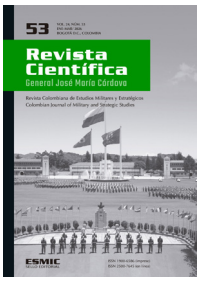

Revista Científica General José María Córdova
Revista Colombiana de Estudios Militares y Estratégicos

Bogotá D.C., Colombia
ISSN 1900-6586 (impreso), 2500-7645 (en línea)
https://doi.org/10.21830/19006586.1545

ARTÍCULO DE INVESTIGACIÓN

Sistemas anticipatorios y la función de inteligencia: sistemas de actores no estatales y análisis de redes multicapa

Anticipatory Systems and the Intelligence Function: Systems of Non-State Actors and Multilayer Network Analysis

Rubén Arcos
Universidad Rey Juan Carlos, España
ruben.arcos@urjc.es
Marina Alonso-Villota
Instituto Universitario General Gutiérrez Mellado (IUGM-UNED), España
malonso1139@alumno.uned.es
Rudy Milani
University of the Bundeswehr Munich, Alemania
rudy.milani@unibw.de

Citación APA: Arcos, R., Alonso-Villota, M., & Milani, R. (2026). Sistemas anticipatorios y la función de inteligencia: sistemas de actores no estatales y análisis de redes multicapa. *Revista Científica General José María Córdova, 24*(53), 159-179.
https://doi.org/10.21830/19006586.1545

Publicado en línea: 20 de febrero de 2026

Enviar un artículo a la Revista

Revista Científica General José María Córdova
Revista Colombiana de Estudios Militares y Estratégicos

Bogotá D.C., Colombia
Volumen 24 número 53, enero-marzo 2026, pp. 159-179
https://doi.org/10.21830/19006586.1545

ARTÍCULO DE INVESTIGACIÓN

Sistemas anticipatorios y la función de inteligencia: sistemas de actores no estatales y análisis de redes multicapa

Anticipatory Systems and the Intelligence Function: Systems of Non-State Actors and Multilayer Network Analysis

Rubén Arcos
Universidad Rey Juan Carlos, España
Marina Alonso-Villota
Instituto Universitario General Gutiérrez Mellado (IUGM-UNED), España
Rudy Milani
University of the Bundeswehr Munich, Alemania

RESUMEN. Este artículo discute el concepto de sistemas anticipatorios y las implicaciones de su aplicación en el ámbito de la seguridad y la acción exterior de la Unión Europea; explora la función de inteligencia como parte de los sistemas anticipatorios para la toma de decisiones en materia de seguridad y defensa, y analiza las configuraciones de los sistemas anticipatorios frente a diferentes amenazas y desafíos a la seguridad. En particular, desarrolla el enfoque conceptual de los Sistemas de Actores No Estatales (SNSA) operacionalizándolo mediante el modelo de análisis de redes multicapa aplicado al estudio de caso del SNSA de la organización terrorista Euskadi Ta Askatasuna. La introducción de esta perspectiva facilita el análisis integral de la amenaza y contribuye a la comprensión y predicción del comportamiento de los actores involucrados.

Palabras clave: inteligencia; seguridad; sistema de actores no estatales; sistemas anticipatorios; terrorismo

ABSTRACT. This article discusses the concept of anticipatory systems and their implications for the security and external action of the European Union. It explores the role of intelligence within anticipatory systems for security and defense decision-making and analyzes the configurations of such systems in the face of diverse security threats and challenges. In particular, it develops the conceptual approach of the System of Non-State Actors (SNSA), operationalizing it through the multi-layered network analysis model applied to the case study of the SNSA of the terrorist organization Euskadi Ta Askatasuna. The introduction of this perspective facilitates comprehensive threat analysis and contributes to understanding and predicting the behavior of the actors involved.

Keywords: intelligence; security; System of Non-State Actors; anticipatory systems; terrorism

Recibido: 24 de mayo de 2025 • **Aceptado:** 1 de febrero de 2026

Contacto: Rubén Arcos ruben.arcos@urjc.es

Introducción

Los Estados, como actores clave de la seguridad internacional, cuentan con sistemas de inteligencia para informar la toma de decisiones de las autoridades y reducir la incertidumbre de los decisores políticos en materia de seguridad y defensa. Los sistemas de inteligencia proporcionan diferentes tipos de productos analíticos y valoraciones sobre amenazas actuales procedentes de otros Estados y de actores no estatales, como organizaciones terroristas que emplean la violencia y producen masacres con sus atentados para obtener objetivos políticos, y también grupos de crimen organizado que, además de desarrollar todo tipo de tráficos ilícitos y actividades ilegales, socavan la estabilidad de los Estados a los que parasitan mediante la corrupción. Los objetivos de los sistemas de inteligencia pueden ser, a su vez, no solamente actores no estatales aislados, sino conformar sistemas complejos (Clark, 2004). Los Sistemas de Actores No Estatales o SNSA (Sytem of Non-State Actors, por sus siglas en inglés) combinan tácticas convencionales y no convencionales atacando las instituciones democráticas y los derechos humanos (Alonso-Villota & Arcos, 2024).

Los servicios de inteligencia proporcionan, con sus fuentes propias y métodos especiales, inteligencia actual, estratégica y anticipatoria a sus clientes gubernamentales y otros consumidores de inteligencia sobre amenazas y desafíos para la seguridad de los Estados y de sus ciudadanos. Desde el punto de vista de los objetivos de inteligencia o de las prioridades a las que los servicios deben atender de acuerdo con su misión, el concepto de *amenaza*, como ha señalado Gregory Treverton (2009), puede entenderse como un espectro: en un extremo se encontrarían las amenazas que conllevan actores de la amenaza con intenciones deliberadamente hostiles o de infligir daños; en el otro extremo, se encuentran, de acuerdo con esta lógica, aquellas amenazas sin actores de la amenaza o amenazas sistémicas en que la amenaza se constituye como efecto acumulativo de las acciones tomadas sin una intención deliberadamente hostil, como es el caso de la propagación de patógenos en epidemias y pandemias, el cambio climático de origen antropogénico o los efectos políticos y económicos no deseados de afluencias migratorias masivas en los países receptores (Treverton, 2009; Arcos, 2023).

El amplísimo espectro de necesidades informativas, actuales y potenciales, de los tomadores de decisiones sobre amenazas y desafíos para la seguridad de los Estados y de sus ciudadanos a los que los servicios de inteligencia están llamados a responder con eficacia y oportunidad en el entorno de seguridad actual sugiere la necesidad de contar de igual modo con un amplísimo equipo de expertos con conocimientos y competencias. Unas capacidades que no todos los Estados están en posición de permitirse, pero que además suponen un desafío desde el punto de vista de su mantenimiento e incremento eventual como medios propios, ante la posible materialización de amenazas latentes.

De otra parte, desde el punto de vista de las decisiones que en materia de seguridad y defensa la inteligencia tiene por objeto informar, los análisis y valoraciones de los servicios de inteligencia pueden considerarse como una parte importante, si bien no la única, de los

inputs especializados que reciben los tomadores de decisiones. Es decir, una contribución de altísimo valor dentro del *pool* de información cualificada y complementaria susceptible de ser incorporada al proceso de toma de decisiones.

