Universidad Miguel Hernández

Facultad de Ciencias Sociales y Jurídicas de Elche

GRADO EN SEGURIDAD PÚBLICA Y PRIVADA

TRABAJO FIN DE GRADO

Curso académico: 2021/2022

ESTRUCTURA Y ESTRATEGIAS DE LOS SERVICIOS DE INTELIGENCIA

ALUMNO: Francisco Javier Quinto García

TUTOR: D. Ignacio Díaz Castaño

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ABREVIATURAS

CESID - Centro Superior de Información de la Defensa

CI - Comunidad de Inteligencia

CNI - Centro Nacional de Inteligencia Española

CPA - Acción Política Encubierta

FSB - Servicio Federal de Seguridad

IRD - Departamento de Investigación de la Información

OCN - Organización Contrasubversiva Nacional

RAW - Research and Analysis Wing

SECED - Servicio Central de Documentación

Biblioteca
UNIVERSITAS Miguel Hernández

RESUMEN

A lo largo de la última década se ha hecho más perceptible la necesidad de promover la acción de la Comunidad de Inteligencia en cuanto a entidad que aúna los esfuerzos y trabajos en materia de inteligencia, con el objetivo de maximizar las capacidades de cada Estado de prevenir y dar respuesta ante las posibles amenazas externas. De este concepto esencial parte la presente investigación que pretende conocer la evolución de los servicios de seguridad, tanto en España como en el ámbito internacional. Por consiguiente, el objetivo general es analizar la estructura y las estrategias de los servicios de inteligencia en la lucha contra el terrorismo. A partir de una revisión sistemática que arrojó una muestra de 22 artículos, pudieron analizarse estas estrategias. Tanto los esfuerzos en materia de cooperación, colaboración y coordinación, al igual que las reformas en el ámbito del conocimiento fueron las estrategias que mayor relevancia presentaron. El aumento de recursos y de presupuesto destinado a los servicios de inteligencia y la seguridad también es de notoria relevancia, seguido de las mejoras en las estructuras. De esta manera puede comprenderse que, a partir del 11S, las estrategias que se aplicaron en materia de seguridad y servicios de inteligencia fueron múltiples, pero todas se enfocan en la prevención de riesgos, en la optimización y mejora de los recursos, en el fortalecimiento de las relaciones regionales e internacionales, y la divulgación de información e investigaciones. Se concluye que es necesario seguir avanzando, respondiendo a las demandas de la sociedad y adecuándose a los avances tecnológicos.

Palabras clave: servicios de inteligencia – comunidad de inteligencia – estrategias de seguridad – terrorismo.

ABSTRACT

Over the last decade, the need to promote the action of the Intelligence Community as an entity that unites efforts and work in intelligence matters has become more perceptible, with the aim of maximizing the capacities of each State to prevent and respond to possible external threats. This essential concept is the starting point of this research, which aims to discover the evolution of security services, both in Spain and internationally. Therefore, the general objective is to analyze the structure and strategies of the intelligence services in the fight against terrorism. From a systematic review that yielded a sample of 22 articles, these strategies could be analyzed. Both the efforts in terms of cooperation, collaboration and coordination, as well as the reforms in the field of knowledge were the strategies that presented the greatest relevance. The increase in resources and budget allocated to intelligence and security services is also of notable importance, followed by improvements in structures. In this way, it can be understood that, as of 9/11, the strategies that were applied in matters of security and intelligence services were multiple, but all of them focus on risk prevention, on optimizing and improving resources, on strengthening of regional and international relations, and the dissemination of information and research. It is concluded that it is necessary to continue advancing, responding to the demands of society and adapting to technological advances.

Keywords: intelligence services – intelligence community – security strategies – terrorism.

1. INTRODUCCIÓN

A lo largo de la historia, ha habido muchos eventos y peligros que amenazan la seguridad de los Estados, causando grandes pérdidas de vidas, enfermedades, lesiones, destrucción de bienes, desplazamiento de un gran número de personas y enormes pérdidas económicas.

El concepto de seguridad ha evolucionado gradualmente y el impacto persistente de la política del mundo bipolar ofrece la oportunidad de comprender e identificar nuevas amenazas y conflictos emergentes, además de muchos problemas sin resolver. Simultáneamente, la globalización ha cambiado las reglas y normas internacionales, para facilitar el rápido flujo de capital y tecnología, con un debilitamiento de las barreras nacionales. Los actores no gubernamentales desempeñan ahora un papel clave en la política internacional, algunos como una amenaza y otros tendiendo un puente entre comunidades y naciones (González-García y Guirao, 2020).

Hoy en día, una de las principales cuestiones que preocupan en todo el mundo y que suscita un acalorado debate tanto a nivel nacional como internacional, es el terrorismo. La amenaza del terrorismo nunca ha sido tan importante como parece serlo en la actualidad. El terrorismo es un fenómeno antiguo que ha existido desde la aparición de las sociedades humanas, pero su amenaza ha aumentado constantemente en los últimos 30 años. Con los avances tecnológicos y técnicos, las acciones de los terroristas se han vuelto más peligrosas y destructivas, mientras que los autores de dichos actos son cada vez más evasivos (González, 2016).

