, *169(7)*, 467-473. https://doi.org/10.7326/M18-0850
- Trujillo Álvarez, P. (2024). La tríada de la guerra de Clausewitz: un modelo en evolución para el análisis de conflictos. *Seguridad y Poder Terrestre*, *3(4)*, 21-42. https://doi.org/10.56221/spt.v3i4.69
- Tuinier, D. H. (2025). *The social ties that bind: The role of social relations and trust in EU intelligence cooperation* [Tesis doctoral, Universiteit Leiden]. Leiden University Scholarly Publications. https://hdl.handle.net/1887/4177160
- Weissmann, M. (2023). Chinese and other foreign influence in Serbia and the Western Balkans: A tale of cooperation, competition, and distrust*? Connections: The Quarterly Journal*, *22(4)*, 9-26. https://doi.org/10.11610/Connections.22.4.01

Bibliografía complementaria

- Comisión Europea. (2020). Primer informe de situación sobre la Estrategia de la UE para una Unión de la Seguridad [COM(2020) 797 final].
- Comisión Europea y Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. (2016). Comunicación conjunta. Lucha contra las amenazas híbridas: una

respuesta de la Unión Europea [JOIN(2016) 18 final]. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016JC0018

- Comisión Europea y Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. (2018). Comunicación conjunta. Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas [JOIN(2018) 16 final]. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018JC0016
- Consejo de la Unión Europea. (2022a). Conclusiones del Consejo sobre un marco para una respuesta coordinada de la UE a las campañas híbridas (Documento 10016/22).
- Consejo de la Unión Europea. (2022b). Una Brújula Estratégica para la Seguridad y la Defensa (Documento 7371/22). https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf
- Consejo de la Unión Europea. (2026). Conclusiones del Consejo sobre el desarrollo de la capacidad de la Unión Europea para luchar contra las amenazas híbridas (Documento 7349/26). https://data.consilium.europa.eu/doc/document/ST-7349-2026-INIT/es/pdf
- Servicio Europeo de Acción Exterior. (2015). *EU Intelligence and Situation Centre (EU INTCEN)* [Ficha informativa]. Statewatch. https://statewatch.org/wp-content/uploads/2026/04/eu-intcen-factsheet.pdf
- Servicio Europeo de Acción Exterior. (2025). *Annual progress report on the implementation of the Strategic Compass for Security and Defence* [Informe anual de situación sobre la aplicación de la Brújula Estratégica para la Seguridad y la Defensa] (Documento del Consejo 8023/25). https://data.consilium.europa.eu/doc/document/ST-8023-2025-INIT/en/pdf
- Servicio Europeo de Acción Exterior. (2026). *4th EEAS report on foreign information manipulation and interference (FIMI) threats: Dismantling the FIMI house of cards*. Unión Europea.
- Unión Europea y Organización del Tratado del Atlántico Norte. (2023, 10 de enero). *Joint Declaration on EU-NATO Cooperation*. https://www.consilium.europa.eu/en/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/

Legislación citada

- Tratado de la Unión Europea (versión consolidada). *Diario Oficial de la Unión Europea*, C 202, de 7 de junio de 2016.
- Tratado de Funcionamiento de la Unión Europea (versión consolidada). *Diario Oficial de la Unión Europea*, C 202, de 7 de junio de 2016.

Fuentes hemerográficas

- Foy, H. (2025, 11 de noviembre). EU to set up new intelligence unit under Ursula von der Leyen. *Financial Times*. https://www.ft.com/content/b8a3aee3-222b-4b4f-a1e2-e7a819ac0dd2
- Roussi, A., y Barigazzi, J. (2026, 9 de febrero). *Von der Leyen softens plan for intelligence cell*. POLITICO. https://www.politico.eu/article/ursula-von-der-leyen-backs-down-intelligence-cell-plan/
- Wax, E. (2025, 17 de noviembre). *EU's top diplomat Kallas rejects Commission's proposed intelligence 'cell'*. Euractiv. https://www.euractiv.com/news/eus-top-diplomat-kallas-rejects-commissions-proposed-intelligence-cell/

Listado de abreviaturas

- AIS: *Automatic Identification System*. En español, Sistema de Identificación Automático. Sistema que emite en abierto la identidad, posición y otros datos de buques en navegación.
- BRI: *Belt and Road Initiative*. En español, Iniciativa de la Franja y la Ruta desplegada por China.
- COSI: Comité Permanente de Cooperación Operativa en materia de Seguridad Interior.
- EEAS: *European External Action Service*. En español, Servicio Europeo de Acción Exterior (SEAE).
- FIMI: *Foreign Information Manipulation and Interference*. En español, Manipulación de la Información e Injerencia Extranjera.
- GEOINT: *Geospatial Intelligence*. En español, Inteligencia Geoespacial.
- GPS: *Global Positioning System*. En español, Sistema de Posicionamiento Global.
- HUMINT: *Human Intelligence*. En español, Inteligencia de Fuentes Humanas.
- ICE: *Intelligence College in Europe*. En español, Colegio de Inteligencia en Europa.
- IEEE: Instituto Español de Estudios Estratégicos.
- IMINT: *Imagery Intelligence*. En español, Inteligencia de Imágenes.
- INTCEN: *Intelligence and Situation Centre*. En español, Centro de Inteligencia y Situación de la Unión Europea.
- MENA: *Middle East and North Africa*. En español, Oriente Medio y norte de África.
- NRBQ: referido a un riesgo o amenaza, nuclear, radiológico, biológico y químico.
- OSINT: *Open Source Intelligence*. En español, Inteligencia de Fuentes Abiertas.
- OTAN: Organización del Tratado del Atlántico Norte.
- PCSD: Política Común de Seguridad y Defensa de la Unión Europea.
- PESC: Política Exterior y de Seguridad Común de la Unión Europea.
- PRISMA: *Preferred Reporting Items for Systematic reviews and Meta-Analyses*. Guía para la redacción de revisiones sistemáticas y metaanálisis.
- SatCen: Centro de Satélites de la Unión Europea.
- SIAC: *Single Intelligence Analysis Capacity*. En español, Capacidad Única de Análisis de Inteligencia de la Unión Europea.
- SIGINT: *Signals Intelligence*. En español, Inteligencia de Señales.
- TFUE: Tratado de Funcionamiento de la Unión Europea.
- TUE: Tratado de la Unión Europea.
- UE: Unión Europea.
- URSS: Unión de Repúblicas Socialistas Soviéticas.