Arcos y Palacios (2025) han introducido la perspectiva de los sistemas anticipatorios para el caso de estudio de un actor internacional como es la Unión Europea (UE) y que es ilustrativa de lo anterior. De acuerdo con esta perspectiva, la UE cuenta con todo un sistema anticipatorio que abarca diferentes estructuras que fundamentan su proceso de toma de decisiones en materia de seguridad y diplomacia, así como su acción exterior (Arcos & Palacios, 2025, p. 3). Este sistema anticipatorio opera con la inteligencia proporcionada por la *Single Intelligence Analysis Capacity* (SIAC) pero también con otros tipos de análisis e informaciones para fundamentar las decisiones en curso y orientar el comportamiento actual. De acuerdo con estos autores, las estructuras de la UE que proporcionan análisis de inteligencia forman parte del sistema anticipatorio, pero este dispone además de otras estructuras que realizan contribuciones como análisis prospectivos, imágenes satelitales e información geoespacial, información científica y análisis cualificados basados en fuentes abiertas de información (Arcos & Palacios, 2025, p. 3). Se trata de una perspectiva similar a la que plantean Calof y Bishop (2020) para el caso de las organizaciones empresariales y que considera como parte del sistema anticipatorio de la organización funciones como la prospectiva, la inteligencia competitiva, el *environmental scanning* y otros sistemas de detección. En el caso de estudio de la UE, las contribuciones complementarias a las de las capacidades de inteligencia de su sistema anticipatorio consistirían, de acuerdo con Arcos y Palacios (2025, pp. 4-5), en aportaciones de otras estructuras en áreas políticas específicas:

- Terrorismo y delincuencia organizada. Ejemplo: valoraciones de la amenaza de Europol como el EU-SOCTA 2025 (European Union Agency for Law Enforcement Cooperation, 2025).
- Ciberseguridad. Ejemplo: los informes de prospectiva de amenazas de ciberseguridad elaborados por ENISA (European Union Agency for Cybersecurity, 2024).
- Desinformación y manipulación e interferencia de información extranjera. Ejemplo: los informes de la División de Comunicación Estratégica, Grupos de Trabajo y Análisis de la Información del Servicio Europeo de Acción Exterior (European Union External Action, 2025).
- Fronteras y guardacostas. Ejemplo: análisis de riesgos y situacional de FRONTEX, la Agencia Europea de la Guardia de Fronteras y Costas (FRONTEX, 2025).
- Amenazas híbridas. Ejemplo: productos de investigación y análisis del Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas —*Hybrid CoE*— (Hybrid CoE, 2025).

Los sistemas anticipatorios son, de acuerdo con Robert Rosen (1985), "sistemas que contienen modelos predictivos internos de sí mismos o de su entorno, y que utilizan las pre-

dicciones de sus modelos para controlar su comportamiento actual"[1] (p. vii). Según Rosen, "un comportamiento anticipatorio es aquel en que se produce un cambio de estado en el presente en función de un estado futuro previsto, y el agente mediante el cual se realiza la predicción debe ser, en el sentido más amplio, un modelo"[2], y resultan abundantes los ejemplos de comportamiento anticipatorio en los diferentes niveles de organización biológica y es gran parte de nuestro comportamiento humano consciente también de esta naturaleza (Rosen, 1985, p. 8).

Como función de apoyo a la toma de decisiones, la inteligencia contribuye al sistema anticipatorio de seguridad y defensa mediante análisis situacional, explicativo, predictivo y anticipatorio para apoyar la toma de decisiones en tiempos de paz y de guerra (Omand, 2010; Arcos, 2023). Esta conceptualización de la inteligencia desde un enfoque funcionalista puede identificarse en teorizaciones tempranas como las de Lasswell (1942; Arcos, 2023). No obstante, reconociendo que la producción de conocimiento especializado de interés para la seguridad y la defensa, a través de la investigación y el análisis, no es algo exclusivo de los servicios de inteligencia, es posible plantear sistemas anticipatorios capaces de nutrirse de forma complementaria de esa otra experticia y de sus productos en forma de inteligencia OSINT comercial, investigación académica en seguridad internacional y defensa, análisis y valoraciones sobre amenazas y desafíos a la seguridad elaborados en el contexto de centros de excelencia multinacionales, o información procedente de sistemas de alerta temprana en el contexto de la prevención de conflictos o la protección civil.

Este enfoque es consistente con el *comprehensive approach* o enfoque integral a partir de la combinación de instrumentos políticos, civiles y militares prescrito por la Organización del Tratado del Atlántico Norte (OTAN, 2024). De acuerdo con esta doctrina, "la implementación de este enfoque integral es fundamental en muchas actividades recientes y actuales de la OTAN, como su contribución a la lucha de la comunidad internacional contra el terrorismo y los esfuerzos para promover la estabilidad, así como su papel en la respuesta a las amenazas híbridas" (OTAN, 2024).

Es precisamente en el contexto de la lucha contra las organizaciones terroristas y la respuesta frente a amenazas híbridas en que se inscribe este artículo, desde el planteamiento ya enunciado, que tiene como objetivo profundizar en el análisis de la amenaza mediante marcos analíticos y métodos que contribuyan a la comprensión y predicción del comportamiento de los actores involucrados. En particular, toma como punto de partida el enfoque conceptual del SNSA, y lo operacionaliza a través del modelo de análisis de redes multicapa.

1 Traducción de los autores.

2 Traducción de los autores.

Marco teórico

Uno de los problemas fundamentales a los que se enfrentan los sistemas anticipatorios es precisamente contar con buenos modelos internos capaces de proporcionar predicciones precisas basadas en un conocimiento adecuado de sí mismos y del entorno operativo. En este sentido, el análisis y valoración de vulnerabilidades internas sistémicas que pudieran ser explotadas por actores de la amenaza forma parte de las actividades planteadas en el contexto de la respuesta holística frente a amenazas híbridas. Si bien la perspectiva de amenazas híbridas reconoce el papel de actores estatales y también no estatales, estos últimos se encuentran comparativamente investigados en menor medida y, cuando son objeto de investigación, suelen serlo en su condición de *proxies* de los actores estatales. Además, los actores no estatales se han analizado principalmente en relación con las tácticas violentas e ilegales que realizan, obviando aquellas no violentas e incluso legales, que algunos han demostrado utilizar de manera combinada (Alonso-Villota & Arcos, 2024).

En este sentido, el Marco Analítico de Coerción-Manipulación-Persuasión (CMPF) desarrollado por los autores persigue proporcionar comprensión sobre el *modus operandi* de los SNSAs desde una perspectiva holística (Alonso-Villota & Arcos, 2024). Este marco, "combina modos de influencia (es decir, coerción, manipulación y persuasión) con diferentes categorías (es decir, física/material, simbólica, institucional y estratégica) para facilitar la elaboración de hipótesis sobre las tácticas que podrían emplearse y guiar su análisis" (Alonso-Villota & Arcos, 2024, p. 3). El concepto de SNSA, planteado por los autores debe entenderse como,

> un conjunto de entidades (personas u organizaciones) que comparten una ideología y objetivos políticos estratégicos específicos, y cuyos líderes trabajan para lograrlos con cierto grado de coordinación y/o colaboración. Un SNSA puede representar una amenaza para la seguridad cuando su ideología y objetivos estratégicos atentan contra los derechos humanos y/o buscan socavar los valores e instituciones democráticas. (Alonso-Villota & Arcos, 2024, 5)

Lejos de aspirar a criminalizar a todas las entidades involucradas, el enfoque del SNSA establece el límite analítico en el sistema más amplio que los actores consolidan: reconoce, primero, que tanto las entidades legales como las ilegales o alegales que participan en tácticas de diversa legalidad pueden ser parte de dicho sistema, y, segundo, que la combinación de tácticas y entidades de tan diverso estatus legal puede convertirse en una amenaza para los derechos humanos y para los valores e instituciones democráticos, sobre todo cuando está diseñada estratégicamente para eso (Alonso-Villota & Arcos, 2024). Esta amenaza ha sido ampliamente evidenciada por los análisis realizados sobre el *modus operandi* de los actores estatales desde la perspectiva de las amenazas híbridas (Giannopoulos et al., 2021), pero sigue siendo poco investigada en su aplicación a los actores no estatales. Al operar en conjunto y no como la suma de sus partes, los SNSAs han demostrado la capacidad de po-

tenciar el efecto de sus tácticas, logrando efectos cascada, aprovechando vulnerabilidades sistémicas de los sistemas democráticos —tales como el derecho a la libertad de expresión o el derecho a la asociación política— y facilitando su adaptación a los entornos en que operan (Alonso-Villota & Arcos, 2024).