El fenómeno del terrorismo está cambiando, mientras que los motivos del terrorismo siguen siendo los mismos. El sistema internacional, los sistemas de inteligencia, los procedimientos de seguridad y las tácticas que se esperan para proteger a las personas, las naciones y los gobiernos, no son capaces de hacer frente a este nuevo y devastador enemigo. Los métodos y estrategias desarrollados para combatir el terrorismo a lo largo de los años están resultando ineficaces, pues el enemigo ya no ataca solo con aviones, camiones bomba o terroristas suicidas. Los terroristas pueden dedicarse al

ciberterrorismo, el uso del ciberespacio para lanzar ataques. La integración de los mundos virtual y físico, es una debilidad a la que se enfrentan los agentes de seguridad. Desde la perspectiva de la lucha contra el terrorismo, resulta necesario describir los servicios de inteligencia como el resultado de las organizaciones profesionales – gubernamentales o privadas – que recogen, analizan y procesan información secreta con el fin de ayudar a la toma de decisiones en el ámbito de la política de seguridad estratégica y táctica. (González, 2016).

Como concluye el informe del ESSTRT ("European Security: Threats Responses and Relevant Technologies"), aunque la Unión Europea podría beneficiarse de la inversión en una amplia gama de tecnologías que reforzarían la protección contra los atentados terroristas, las medidas preventivas y preparatorias más amplias, la comunicación pública, la mejora de los servicios de inteligencia y una sólida asociación internacional son igualmente importantes a la hora de que los gobiernos desarrollen estrategias de lucha contra el terrorismo (European Council, 2021).

En el ámbito de la lucha antiterrorista, la inteligencia fiable y oportuna desempeña un papel fundamental y hace posible la prevención táctica y estratégica en el sentido real de su significado. Por un lado, ofrece a los profesionales de la seguridad la oportunidad de actuar antes de que se produzca un atentado terrorista y por otro es la condición previa para el análisis de las amenazas, lo que permite la toma de decisiones políticas con un enfoque a largo plazo sobre la evolución de los problemas de seguridad (Richards, 2012).

La cooperación en materia de inteligencia a nivel europeo, al igual que todas las cuestiones europeas "calientes" se enfrenta al problema de establecer un equilibrio entre dos tendencias: la soberanía nacional y la toma de decisiones común europea, en este caso en lo que respecta a los servicios de inteligencia. Sin embargo, los esfuerzos de inteligencia en la lucha antiterrorista a nivel europeo, junto con la aplicación de la ley a través de Europol y Eurojust, constituyen el triángulo básico de la política de seguridad europea contemporánea en respuesta al terrorismo (Díaz, 2016).

Pero todavía no existe un organismo que funcione como una Agencia Europea de Inteligencia, por lo que sigue siendo cuestionable si la voluntad política de mejorar la acción común contra el terrorismo se está aplicando con suficiente decisión. Ni la Estrategia Antiterrorista de la Unión Europea, ni el documento sobre la aplicación del Plan de Acción para la Lucha contra el Terrorismo, prevén una vía clara hacia la creación de una agencia europea de inteligencia común. No obstante, la evolución reciente del sector de la seguridad de la Unión, indican ciertos movimientos hacia el desarrollo de dicho organismo. Si bien la cooperación europea en materia de inteligencia se lleva a cabo actualmente en el Centro de Satélites de la Unión Europea, el Centro de Situación de las Naciones Unidas y a través del Club de Berna, en Suiza, la cuestión del intercambio total de información sigue abierta.

Supuestamente, a partir del 1 de enero de 2008, toda la información de inteligencia de un país debe ponerse a disposición de todos los Estados miembros. Esto podría significar que una Agencia Europea de Inteligencia debería encargarse de recopilar datos de las agencias de inteligencia de los Estados miembros, con el fin de analizarla de forma independiente y procesar sus resultados para la Comisión Europea y el Consejo sobre relaciones exteriores y seguridad, para una adecuada toma de decisiones (Díaz-Caneja, 2014).

Los ataques terroristas del 11 de septiembre de 2001 revelaron la importancia vital de mejorar las operaciones de inteligencia de Estados Unidos. Desde ese día, se ha prestado una enorme atención, se ha centrado en la necesidad de introducir cambios constructivos en la inteligencia de las fuerzas de seguridad. Las operaciones de inteligencia han sido revisadas, estudiadas y se han transformado lenta pero constantemente. La mayoría de los esfuerzos se han centrado en la reorganización de las infraestructuras de inteligencia a nivel internacional. Estas mejoras permiten que los organismos policiales, estatales y locales puedan desempeñar un mejor papel en la seguridad nacional. Y lo que es más importante, las mejoras en las operaciones de inteligencia ayudan a las fuerzas del orden locales a responder a los delitos "tradicionales".

Dado que las operaciones de inteligencia eficaces pueden aplicarse por igual a las amenazas terroristas y a los delitos, la comunidad, la seguridad nacional y la prevención de la delincuencia local no son mutuamente excluyentes. Sin embargo, las operaciones de inteligencia de los organismos policiales estatales y locales suelen estar plagadas de falta de políticas, procedimientos y protocolos para recopilar y evaluar la información esencial. Para corregir este problema, se necesitan cambios fundamentales en la forma de reunir, evaluar y redistribuir la información. Las funciones tradicionales y jerárquicas de la inteligencia tradicionales y jerárquicas requieren ser sustituidas por estructuras cooperativas y fluidas que puedan recoger información y trasladarla a los usuarios finales con mayor rapidez.

La inteligencia en el entorno policial actual debe adaptarse a las nuevas realidades que presentan el terrorismo y los delitos convencionales. Estas nuevas realidades requieren una mayor colaboración en la recopilación de información y el intercambio de inteligencia. Como resultado, partes de la comunidad que antes no recibían mucha atención de las agencias estatales y locales de aplicación de la ley requieren ahora mayores cuidados. El personal que trabaja en estos y otros sectores clave son ahora activos en la prevención del terrorismo y el control de la delincuencia. Del mismo modo, la policía orientada a la comunidad y a los problemas debe integrarse en las operaciones de inteligencia para abordar los problemas de la delincuencia convencional. El compromiso y la colaboración con la comunidad a todos los niveles es esencial.

El presente estudio pretende realizar una aproximación a los servicios de inteligencia tanto nacionales como internacionales, en su papel de la lucha antiterrorista, analizando qué estrategias y políticas han ido estableciendo para hacer frente a la amenaza global del terrorismo, especialmente a raíz del atentado del 11-S. Tras una primera parte en la que se conceptualizarán los elementos que conforman este estudio, tales como concepto de inteligencia, comunidad de inteligencia, ciberterrorismo o ciberseguridad; el bloque central del estudio revisará la historia y la estructura de los servicios de inteligencia internacionales y españoles; siendo el tercer bloque el destinado a analizar las diferentes estrategias que se han llevado a cabo por la Comunidad de Inteligencia, tras el 11S, llegando así a las conclusiones finales.

2. MARCO TEÓRICO

2.1. Concepto de Inteligencia

Uno de los primeros autores en definir el concepto de inteligencia fue Serman Kent en 1949, que la identificó como tres conceptos (Kent, 1949):

- El producto derivado de la transformación de la información y el conocimiento en inteligencia.
- La organización que realiza esta tarea.
- El proceso mediante el que se lleva a cabo.

Asimismo, podemos definir la inteligencia como el producto que se obtiene, del resultado de someter determinados datos a un proceso intelectual, que los convierte en informes que tratan de satisfacer las necesidades de los decisores políticos, militares, policiales, empresariales, etc., así como para proteger a aquellos mediante las tareas de contrainteligencia (Jiménez, 2018).

Estos servicios se caracterizan por desempeñar sus funciones como asesores del poder político, que, en definitiva, son los que establecen los objetivos a conseguir por parte de la organización de inteligencia. Con motivo de esta labor de asesoramiento, la acción va pasando a un segundo plano. Este proceso es identificado por algunos autores, como un avance hacia la especialización de los servicios como proveedores de inteligencia (Díaz, 2005).

Información e inteligencia no son lo mismo. La información es el punto de partida del denominado ciclo de inteligencia, y es a partir de esa información cuando los analistas aplican unas metodologías en busca de unos objetivos determinados, resultando finalmente que, información e inteligencia, apenas tienen puntos en común. Además, el valor añadido de la inteligencia no se mide únicamente porque es capaz de anticipar acontecimientos, sino también porque aporta un importante y especializado conocimiento.

(Díaz, 2016).

Según figura en la página web del Centro Nacional de Inteligencia (CNI), el término información debe diferenciarse del de inteligencia, ya que información equivale a la noticia de un hecho en su sentido más amplio (CNI, 2016).

Díaz-Caneja (2016), sostiene que, de forma general, la inteligencia puede ser considerada como un proceso complejo que trata de analizar y comprender el significado de la información disponible. La finalidad de la inteligencia es determinar unos hechos, y luego desarrollar inferencias (hipótesis, estimaciones, conclusiones, etc.), que sean precisas y fiables, con el fin de que se puedan utilizar en un proceso de toma de decisiones.

Una definición interesante sobre lo que podemos considerar como inteligencia, sería la acuñada por Thomas F. Troy, a partir de la crítica de la identificación simplista entre información y conocimiento, como conocimiento del enemigo presidido por el secreto, para cuya creación se nutre de las informaciones obtenidas por agentes de información, por medios técnicos o de fuentes y recursos de información abiertos (Esteban, 2004).