La operacionalización de marcos conceptuales como métodos analíticos es crucial para la generación de inteligencia que informe sistemas anticipatorios en el estudio de los SNSAs. Ante todo, el primer paso es entender su estructura y desarrollo para poder comprender su comportamiento y dinámicas subyacentes, desde una perspectiva lo más comprensible posible. Durante décadas, una amplia gama de problemas complejos se ha analizado y estudiado mediante el uso de la representación compleja de redes, ya que facilita la extracción de más información que las metodologías tradicionales, tales como la identificación de características ocultas de los datos mediante el cálculo de métricas abstractas centradas en meras estructuras gráficas (Wasserman & Faust, 1994). En particular, el análisis de redes sociales (SNA, por sus siglas en inglés) permite analizar la estructura, las relaciones y el rendimiento de un conjunto de actores incluidos en un límite analítico definido. Las redes sociales se modelan fácilmente como grafos, definiendo el alcance bajo ciertas reglas de relación específicas y considerando las diferentes entidades como nodos. Si bien la formalización de este tipo de datos es sencilla, las aplicaciones y los problemas reales que se pueden abordar son múltiples.

El SNA se originó en la década de 1930 en el campo de la sociometría, pero no fue hasta finales de los años 1970 y 1980 cuando profesionales de la sociología, psicología social y antropología desarrollaron el enfoque que, para finales de los años 1990, se había convertido en una "perspectiva analítica madura y autoconsciente"[3] (Wetherell, 1998, p. 126). En el campo de los estudios sobre terrorismo, la teoría de redes llevó a varios autores a reconocer la estructura cada vez más interconectada de las organizaciones criminales, que debía ser contrarrestada mediante enfoques asimétricos (Arquilla & Ronfeldt, 2001). Sin embargo, fue tras los atentados del 11S cuando los métodos de redes sociales se posicionaron rápidamente como herramientas analíticas importantes para comprender y combatir el terrorismo (Perliger & Pedahzur, 2011; Zech & Gabbay, 2016). Poco después del 11S, la principal organización de redes sociales, la International Network for Social Network Analytics (INSNA), publicó un número sobre SNA y terrorismo que abordaba explícitamente el papel potencial del SNA, incluyendo artículos de referencia como los de Krebs (2002) y Carley et al. (2002).

El SNA se ha utilizado desde entonces para analizar diversos temas, como el surgimiento de las células responsables de atentados terroristas (Magouirk et al., 2008) y su estructura (Rodriguez, 2005), la detección de clústeres dentro de redes terroristas más amplias (Sageman, 2004), la dinámica interna de células terroristas (Koschade, 2007) y redes suicidas

3 Traducción de los autores.

(Pedahzur & Perliger, 2006), la red de los llamados *lobos solitarios* (Hoffman, 2018), las comunidades extremistas en línea y sus discursos (Downing et al., 2022), y la formación de redes radicales y su relación con su comunidad de referencia (Malthaner, 2018). Además, se han desarrollado diversos modelos y métodos de SNA para profundizar en diferentes elementos de las organizaciones terroristas, como la estimación de vulnerabilidades dentro de las redes terroristas para desestabilizarlas (Carley, 2004) y la detección de cambios significativos en la estructura y sus posibles causas (Everton & Cunningham, 2013).

A pesar de los grandes avances en el entendimiento de organizaciones terroristas, este enfoque y aplicación presenta varias limitaciones. La mayoría de los análisis de redes sociales realizados en el ámbito del terrorismo se ha centrado en el análisis intraorganizacional utilizando nodos a nivel individual (es decir, los individuos que pertenecen a una organización terrorista) como unidad de análisis (Zech & Gabbay, 2016). Esto ha permitido medir las relaciones individuales según diferentes naturalezas y pesos, como los vínculos débiles (relaciones con conocidos) y los fuertes (familiares y amigos cercanos) (Granovetter, 1973), el tiempo que los individuos pasan juntos (Krebs, 2002) y las relaciones familiares, amistades a largo plazo y conocidos (Pedahzur & Perliger, 2006).

Sin embargo, según el conocimiento de los autores, aún no se ha aplicado para evaluar los vínculos de la organización terrorista (entendida como un solo nodo) con sus entidades colaboradoras, principalmente desde el entendimiento de su consolidación como un sistema complejo y no la suma de sus partes. Por ello, expandir el foco de análisis de la organización terrorista —entendida como un sistema en sí— al sistema integral en el que se inserta dicha organización permite revelar información significativa, ofreciendo una comprensión más profunda y estratégica del problema analizado.

Métodos

En este contexto, la operacionalización del marco conceptual de los SNSAs a través del análisis de redes multicapa propone dos elementos diferenciales:

- La incorporación de nodos a nivel grupal: frente al enfoque centrado en individuos el uso de nodos que representan entidades permite analizar sus dinámicas y conexiones ampliando la escala y foco del análisis al sistema que conforman.
- La aplicación de un análisis diacrónico a través de una perspectiva multicapa: a diferencia de los análisis de redes estáticos, este enfoque facilita la comprensión de la evolución del sistema a lo largo de un periodo específico, mostrando tanto las relaciones entre nodos en un periodo particular como los cambios estructurales entre periodos diferentes.

Desde una perspectiva analítica, y basándose en la teoría de redes, un SNSA conforma lo que se ha denominado una *red interorganizacional*: "el conjunto de las relaciones formales e informales entre las organizaciones como entidades independientes y las relaciones

formales e informales entre sus miembros, si actúan, al menos parcialmente, en su función como miembros de la organización (relaciones interorganizacionales)"[4] (Raab, 2018). Las redes interorganizacionales facilitan la comprensión de los patrones de relación entre organizaciones y pueden ayudar a detectar cómo estos patrones habilitan o limitan ciertas estrategias. Así, el enfoque del SNSA puede permitir, entre otras cosas, el análisis de la dinámica entre la red terrorista y otras entidades colaboradoras, la detección de clústeres (p. ej., por tipo de legalidad, por tácticas empleadas, por tipos de nodos) y su participación dominios específicos, como el cultural, económico o político.

Además, al adoptar una versión avanzada de la representación clásica de la red, es decir, las redes multicapa, las relaciones entre entidades también pueden estudiarse diacrónicamente, incluyendo su evolución (Figura 1). Mediante el modelo matemático de la red multicapa, cada capa (es decir, de T_1 a T_n) representa la estructura del sistema en un periodo específico, incluyendo los nodos (entidades involucradas) y sus respectivas aristas (conexiones). Las aristas entre nodos ubicados en diferentes capas (p. ej., entre T_1 y T_2) representan la evolución del nodo a lo largo del tiempo (pudiendo representar, p. ej., un nodo que permanece igual, un nodo que se divide en dos, varios nodos que se fusionan para crear uno, un nodo que crea uno nuevo/cambia su nombre, etc.).

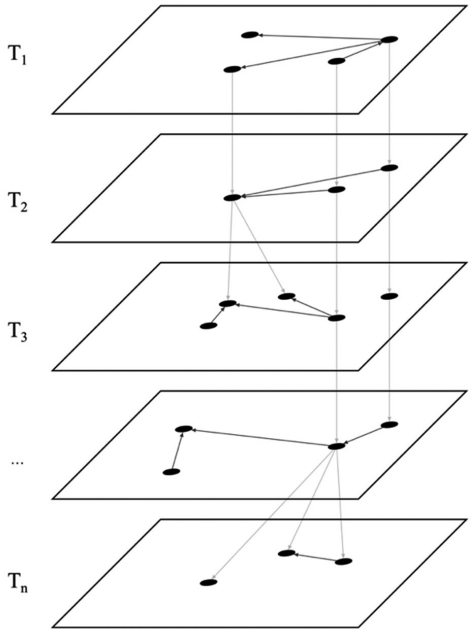

Figura 1. *Ejemplo de representación de un SNSA mediante una red multicapa.*
Fuente: elaboración propia.