2.2. Concepto de Comunidad de Inteligencia

No resulta posible analizar los diferentes estudios en materia de estrategias en la lucha contra el terrorismo sin antes abordar el concepto de "Comunidad de Inteligencia". Para ello se debe de tener en cuenta la complejidad inherente al propio concepto, que fue acuñado desde una perspectiva funcional e intencional en enero del año 1946, cuando, después del malogro informativo que no pudo evitar el desastre de Pearl Harbor, el presidente estadounidense Harry S. Truman emitió la orden de que cualquier actividad que estuviese relacionada con la seguridad nacional y que hubieran de ser desarrolladas por las distintas agencias de inteligencia que, hasta el momento, actuaban sin una mínima interconexión, fuesen planificadas y desarrolladas de un modo coordinado (Galvache, 2005).

Aunque no hay una definición conceptual que esté aceptada generalmente a nivel internacional, sí que hay una postura bastante unánime en lo que se refiere a la naturaleza del concepto: más que una mera lista de datos recopilados a través de distintas fuentes es más bien el producto de un proceso de conexión y análisis de esos datos por parte de los expertos analistas, con el fin de entender y evaluar los hechos que abordan y estar previstos para su posible evolución. De este modo será posible también el suministro de información específica y estructurada que permita a la toma de decisiones adecuadas y la minimización de los riesgos que pueda conllevar cualquier acción (Lista, 2004).

La Comunidad de Inteligencia (en adelante, CI) es un conjunto de organizaciones y agencias dependientes del poder ejecutivo que trabajan separadamente y también en colaboración con el fin de desarrollar actividades de inteligencia requeridas para el buen curso de las relaciones exteriores y la protección de la seguridad del país (Martín, 2019). La CI se ocupan coordinadamente de los objetivos en materia de estrategia del Gobierno de cada nación, gracias al trabajo de una estructura que impulsa y asegura las relaciones y las conexiones precisas dirigidas a optimizar los resultados que se persiguen. El nivel de centralización, las personas que se ubican en la cúpula de la CI o la cifra de agencias y organismos que la conforman son factores vinculados a la administración burocrática de cada Estado, concretamente, el tamaño del país o la categoría de sus estructuras de seguridad e inteligencia (Martín, 2019).

A lo largo de la última década se ha hecho más perceptible la necesidad de promover la acción de la CI en cuanto a entidad que aúna los esfuerzos y trabajos en materia de inteligencia, con el objetivo de maximizar las capacidades de cada Estado de prevenir y dar respuesta ante las posibles amenazas. En este empeño por conseguir una coordinación eficaz, todos los esfuerzos se concentran en el modo de dar a la CI el dinamismo y la flexibilidad necesarias para que se adapten a un entorno cambiante y a unas amenazas inestables y mutables, tal y como recoge el Real Decreto 436/2002 que establece la estructura del Centro Nacional de Inteligencia Española (en adelante, CNI).

Cabe mencionar que, junto a los propios Servicios de Inteligencia, cuyo concepto se abordó en los epígrafes anteriores, cooperan otras organizaciones que se encargan de

suministrar informaciones al Gobierno. En el caso de España, por ejemplo, la Presidencia del Gobierno o los consulados y embajadas, así, ministerios, aduanas, agregados militares que se encuentren en el extranjero o los servicios de información policial conforman una estructura que es necesario integrar dentro de la CI (Rueda, 2015).

Del mismo modo que las necesidades en materia de inteligencia en un Estado aumentan, también evolucionan sus estructuras informativas, lo que a conlleva que sea más complicado de definir las líneas de delimitación entre unas y otras organizaciones y es aquí donde juega su papel la coordinación, como la única forma de lograr el buen funcionamiento de la CI. De todas formas, las estrategias de cooperación no siempre funcionan, a pesar de que sean técnicamente correctas, bien sea por las dos caras marcadas que comporta la CI – una cara cooperativa hacia la toma de decisiones estatales y otra cara en la que las burocracias se disputan la atención y el enriquecimiento (Aranda, 2004).

Pese a la relevancia que tiene la colaboración entre los distintos servicios y organizaciones para el correcto flujo de información y su análisis posterior, resulta bastante frecuente que cada CI nacional opere como una agrupación confederada de servicios en la que no faltan las rivalidades de carácter presupuestario o corporativo y que en más de una ocasión han sido la causa de fallos de funcionamientos que han tumbado la operación en la que se trabajaba. Una de los ejes principales de cualquier CI, independientemente de su ámbito de trabajo o de su tamaño, es su capacidad de coordinar las acciones de todos sus miembros, pudiendo articularse desde una esfera intraestatal – en la que se cuenta con la colaboración entre diferentes Servicios de Inteligencia del Estado –, interestatal – en la que se coordinan las acciones de los Servicios de Inteligencia de diferentes estados, si bien no se contempla cualquier iniciativa hacia la implantación de una CI supranacional ni siquiera a nivel europeo (Álvarez, 2019).