4 Traducción de los autores.

Este enfoque permite visualizar los clústeres dentro del sistema y su evolución, proporcionando una visión más profunda y clara de su desarrollo. Además, de esta manera también es posible formalizar la desaparición de una entidad mediante la eliminación de su nodo correspondiente en las capas posteriores y la desagregación de instituciones en múltiples subgrupos con conexiones entre el nodo principal y los nodos secundarios. Por lo tanto, al combinar conexiones entre capas con información sobre el sistema en un periodo determinado y conexiones dentro de capas que proporcionan la información a lo largo del tiempo, la perspectiva del SNSA permite analizar cada entidad individual desde su nacimiento hasta su desaparición y la combinación de todas las entidades como parte de un único sistema.

En esta perspectiva analítica, los nodos son nodos a nivel de grupo, lo que significa que cada uno representa un grupo, una institución, una entidad o un individuo que actúa en nombre de una institución como persona jurídica. Se ha argumentado que el uso de nodos a nivel de grupo como unidades analíticas es beneficioso para comprender los patrones de relaciones entre grupos, aunque su uso en el análisis de redes militantes aún está poco desarrollado (Zech & Gabbay, 2016). Con este enfoque, se centra la atención en las conexiones de las instituciones involucradas y su rol dentro del sistema, y el SNSA resultante se entiende como un todo y no como la suma de sus partes.

Con el objetivo de validar el método analítico propuesto, se utiliza el estudio de caso del SNSA del que la organización terrorista Euskadi Ta Askatasuna formaba parte ($SNSA_{ETA}$) durante sus primeros 25 años de actividad (1958-1983). Este estudio de caso se selecciona por dos motivos: el primero, atendiendo al periodo elegido para el análisis, porque el análisis del desarrollo histórico de un SNSA resulta indispensable para anticipar dinámicas futuras, ya que la comprensión del pasado es crucial para generar inteligencia y conciencia situacional, y para generar inteligencia prospectiva e informar sistemas anticipatorios; y el segundo, atendiendo a la necesidad de datos robustos para realizar el análisis, porque se dispone de datos verificados extraídos de la sección de "Hechos probados" de una sentencia (Número 73, Sumario 18/98, 2007) y un auto (Sumario 35/02 Y, 2002) judiciales, lo que garantiza la solidez y fiabilidad de los datos empleados, al prescindir de fuentes secundarias5.

El estudio se realizó en tres pasos: 1) el análisis de nodos; 2) el análisis de aristas, y 3) el análisis de redes. Primero, se determinaron los nodos por evaluar. Definir criterios específicos es crucial para la inclusión de entidades en un SNSA. Por lo tanto, deben tenerse en cuenta al menos dos indicadores: en primer lugar, las entidades deben tener una visión (ideología) y una misión (voluntad de trabajar para lograr la visión) comunes a los demás no-

5 Las sentencias constituyen la resolución final de un caso, mientras que los autos son una resolución provisional o intermedia, susceptible de repetición. Ambos documentos incluyen una sección llamada *Hechos probados*. Esta sección describe los resultados de la investigación de las pruebas, en que los hechos se describen con precisión, claridad y la mayor proximidad posible a la realidad. En España, estos hechos se denominan *verdad judicial* y son relevantes para la resolución de un caso (Ver *Diccionario panhispánico del español jurídico*, 2023).

dos del SNSA en el periodo específico en que se incluye el nodo (ya que el sistema también puede evolucionar en paralelo y dos nodos que comparten visión y misión en T_1 pueden dejar de compartirlas en T_{1+n}), y en segundo lugar, las entidades deberán tener cierto grado de coordinación o colaboración con una o más entidades pertenecientes al SNSA para lograr su visión y misión compartidas. Es importante definir criterios específicos antes de realizar el análisis.

Las dos fuentes de análisis — la sentencia (Número 73, Sumario 18/98, 2007) y el auto (Sumario 35/02 Y, 2002) — se analizaron utilizando MAXQDA, un *software* de análisis de métodos mixtos que permite codificar, visualizar y analizar extensos documentos escritos. Se detectaron automáticamente las palabras más utilizadas en cada sección de "Hechos probados" y, entre ellas, las que se referían a entidades se codificaron automáticamente, incluyendo las veinticinco palabras anteriores y posteriores al código. Se incluyeron en el análisis las entidades sobre las que los escritos de acusación demostraban haber colaborado con ETA compartiendo los mismos objetivos estratégicos (es decir, perseguir la independencia de su autodenominada *Euskal Herria*).

Posteriormente, se elaboró un perfil para cada una de estas entidades, incluyendo 1) el nombre y el apodo de la entidad; 2) las fechas de origen, disolución, registro legal e ilegalización, cuando corresponda; 3) el tipo de organización (es decir, grupo armado, partido político, institución educativa, organización juvenil, agencia de medios, empresa, etc.); 4) el frente al que pertenecían, si lo hubiera, y 5) las entidades relacionadas, como las entidades anteriores y posteriores (en caso de cambio de nombre) y el nodo principal (para mostrar su dependencia, como en el caso de una revista de una entidad). Este perfil facilitaría posteriormente la consulta de las características de los nodos (p. ej., los frentes en que participaban o los años en los que estuvieron activos, visualizadas a través del análisis de redes multicapa).

Segundo, con el objetivo de entender las conexiones entre nodos, se atendió a dos criterios: las conexiones intracapa, es decir, las conexiones del nodo en un periodo específico, y las conexiones intercapa, es decir, aquellas conexiones entre nodos en diferentes periodos. Para este propósito, se construyó una matriz de supraadyacencia compuesta por cuatro matrices de adyacentes relativas a cuatro periodos, a saber: T_1 (1958-1966), T_2 (1967-1973), T_3 (1974-77) y T_4 (1978-1983), cada una de las cuales estaba delimitada por cambios específicos en el SNSA reflejados en los datos; y doce matrices de interconexión para los bordes que unen nodos en dos periodos diferentes (Figura 2). A partir de esta matriz de supraadyacencia fue posible generar una visualización de red multicapa compuesta por cuatro capas, cada una de las cuales representaba un periodo específico. Los nodos activos en cada periodo se incluyeron en su matriz correspondiente, y sus conexiones se evaluaron de forma binaria (tenían conexión con otro nodo o no), construyendo de este modo una matriz de supraadyacencia no ponderada.

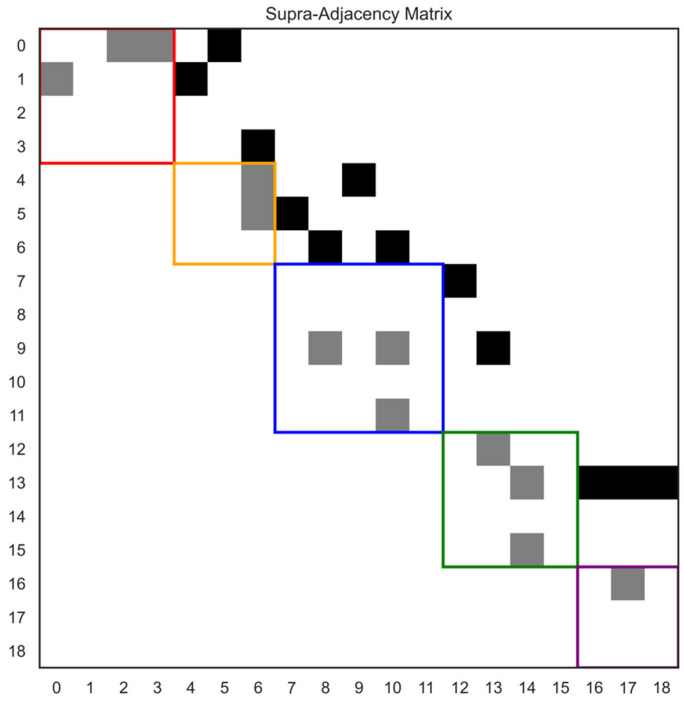

Figura 2. *Ejemplo de una matriz de supraadyacencia.*

Nota: cada cuadrado de color corresponde a una capa, en que los cuadrados grises son las conexiones intracapa entre nodos. Los cuadrados negros corresponden a las matrices de interconexión que reflejan las conexiones intercapa entre nodos.

Fuente: elaboración propia.

En cuanto a las conexiones intracapa, una conexión entre dos nodos se marcó como positiva y dirigida cuando los datos mostraron algún tipo de poder del nodo A sobre el nodo B (p. ej., en situaciones como A lidera las actividades de B, A financia a B, A crea a B). Por otro lado, una conexión se marcó como positiva y bidireccional cuando los datos reflejaban una relación igualmente poderosa (p. ej., a través de actividades como participar en las mismas reuniones, organizar una protesta juntos o pertenecer a la misma coalición). Para simplificar la lectura de los resultados, se adoptó una visualización dirigida para las conexiones direccionales y no dirigida para las conexiones bidireccionales. Respecto de las intercapa, una conexión se marcó como positiva cuando un nodo permaneció en el tiempo (p. ej., el nodo A continuó siendo el nodo A en la capa siguiente), cuando un nodo se transformó en un nuevo nodo (p. ej., el nodo A se convirtió en el nodo B en la capa siguiente) o cuando se dividió en varios nodos (p. ej., el nodo A se dividió en los nodos B y C en la capa siguiente).

Una vez completadas las matrices, se realizó el análisis de redes multicapa. Para la visualización de los nodos se calculó la medida de centralidad de proximidad y se asoció con

la dimensión de los nodos. La elección de esta métrica se justifica por el supuesto de que los nodos estrechamente relacionados con la mayoría de las demás entidades pueden desempeñar un papel importante en el sistema. Es esencial destacar que las métricas de centralidad siempre dependen del contexto en el que se han calculado. Por lo tanto, cuando se muestra la red multicapa completa, las mediciones de centralidad correspondientes se relacionan con la estructura completa. Sin embargo, si se atendiera al análisis de una capa específica aislada de su estructura completa, los valores de centralidad obtenidos se derivarían de la consideración de los nodos presentados allí únicamente.

Diferentes elementos pudieron ser considerados dentro del mismo análisis:

- El desarrollo diacrónico del sistema y su estructura en periodos específicos representados en cada capa, incluyendo los nodos (entidades involucradas) y sus respectivas aristas (conexiones). Los periodos específicos fueron delimitados atendiendo a la información proporcionada por los datos, concluyendo en cuatro capas específicas (es decir, T_1 a T_4).
- Estructura del sistema en diferentes niveles (entidad y subentidad). Los datos destacaban las conexiones internas de un nodo específico durante los periodos T_1 y T_2. Por lo tanto, se decidió crear dos matrices adicionales que reflejaran el nivel de subentidad en cada uno de los periodos. Para reflejar esta sincronización de dimensiones, las conexiones a nivel de subentidad durante los periodos T_1 y T_2, se incluyó un eje adicional donde se proyectaron las conexiones internas de la entidad específica.
- Diversidad y tipología de los nodos analizados, representando a través de colores información específica.
- Diversidad y tipología de vínculos relacionales, representando a través de diferentes versiones de aristas, diferentes tipos de conexiones entre nodos (en cada capa: direccional o bidireccional; entre capas: evolución, transición o permanencia).

Resultados

Este estudio desarrolla el análisis de redes multicapa aplicado al estudio de la estructura y evolución de los SNSAs, a través del estudio de caso del SNSA del que la organización terrorista Euskadi Ta Askatasuna formaba parte ($SNSA_{ETA}$) y su evolución entre 1958 y 1983. La red multicapa del sistema de $SNSA_{ETA}$(1958-1983) resulta compuesta por cuatro capas (es decir, de T_1 a T_4) (Figura 3). Cada capa representa la estructura del sistema en un periodo específico, incluyendo los nodos (entidades involucradas) y sus respectivas aristas (conexiones): T_1 (1958-1966), T_2 (1967-1973), T_3 (1974-1977) y T_4 (1978-1983). Los resultados muestran un incremento del $SNSA_{ETA}$ tanto en relación con su tamaño, al incrementar de 1 a 27 nodos, como a su complejidad, al incrementar de 0 a 55 aristas (conexiones entre nodos) a lo largo de 25 años (Tabla 1).

Tabla 1. *Número de nodos, aristas dirigidas y aristas no dirigidas por capa del sistema del SNSA$_{ETA}$*

Capas	Nodos	Aristas dirigidas	Aristas no dirigidas
T_1 (1958-1966)	1	0	0
T_2 (1967-1973)	3	2	0
T_3 (1974-1977)	21	15	14
T_4 (1978-1983)	27	24	31

Fuente: elaboración propia.

Los colores de los nodos representan el tipo de frente en el que los datos afirman que el nodo era activo: rojo como el frente militar, azul como el frente político (hasta 1977) y político-institucional (1978-1983), amarillo como el frente laboral, rosa como el frente cultural (hasta 1977) y cultural-mediático (1978-1983), verde como el frente de masas, naranja como coordinación de diferentes frentes, y gris reflejando la ausencia de información relativa al frente al que un nodo pertenecía. Las aristas entre nodos ubicados en diferentes capas (p. ej., entre T_1 y T_2) representan su conexión a lo largo del tiempo, siendo una arista discontinua cuando el nodo de una capa superior cambia en la siguiente (p. ej., un nodo se divide en dos, un nodo crea uno nuevo, cambia su nombre, etc.); y una arista continua cuando el nodo de la capa superior permanece sin cambios en la capa siguiente. Las capas de la izquierda representan los nodos a nivel de entidad, la unidad base de análisis; las capas de la derecha (solo incluidas para T_1 y T_2) representan los nodos a nivel de subentidad (es decir, la estructura interna del nodo ETA). Esta información adicional se incluyó por la siguiente razón: entre T_2 y T_3, los resultados muestran una evolución particularmente interesante desde los frentes de ETA a nivel de subentidad (en T_2) a los frentes a nivel de entidad (en T_3). En este momento, la organización terrorista decide deliberadamente externalizar algunos de sus frentes a entidades de nueva creación para cubrirlos legalmente. Los datos sostienen que, desde principios de la década de 1970, esta reorganización se inspiró en el principio maoísta de las tres armas mágicas de la revolución, según el cual un grupo armado ilegal debe combinar sus esfuerzos con la consolidación de un partido político fuerte y un frente popular unido para tener éxito con su agenda (*Auto-Sumario 35/02 Y*, 2002, p. 22; Tsou & Halperin, 1965).

Los periodos T_1 y T_2 transcurrieron durante la dictadura franquista (1939-1975), un contexto en el que la organización terrorista ETA prosperó, primero con una estructura jerárquica (en T_1) y luego con la adopción de una estructura frentista (en T_2). Durante estos dos periodos, los resultados muestran que la organización terrorista estuvo principalmente aislada de otras entidades. Las primeras conexiones de la organización terrorista ETA con otras entidades aparecen en el periodo T_2.