2.3. Intelligence-Led Policing

La “actuación policial basada en la inteligencia” (el término original conocido como “intelligence-led policing”, en adelante ILP) es una práctica que aprovecha los avances tecnológicos en la recopilación y el análisis de datos para generar una valiosa

"inteligencia" que puede utilizarse para dirigir de forma más eficiente los recursos de las fuerzas de seguridad (Martín y Torrente, 2016).

Varias estrategias y filosofías actuales en la aplicación de la ley de las fuerzas del orden tienen una relación directa con la ILP. El término ILE se originó en Gran Bretaña cuando las autoridades policiales del condado de Kent desarrollaron el concepto en respuesta al fuerte aumento de los delitos contra la propiedad, sobre todo robos y hurtos de automóviles, en un momento en el que los presupuestos policiales estaban siendo recortados. Las autoridades creían que un número relativamente pequeño de personas era responsable de un porcentaje comparativamente alto de delitos y se consideró que los agentes de policía tendrían el mejor efecto sobre la delincuencia, centrándose en los delitos más frecuentes que ocurrían en su jurisdicción (James, 2014).

En un esfuerzo por comprender esta nueva filosofía, el ILP ha sido comparado con recientes innovaciones policiales como la policía de proximidad, las estadísticas comparativas y la policía orientada a los problemas. Aunque estos paradigmas policiales tienen puntos en común con la especificidad de los delitos y los problemas en lugar de un enfoque general y el uso de datos para la toma de decisiones basada en pruebas, hay características únicas de la ILP que requieren un cambio en la filosofía y la práctica de la organización (Medina, 2011).

En lugar de ser simplemente un punto de información que se ha añadido a la organización, el ILP proporciona una integración estratégica del análisis de inteligencia en la misión general de la organización. Ratcliffe (2008) se hace eco de este planteamiento al considerar que el ILP implica un reajuste integral de las funciones organizativas derivadas de la capacidad de inteligencia; además, continúa señalando las características organizativas que deben apartarse de las prácticas tradicionales para que un organismo pueda aplicar el ILP. Estas características incluyen la formación específica en materia de inteligencia, la comunicación de la inteligencia en todos los aspectos de la organización y la utilización de la inteligencia para la toma de decisiones estratégicas, tácticas y operativa, un aspecto que solo se puede conseguir si la inteligencia es procesable (Medina, 2011).

Gran parte de la bibliografía relacionada con la aparición del ILP se enmarca en el ámbito de la seguridad nacional. Los autores suelen fusionar los dos conceptos, adoptando la postura de que el ILP es, o bien un componente de la función de seguridad nacional para mejorar la actuación policial tras el 11-S (Oliver 2006; Carter y Carter 2009b) o bien un elemento impulsado por la seguridad nacional como resultado de los incentivos de financiación (Schaible y Sheffield 2012).

La IPL es una empresa de colaboración basada en la mejora de las operaciones de inteligencia y orientada a la comunidad y a la resolución de problemas, que este sector ha considerado beneficioso durante muchos años. Para poner en práctica la IPL, las organizaciones policiales deben reevaluar sus políticas y protocolos actuales. La inteligencia debe incorporarse al proceso de planificación para reflejar los problemas y cuestiones de la comunidad. El intercambio de información debe llegar a ser una política, no una práctica informal y lo más importante es que la inteligencia debe estar supeditada a un análisis de calidad de los datos (Carter, 2019).

El desarrollo de técnicas analíticas, la formación y la asistencia técnica deben ser apoyados, pero debido al tamaño y a los presupuestos limitados, no todos los organismos pueden emplear analistas de inteligencia. No obstante, todos los organismos encargados de la aplicación de la ley tienen un papel en la transformación de las operaciones nacionales de inteligencia.

Varias estrategias y filosofías actuales en la aplicación de la ley tienen una relación directa con la ILP:

1) El “Modelo Nacional de Inteligencia” del Reino Unido considera como resultados deseados de una inteligencia la seguridad de la comunidad, la reducción y el control de la delincuencia. Para lograr estos resultados, el modelo establece los siguientes objetivos:

- Establecer un proceso de tareas y coordinación.
- Desarrollar productos de inteligencia básicos para impulsar la operación

- Desarrollar normas para mejorar las prácticas de formación a todos los niveles
- Desarrollar sistemas y protocolos de inteligencia.

2) “Actuación policial orientada a la solución de problemas” (en adelante, POP) es una filosofía policial desarrollada por Herman Goldstein. Tal y como se concibió originalmente, consideraba el control de la delincuencia como un estudio de los problemas que conduce a una serie de estrategias correctivas y de aplicación de la ley. El modelo sostiene que el análisis, el estudio y la evaluación son el núcleo de esta actuación policial que requiere evaluar cada nuevo problema y desarrollar una respuesta a medida. Este enfoque precisa creatividad continua y no simplemente encontrar una buena idea y aplicarla unilateralmente (Carter, 2019).

El modelo SARA (Scanning, Analyzing, Responding, and evaluation) se considera a veces como sinónimo de esta actuación, si bien es un modelo analítico más amplio que se utiliza en muchos campos.