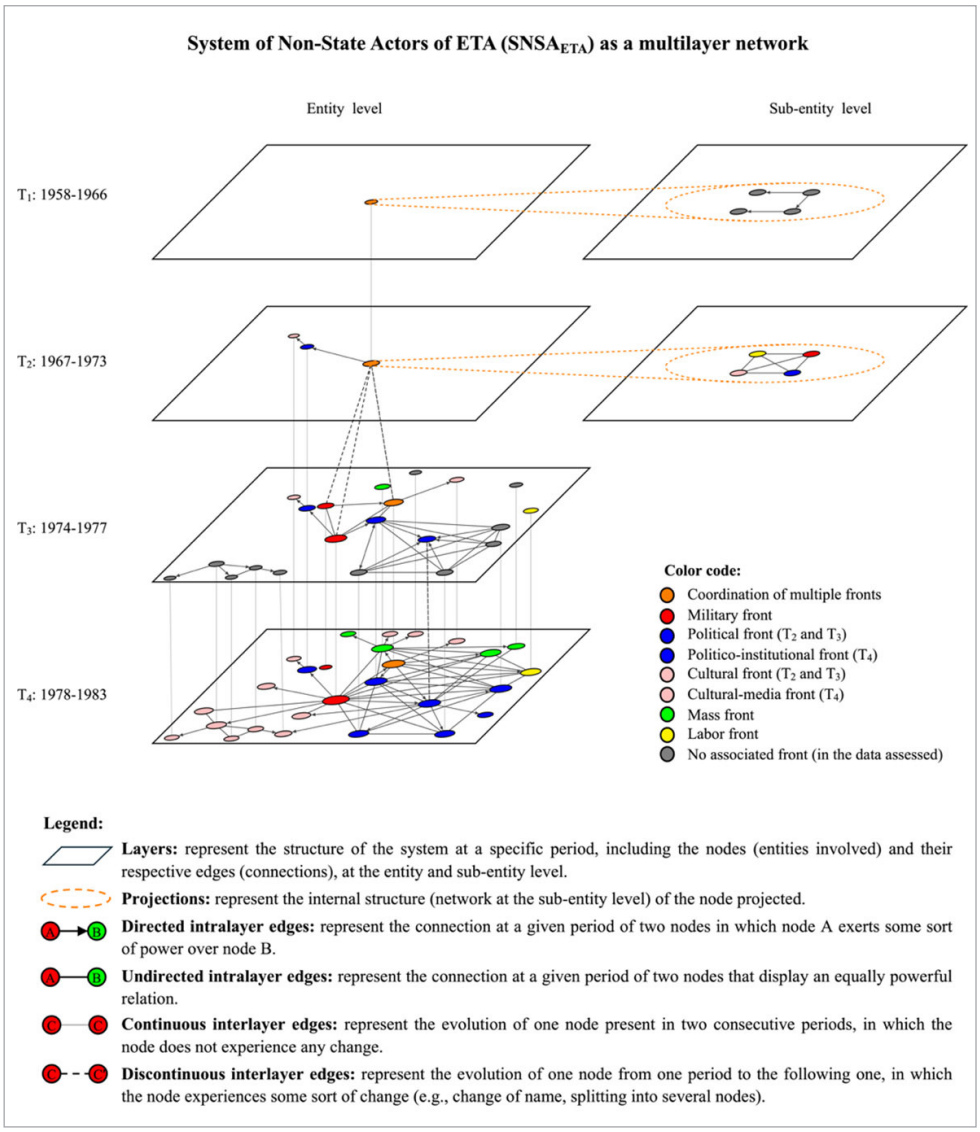

Figura 3. *Representación del SNSA$_{ETA}$ como red multicapa.*

Fuente: elaboración propia.

Durante el periodo T$_3$, ante el fin de la dictadura y la inminente transición a la democracia, el SNSA$_{ETA}$ experimentó el primer gran cambio y el drástico aumento de tamaño y complejidad, cuando llegó a contar con al menos 21 nodos y 29 aristas (15 dirigidas y 13 no dirigidas). Tres acontecimientos clave destacan durante este periodo: la escisión de la dirección de ETA en ETA político-militar (ETApm) y ETA militar (ETAm); la externalización

de los frentes político, cultural y laboral a entidades de nueva creación y aparentemente independientes, siguiendo la teoría del desdoblamiento, con el fin de proporcionarles la cobertura legal para actuar dentro del próximo sistema democrático; y la creación de la Koordinadora Abertzale Sozialista (KAS) como una asociación alegal que funcionaría como *proxy* para coordinar las actividades de estas nuevas entidades y los diferentes frentes bajo la dirección de la organización terrorista ETApm (hasta 1977) y posteriormente bajo la dirección de ETAm.

Por último, el periodo T_4 inicia en el contexto de la redacción y aprobación de una nueva Constitución democrática española. Tras la amnistía general concedida en 1977 se liberaron a muchos militantes de ETA encarcelados, que se reincorporaron a la organización terrorista. ETAm asumió el liderazgo del $SNSA_{ETA}$ y se consolidaron el principio de la doble militancia —a través del cual militantes de ETAm también participaban en las otras entidades del sistema— y la estrategia del desdoblamiento, dotando al $SNSA_{ETA}$ de un tamaño y una complejidad cada vez mayores. Lejos de reducir su violencia tras la amnistía general y el establecimiento de un gobierno democrático con las primeras elecciones generales libres en 1977, este periodo fue testigo de un importante aumento de los atentados terroristas y asesinatos.

Discusión

Este estudio presenta una aplicación del análisis de redes multicapa al estudio de la estructura y evolución de los SNSAs, utilizando el estudio de caso del SNSA del que la organización terrorista Euskadi Ta Askatasuna formaba parte ($SNSA_{ETA}$) y su desarrollo durante el periodo comprendido entre 1958 y 1983. Los resultados identifican cuatro momentos específicos en su evolución, caracterizados por transformaciones estructurales debido a decisiones estratégicas del sistema: T_1 (1958-1966), T_2 (1967-1973), T_3 (1974-1977) y T_4 (1978-1983). En general, se observa un incremento del tamaño y la complejidad del $SNSA_{ETA}$ que aumenta de 1 a 27 nodos y de 0 a 55 aristas a lo largo de 25 años.

El marco conceptual del SNSA y su operacionalización a través del análisis de redes multicapa permite trascender la visión de una organización terrorista aislada y entenderla dentro del sistema de actores al que pertenece. Como se observa en el análisis del $SNSA_{ETA}$, este enfoque revela que, lejos de ser *solo* una organización terrorista aislada, ETA consolidó y dirigió un SNSA con el propósito de avanzar sus objetivos estratégicos. Durante décadas, entidades legales, alegales e ilegales trabajaron bajo la dirección y coordinación de una organización terrorista, consolidando un sistema complejo en el que la amenaza a la seguridad no solamente era ejercida a través de tácticas físicamente violentas, sino a través de tácticas físicamente no violentas e, incluso, legales o alegales.

Las enseñanzas derivadas de la lucha integral contra ETA y lo que se denominó *el entorno de ETA* fueron, en cierta medida, pasadas por alto en el plano analítico, ya que no

llegaron a formalizarse como marco teórico o metodológico para su aplicación a otros casos o contextos. Los documentos utilizados como fuentes del presente estudio forman parte de los juicios a gran escala que tuvieron lugar a entre las décadas de 1990 y 2000 para procesar a las entidades que colaboraron o apoyaron a la organización terrorista ETA, incluyendo partidos políticos, organizaciones juveniles, bufetes legales, bares y empresas (Portero, 2008). Estos juicios demostraron que la amenaza para la seguridad que representaba ETA era más amplia que la de los militantes de la organización terrorista: ETA estaba inserta en un sistema de actores que colaboraban bajo su liderazgo en la búsqueda de la independencia de su autodenominada *Euskal Herria*, utilizando tácticas tanto legales como ilegales para multiplicar su impacto. Como resultado de estos juicios, múltiples entidades fueron ilegalizadas y desmanteladas, y sus actividades fueron prohibidas. Sin embargo, muchas de las entidades desmanteladas se reorganizaban bajo nuevos nombres para seguir operando, evitar las prohibiciones y explotar los umbrales legales; y algunas de ellas fueron, de nuevo, ilegalizadas nuevamente, reiniciando el ciclo (Portero, 2008).

El marco del SNSA retoma y sistematiza la aproximación integral al análisis de este fenómeno, dotándolo de un marco conceptual y una posible operacionalización a través del análisis de redes multicapa. Se introduce así una perspectiva conceptual y analítica que permite comprender fenómenos complejos en retrospectiva, profundizar problemas de seguridad actuales desde una perspectiva más amplia e informar, de este modo, sistemas anticipatorios proponiendo un alcance más amplio —como se hace actualmente con el análisis de actores estatales desde la perspectiva de las amenazas híbridas (Giannopoulos et al., 2021; Jungwirth et al., 2023).

Algunas limitaciones deben tenerse en consideración para contextualizar el análisis. A pesar de los múltiples beneficios para comprender la estructura de las organizaciones, el SNSA depende en gran medida de la disponibilidad de datos y la caracterización de la red. Por lo tanto, la interpretación de los resultados puede ser engañosa si no se tienen en cuenta ciertas consideraciones.