Biblioteca
UNIVERSITAS Miguel Hernández

2.4. Los servicios de inteligencia

2.4.1. Las agencias internacionales

Los servicios de inteligencia son organismos gubernamentales que se ocupan de la recogida y el análisis de información crítica para garantizar la seguridad y la defensa nacionales. Los métodos de recogida de información pueden incluir el espionaje, la interceptación de comunicaciones, el criptoanálisis, la cooperación con otras instituciones y la evaluación de fuentes públicas (Marrin, 2012).

Incluso cuando actúan legalmente, los servicios de inteligencia protegen y promueven sus intereses y como resultado, están casi siempre inmersos en complejas luchas políticas en varios frentes. El más importante de ellos es el esfuerzo constante por conseguir el mayor número posible de recursos – personas, fondos e influencia en la toma de decisiones – de sus superiores políticos, y para oponerse a los cambios externos (Esteban, 2004).

Los servicios de inteligencia no son instituciones robotizadas, sino cientos o miles de personas que toman y ejecutan decisiones. Hay pocos estudios sociológicos o comparativos de fuentes abiertas de los oficiales de inteligencia. Los funcionarios del servicio exterior suelen pertenecer a las clases socioeconómicas más altas y la naturaleza de su trabajo - vivir y operar en otros países, presentarse como diplomáticos o empresarios e interactuar con los dirigentes políticos del país y del extranjero, requiere una formación universitaria, conocimiento de idiomas y cultura, y confianza en la interacción con los funcionarios diplomáticos y políticos (Lista, 2004).

El principal objetivo de las organizaciones de inteligencia es garantizar la seguridad, un concepto que evalúa el grado de resistencia o protección a las amenazas; así, varios factores son comunes a varios ámbitos de la seguridad (Esteban, 2004):

- Garantía (el nivel de garantía de que un sistema de seguridad se comportará como ha sido evaluado).
- Contramedida (la forma de impedir que una amenaza desencadene un evento de riesgo).
- Riesgo (un posible evento que podría causar una pérdida).
- Amenaza (una forma de desencadenar un evento peligroso).
- Vulnerabilidad (una debilidad de un objetivo que puede ser explotada por una amenaza de seguridad).
- Explotación (una vulnerabilidad causada por una amenaza).

La recopilación, el análisis y el uso de información sobre los opositores han existido desde la antigüedad, comenzando por el antiguo estratega chino Sun Tzu, aproximadamente el 400 a. C. Francis Walsingham fue el primer europeo que utilizó métodos modernos de espionaje en la Inglaterra isabelina, y para hacer frente a las guerras con Francia, Londres también creó un sistema destinado a recopilar información sobre el país y otras potencias (Navarro, 2014). Durante la Revolución Americana, el general estadounidense George Washington desarrolló con éxito un sistema de espionaje para detectar ubicaciones y planes británicos y en la Guerra Civil Americana (1861-1865), Allan Pinkerton primero operó una agencia de detectives, sirviendo luego como Jefe del Servicio de Inteligencia de la Unión en los primeros años. El Imperio austriaco fundó el Evidenzbureau en 1850 como el primer servicio de inteligencia militar permanente (Navarro, 2014).

Muchos fueron los intentos embrionarios durante el siglo XIX en Europa de crear agencias de inteligencia militar (el departamento topográfico y estadístico de T&SD, Deuxième Bureau, el Abteilung alemán, el Ufficio Informazioni del Commando Supremo de Italia o el Servicio Secreto) hasta que, con el estallido de la Primera Guerra Mundial en 1914, todas las grandes potencias contaban con estructuras muy sofisticadas para entrenar y manipular a los espías y para procesar la información obtenida a través del espionaje (Marrin, 2012).

Los servicios de inteligencia se centran actualmente en la lucha contra el terrorismo, dejando relativamente pocos recursos para vigilar otras amenazas a la seguridad. Por esta razón, a menudo ignoran las actividades de información que no suponen amenazas inmediatas para los intereses de su gobierno. (Lista, 2004). Muy pocos servicios externos -la CIA, el SVR y, en menor medida, el SIS, la DGSE francesa y el Mossad - operan a nivel mundial. Estos servicios suelen depender de las relaciones con estos servicios globales para obtener información sobre zonas más allá de sus vecindades inmediatas, y a menudo venden su experiencia regional para lo que necesitan globalmente (Marrin, 2004).

A lo largo de este epígrafe se pretende analizar los principales servicios de inteligencia internacionales, haciendo especial mención a los españoles.
De entre las principales agencias de inteligencia a nivel internacional destacan:

- La Agencia Central de Inteligencia, que se creó en 1947 con la firma de la Ley de Seguridad Nacional por el presidente Truman (CIA.org, s.f.). Una de las principales funciones de la CIA es asistir al director de la Agencia Central de Inteligencia en el desempeño de sus responsabilidades. Al hacer hincapié en la adaptabilidad de su enfoque, la CIA puede adaptar su apoyo a los principales consumidores de inteligencia.

Durante la "Operación Mangosta" de 1961, la CIA envío a 1.500 exiliados cubanos para invadir Cuba, pero la misión fracasó debido a la mala planificación, seguridad y respaldo (Corvalán, 2011). En el año 1968, el presidente Johnson impulsa el esfuerzo de espionaje

ilegal a ciudadanos americanos a través de la CIA con el objetivo de confirmar si había instigadores rusos dentro de las protestas realizadas contra la guerra de Vietnam. Durante la Guerra del Golfo, EE.UU. liberó Kuwait de Irak; con la ayuda de la CIA, EE. UU. alentó con éxito a Saddam Hussein a invadir Irán y luego eventualmente a infiltrarse en Irak (Corvalán, 2011). Las acciones encubiertas se utilizan con frecuencia en las operaciones de inteligencia y no se limitan a la recopilación de información. La CIA es conocida por alentar o asociarse a los compromisos de torturas, malos tratos, desapariciones y ejecuciones extrajudiciales (Institute for Policy Studies, s.f.).

- El Servicio Secreto de Inteligencia (MI6) se fundó en 1909 para proteger al pueblo del Reino Unido, su economía y sus intereses de las amenazas del exterior (McCrum, 2010). Se centra en tres áreas principales, que son la lucha contra el terrorismo, la interrupción de la actividad de estados hostiles y la delincuencia cibernética, siendo el primer ministro es el responsable de los asuntos de inteligencia y seguridad. El derrocamiento del gobierno nacionalista de Mossadeq en Irán fue llevado a cabo por la CIA con la ayuda del MI6. La lucha del movimiento sionista por un estado judío y los actos terroristas clandestinos contra objetivos británicos se convirtieron en un objetivo para la agencia británica. Además, la formación de la coalición de guerra árabe contra Israel en 1948 fue una de las formas más agresivas de acción política encubierta perseguidas por los oficiales de inteligencia arabistas del MI6 (Zamir, 2019).

- El Mossad es una de las tres principales organizaciones de inteligencia de Israel, junto con Aman y el Shin Bet y se ocupa de la recopilación, el análisis y las operaciones encubiertas. El Mossad ha llevado a cabo una operación encubierta contra enemigos de Israel y criminales de guerra nazis. El Mossad se estableció formalmente en diciembre de 1949 como una institución de Coordinación, siendo el sucesor del brazo de inteligencia de la Haganah (Thomas, 2006). La captura del ex nazi Adolf Eichmann en Argentina alentó la competencia y la confianza de la agencia en tales operaciones de alto riesgo.

- El Servicio Federal de Seguridad (en adelante, FSB) es un órgano ejecutivo federal con autoridad para implementar la política gubernamental en materia de seguridad nacional, la lucha contra el terrorismo, la protección y la defensa de la frontera estatal de la

Federación Rusa. Esto incluye la protección de las aguas marítimas interiores, el mar territorial, la zona económica exclusiva, los recursos naturales, etc.
El FSB es el sucesor más poderoso del KGB. Tras la caída de la Unión Soviética en 1991, el FSB asumió poco a poco las responsabilidades de muchos organismos a nivel nacional con un poder que provenía directamente del presidente Putin que anteriormente sirvió en el KGB. Como presidente, Vladímir Putin ha dado prioridad a la restauración de las funciones y los poderes de la agencia y en el año 2003, el Estatuto del Servicio Federal de Seguridad permitió al FSB absorber varias otras agencias que tenían varios servicios, entre ellos el servicio de contrainteligencia, el servicio de seguridad económica o el servicio de fronteras (Bebler, 2015).

- El Research and Analysis Wing (en adelante, RAW) es un servicio civil que opera en la India aunque sus operaciones también han extendido sus esfuerzos a los Estados Unidos para influir en la política exterior del gobierno (Murphy, 2014).
La RAW empezó con 250 personas y un presupuesto de 400.000 dólares y con dos prioridades iniciales: recopilar información contra Pakistán y China y llevar a cabo acciones encubiertas en Pakistán Oriental, el actual Bangladesh (Murphy, 2014).
El papel de la RAW era entrenar a los luchadores por la libertad, crear un enlace diplomático entre Pakistán Oriental y Occidental, llevar a cabo operaciones especiales contra los insurgentes de Naga y Mizo y desarrollar una guerra psicológica contra los líderes de Pakistán (Kesavan, 2020). Otras actividades de la RAW incluyeron la acción encubierta de India en Afganistán durante la ocupación soviética, la asistencia encubierta al Congreso Nacional Africano en África, y la formación y asistencia a agencias de inteligencia extranjeras como en las Maldivas, Botsuana, etc. (Murphy, 2014).