En primer lugar, los procesos de recopilación de datos son complejos, especialmente en el estudio de redes terroristas, dada la naturaleza intrínsecamente encubierta de estas. En muchas ocasiones, los datos disponibles son inexactos, incompletos, dinámicos, multimodo y multiplex (Carley, 2004, p. 6), y representan solo una parte de la realidad para la cual la información es accesible. A pesar de que en el presente análisis se hayan utilizado los datos incluidos en la sección de "Hechos probados" de documentos legales, solamente dos documentos han podido ser consultados. Por ello, la información proporcionada para poblar el análisis es muy reducida y solo constituye una parcela de la realidad. Las redes visualizadas no tienen por qué ser necesariamente un espejo exhaustivo de la realidad; por el contrario, lo que no está representado puede no existir o existir pero ser desconocido (Ressler, 2006). Esto tiene efecto, p. ej., en la cantidad de nodos incluidos, ya que entidades del $SNSA_{ETA}$ pueden haber sido excluidas del análisis al no estar presentes en las fuentes analizadas, o en el nivel de detalle temporal, ya que contando con información más detallada podría incluirse

un mayor número de capas que detallaran el desarrollo y estructura del sistema con mayor precisión.

En segundo lugar, las diferentes maneras en que se pueden caracterizar los bordes de una red influyen en la red resultante, incluso utilizando las mismas fuentes de información. El tipo de relación que representa la arista, así como la forma de cuantificarla, puede resultar en una visualización diferente de la red, incluso utilizando las mismas fuentes para el análisis. Por consiguiente, comprender cuidadosamente el significado de la visualización y cómo se describe cada parámetro es extremadamente relevante. Esto tiene efecto, p. ej., en el tipo de red consolidada. En el presente estudio, se ha utilizado la clasificación binaria de las relaciones (p. ej., los datos muestran una conexión entre dos nodos en forma de colaboración o cooperación, sí o no). Sin embargo, la red podría tomar una forma diferente si las relaciones entre nodos fueran clasificadas, p. ej., en el tipo de relación (asociación eventual, colaboración informal, acuerdos firmados, etc.).

Finalmente, no comprender las representaciones de red tal como son, una representación de un segmento de datos y no un reflejo exhaustivo de la sociedad, puede llevar a pasar por alto otras dimensiones o tipos de relaciones, con el riesgo de una simplificación excesiva y una interpretación errónea de la realidad. El análisis de redes puede ayudar a reducir la complejidad de las relaciones humanas a redes funcionales unidimensionales manejables para el análisis. Sin embargo, al interpretar los resultados del SNSA, confiar únicamente en la representación de la red puede ser contraproducente, ya que las visualizaciones de la red a menudo son agnósticas del contexto y no profundizan en las causas de los conflictos violentos, pueden usarse para reducir un grupo étnico a un comportamiento específico o usarse para crear perfiles y seleccionar actores para perturbar la red (Mac Ginty, 2010, p. 223).

El marco conceptual del SNSA y su operacionalización a través del análisis de redes multicapa abre grandes oportunidades para entender las amenazas provenientes del SNSA desde un punto de vista integral. Por ejemplo, la continuación del análisis realizado durante toda la vida activa de la organización terrorista ETA y, sobre todo, después de que esta anunciara su disolución en 2018, podría permitir abordar diferentes preguntas de investigación: ¿Cómo reacciona el SNSA cuando uno de sus nodos desaparece? ¿Continúa activo el SNSA cuando la organización terrorista se disuelve?[6]

Comprender cómo se estructuró y evolucionó un SNSA puede ayudar a comprender la situación actual e informar los modelos que utilizan los sistemas anticipatorios y sus valoraciones de la amenaza para realizar predicciones sobre los posibles cursos de acción de los sistemas hostiles y así informar la toma de decisiones en el presente.

6 Desde al menos 2016, España ha sido testigo de cientos de homenajes públicos a militantes de ETA encarcelados que salen de la cárcel, actos de enaltecimiento de ETA, con el uso de pancartas, carteles y grafitis urbanos, y manifestaciones a favor de la amnistía de antiguos militantes de ETA, algunos de los cuales han cometido crímenes de sangre. Sobre los actos públicos de culto al terrorista documentados en España entre 2016 y 2025, véase el Observatorio de radicalización del Colectivo de Víctimas del Terrorismo (COVITE), https://covite.org/observatorio/.

Conclusión

Los sistemas anticipatorios permiten realizar predicciones para entender posibles desarrollos de un evento y, ante esta información, realizar cambios en el presente. La generación de inteligencia contribuye a los sistemas anticipatorios que no obstante cuentan con informaciones y elementos de juicio adicionales.

Ampliar el foco analítico a sistemas permite elaborar análisis estratégicos y anticipatorios con un enfoque más amplio y entender correlaciones que anteriormente se encontraban ocultas, además de responder a nuevas preguntas de investigación que antes permanecían inalcanzables.

El enfoque conceptual de los SNSA operado a través del análisis de redes multicapa ofrece un método innovador para analizar de manera integral —en la medida de lo posible dadas las limitaciones de los datos— el sistema compuesto por las entidades involucradas y su evolución, estructura y naturaleza. De esta manera, facilita la comprensión de sus entidades y cómo estas pueden, como una unidad y no en función de cada una de las partes, representar una amenaza para la seguridad, las instituciones democráticas y los derechos humanos. Además, permite entender que dichas entidades no tienen, necesariamente, que operar dentro de la ilegalidad; por el contrario, la evidencia demuestra que varios SNSAs han operado dentro de la legalidad del país donde actúan, han utilizado zonas grises o aprovechado las vulnerabilidades sistémicas de la sociedad, como el derecho a la libertad de expresión o el derecho de asociación, para avanzar en sus objetivos estratégicos.

Establecer el alcance del análisis en el SNSA al que pertenece la entidad por analizar, en el caso de ETA una organización terrorista, permite a los analistas explicar las conexiones entre la entidad analizada y otras entidades (ya sean legales, ilegales o alegales) con las que la primera podría estar cooperando, y el rol de cada una dentro del sistema. Detectar estas conexiones puede ayudar a explicar el rol de las entidades legales dentro del sistema, la posible externalización de actividades para brindarles cobertura legal, y la capacidad de influencia real del SNSA en la sociedad y su *modus operandi* en general —ya que la influencia puede conseguirse tanto a través de actividades físicamente violentas e ilegales como no violentas y legales—. Debido a ello, aplicar el enfoque conceptual del SNSA y operacionalizarlo a través del análisis de redes multicapa permite producir análisis y valoraciones para informar nuestros sistemas anticipatorios de una manera única.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo. No se emplearon herramientas de generación de contenido por inteligencia artificial para su elaboración.

Financiamiento

Los autores declaran la siguiente fuente de financiamiento para la realización de este artículo: Rudy Milani cuenta con financiación de dtec.bw —*Digitalization and Technology Research Center of the Bundeswehr*, proyecto *RISK.twin*— dtec.bw es financiado por la Unión Europea—NextGenerationEU.

Sobre los autores

Rubén Arcos es profesor titular de la Universidad Rey Juan Carlos y profesor visitante de análisis de inteligencia en el Colegio de Europa de Brujas. Integra el programa de doctorado en seguridad internacional del IUGM-UNED. Es *chair* de la Sección de Estudios de Inteligencia de la International Studies Association (ISA).

https://orcid.org/0000-0002-9665-5874 - Contacto: ruben.arcos@urjc.es

Marina Alonso-Villota es doctoranda en Seguridad Internacional en el Instituto Universitario General Gutiérrez Mellado, Escuela Internacional de Doctorado, Universidad Nacional de Educación a Distancia (IUGM-UNED). Fue investigadora en la Universidad de las Fuerzas Armadas de Múnich durante este estudio. Sus intereses de investigación se centran en el fenómeno del terrorismo y las amenazas híbridas.

https://orcid.org/0000-0002-6541-9123 - Contacto: malonso1139@alumno.uned.es

Rudy Milani es doctorando en la Cátedra de Investigación Operativa de la Universidad de las Fuerzas Armadas de Múnich (UniBW München). Sus intereses de investigación se centran en informática teórica, análisis de redes, aprendizaje por refuerzo y temas clásicos de investigación operativa, como modelización matemática y optimización.

https://orcid.org/0000-0003-0733-3142 - Contacto: rudy.milani@unibw.de

Referencias

Alonso-Villota, M., & Arcos, R. (2025). The Coercion-Manipulation-Persuasion Framework: Analyzing the Modus Operandi of Systems of Non-State Actors. *Terrorism and Political Violence, 37*(5), 632–650. https://doi.org/10.1080/09546553.2024.2357082

Arcos, R. (2023). Intelligence and Awareness. En A. Gruszczak & S. Kaempf (Eds.), *Routledge Handbook of the Future of Warfare* (pp. 272-283). Routledge.

Arcos, R., & Palacios, J.-M. (2025). Intelligence Education and the European Union's External Action. *International Journal of Intelligence and CounterIntelligence*, *38*(3), 750-766. https://doi.org/10.1080/08850607.2025.2454821

Arquilla, J., & Ronfeldt, D. F. (Eds.). (2001). *Networks and netwars: The future of terror, crime, and militancy*. Rand.

Audiencia Nacional. Auto-Sumario 35/02 Y, n.º 00002 2 0006285 /2001 78600 (Juzgado Central de Instrucción n.º 5; Agosto 23 de 2002).

Audiencia Nacional. Sentencia n.º 73, Sumario 18/98 (Juzgado Central de Instrucción n.º 5; Diciembre 19 de 2007).

Calof, J., & Bishop, P. (2020). Guest Editorial, Foresight. *Foresight*, *22*(5/6), 529.

Carley, K. M. (2004). *Estimating Vulnerabilities in Large Covert Networks*.

Carley, K. M., Lee, J.-S., & Krackhardt, D. (2002). Destabilizing networks. *Connections*, *24*(3), 79-92. https://doi.org/10.1093/jrs/14.3.345

Clark, R. M. (2004). *Intelligence analysis: A target-centric approach*. CQ Press.

Diccionario panhispánico del español jurídico. (2023). Definición de "hechos probados". https://dpej.rae.es/lema/hechos-probados

Downing, J., Gerwens, S., & Dron, R. (2022). Tweeting terrorism: Vernacular conceptions of Muslims and terror in the wake of the Manchester Bombing on Twitter. *Critical Studies on Terrorism*, *15*(2), 239-266.

European Union Agency for Cybersecurity. (2024). *Foresight cybersecurity threats for 2030—Update*. Publications Office. https://data.europa.eu/doi/10.2824/349493

European Union Agency for Law Enforcement Cooperation. (2025). *The changing DNA of serious and organised crime* (European Union Serious and Organised Crime Threat Assessment, p. 98). Publications Office. https://doi.org/10.2813/0758057

European Union External Action. (2025). *3rd EEAS Report on Foreing Information Manipulation and Interference Threats. Exposing the architec*

ture of FIMI operations (Report on FIMI Threats, p. 42). https://tinyurl.com/yey6kbbc

Everton, S. F., & Cunningham, D. (2013). Detecting significant changes in dark networks. *Behavioral Sciences of Terrorism and Political Aggression*, *5*(2), 94-114. https://doi.org/10.1080/19434472.2012.725225

FRONTEX. (2025). *EIBM Intelligence Division (INTEL)*. https://tinyurl.com/y57kkfyr

Giannopoulos, G., Smith, H., & Theocharidou, M. (Eds.). (2021). *The Landscape of Hybrid Threats: A conceptual model*. Publications Office of the European Union.

Granovetter, M. S. (1973). The Strenght of Weak Ties. *American Journal of Sociology*, *78*(6), Article 6.

Hoffman, D. (Director). (2018, junio 7). *Questioning the "Loneliness" of Lone-Wolves: A Social Network Analysis of Lone-Wolf Terrorists* [Archivo de video]. https://www.youtube.com/watch?v=7EQjS7Lz3V4

Hybrid CoE. (2025). *Publications*. Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/all-publications/

Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso-Villota, M., Lebrun, M., Aho, A., & Giannopoulos, G. (2023). *Hybrid Threats: A Comprehensive Resilience Ecosystem*. Publications Office of the European Union. https://doi.org/10.2760/37899

Koschade, S. (2007). *The internal dynamics of terrorist cells: A social network analysis of terrorist cells in an Australian context*.

Krebs, V. E. (2002). *Mapping Networks of Terrorist Cells*. https://www.aclu.org/sites/default/files/field_document/ACLURM002810.pdf

Lasswell, H. D. (1942). The Relation of Ideological Intelligence to Public Policy. *Ethics*, *53*(1), 25-34.

Mac Ginty, R. (2010). Social network analysis and counterinsurgency: A counterproductive strategy? *Critical Studies on Terrorism*, *3*(2), 209-226. https://doi.org/10.1080/17539153.2010.491319

Magouirk, J., Atran, S., & Sageman, M. (2008). Connecting Terrorist Networks. *Studies in Conflict & Terrorism*, *31*(1), 1-16. https://doi.org/10.1080/10576100701759988

Malthaner, S. (2018). Spaces, Ties, and Agency: The Formation of Radical Networks. *Perspectives on Terrorism*, *12*(2), 32-43.

NATO. (2024, marzo 7). *A "comprehensive approach" to crises*. https://www.nato.int/cps/en/natohq/topics_51633.htm

Omand, D. (2010). *Securing the State*. Hurst & Company.

Pedahzur, A., & Perliger, A. (2006). The Changing Nature of Suicide Attacks: A Social Network Perspective. *Social forces*, *84*, 1987-2008. https://doi.org/10.1353/sof.2006.0104

Perliger, A., & Pedahzur, A. (2011). Social Network Analysis in the Study of Terrorism and Political Violence. *PS: Political Science and Politics*, *44*(1), 45-50.

Portero, D. (2008). *La trama civil de ETA: el final está muy cerca*. Documentos Arcopress.

Raab, J. (2018). Interorganizational Networks. En R. Alhajj & J. Rokne (Eds.), *Encyclopedia of Social Network Analysis and Mining*. Springer. https://doi.org/10.1007/978-1-4939-7131-2

Ressler, S. (2006). Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research. *Homeland Security Affairs*, *2*(2), Article 8.

Rodriguez, J. A. (2005). *The March 11th Terrorist Network: In its weakness lies its strength*. XXV International Sunbelt Conference.

Rosen, R. (1985). *Anticipatory Systems: Philosophical, Mathematical & Methodological Foundations* (Vol. 1). Pergamon Press.

Sageman, M. (2004). *Understanding Terror Networks*. https://www.upenn.edu/pennpress/book/14036.html

Treverton, G. F. (2009). Approaching Threat Convergence from an Intelligence Perspective. En M. Randstorp & M. Normak (Eds.), *Unconventional Weapons and International Terrorism. Challenges and New Approaches* (Kindle ed., pp. 141-162). Routledge. https://doi.org/10.4324/9780203881958

Tsou, T., & Halperin, M. H. (1965). Mao Tse-tung's Revolutionary Strategy and Peking's International Behavior. *American Political Science Review*, *59*(1), Article 1. https://doi.org/10.2307/1976122

Wasserman, S., & Faust, K. (1994). *Social Network Analysis: Methods and Applications*. Cambridge University Press. https://doi.org/10.1017/CBO9780511815478

Wetherell, C. (1998). Historical Social Network Analysis. *International Review of Social History*, *43*(S6), 125-144. https://doi.org/10.1017/S0020859000115123

Zech, S., & Gabbay, M. (2016). Social Network Analysis in the Study of Terrorism and Insurgency: From Organization to Politics. *International Studies Review*, *18*, viv011. https://doi.org/10.1093/isr/viv011