- Dada la situación internacional de más latente actual cabe hacer una mención especial a la agencia de inteligencia militar de Rusia (GRU). La agencia de inteligencia militar de Rusia es una organización grande, expansiva y poderosa responsable de la recopilación de información extranjera y del funcionamiento de las unidades de las fuerzas especiales (spetsnaz) de Rusia. Debido a sus operaciones y responsabilidades, el GRU es uno de los organismos de inteligencia más conocidos de Rusia y desempeña un papel importante en

la política exterior y de seguridad rusa, incluyendo el uso de la desinformación, propaganda y estrategias cibernéticas (Galeotti, 2015).

En los últimos años, los informes han vinculado al GRU con algunas de las operaciones de inteligencia más agresivas y públicas de Rusia (Espona, 2010).
El GRU opera tanto como agencia de inteligencia, recopilando inteligencia humana, cibernética y de señales y como organización militar responsable del reconocimiento en el campo de batalla y el funcionamiento de las principales fuerzas de Rusia (Galeotti, 2015).

2.4.2. Las agencias españolas

En lo que respecta a los servicios de inteligencia españoles, cabe mencionar como antecedentes la OCN-SECED, que se configuraba como una agencia de seguridad independiente que operaba ante las transformaciones que se producían en la España de la Transición liderada por el coronel José Ignacio San Martín (Martín, 2019):

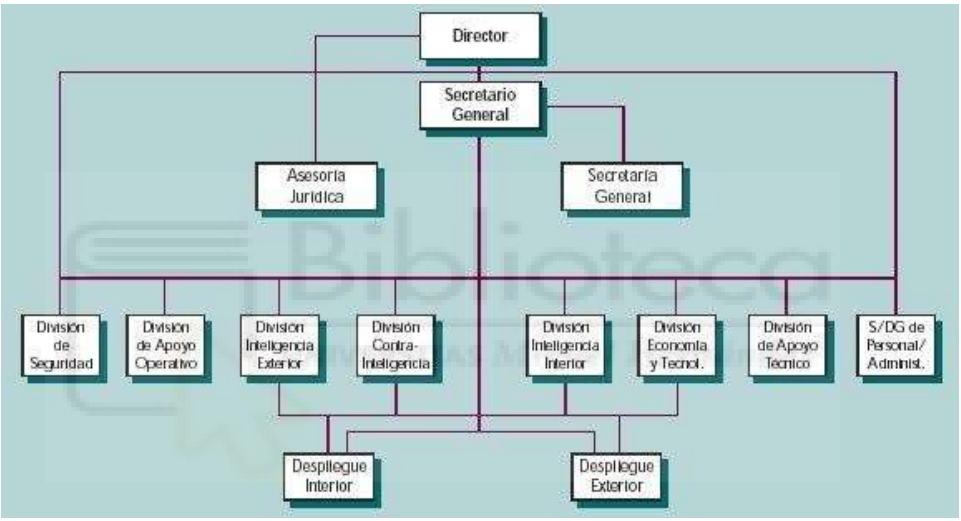
Tras esta organización embrionaria, el primer servicio de información como tal que se creó en España, el CESID, fue creado en el año 1977 en pleno proceso de transformación de las estructuras del régimen franquista.
Durante los primeros años, el CESID puso el foco de su atención en la información militar de cara al interior del Ejército con la finalidad de evitar posibles conspiraciones de regresión al régimen. No obstante, tras el golpe del 23 de febrero de 1981 sus misiones se amplían a procesos de índole terrorista que puedan atentar contra la unidad nacional y la estabilidad de sus instituciones, además de misiones de inteligencia exterior con el fin de conseguir, analizar y divulgar la información precisa para evitar cualquier amenaza o agresión externa contra la integridad del país que comprenda los ámbitos político, militar, económico o tecnológico (Díaz, 2006).

Por último, también le son asignadas misiones de contrainteligencia que comprenden detectar, prevenir, neutralizar y oponerse a actividades de espionaje por parte de servicios de inteligencia extranjeros que puedan ser una amenaza o que supongan un posible

atentado contra los intereses nacionales. Además, a pesar de continuar dependiendo orgánicamente del Ministerio de Defensa, desde el punto de vista funcional pasa a trabajar también para el Presidente del Gobierno (Díaz, 2006).

La estructura del CESID se estructuraba jerárquicamente desde una cúpula en la que figuraba el Director, bajo el que se ubicaba la Secretaría General a la que se incorporaban una serie de unidades, tal y como se refleja en el siguiente organigrama:

Figura 1. *Organigrama organizativo del antiguo CESID*



Fuente. Ministerio de Defensa, 2021.

Cuando Alonso Manglano asumió el mando de la dirección del CESID en el año 1981 comenzó un proceso de modernización de su estructura y el servicio quedaba conformado por las siguientes divisiones: inteligencia interior, inteligencia exterior, contrainteligencia, tecnología y economía (Almenara, 2006).

Esta etapa de expansión y afianzamiento del CESID se vio temporalmente empañada como consecuencia de las filtraciones de información clasificada con fines de manipulación política, algo que suscitó numerosas críticas en contra de los servicios y provocó el nombramiento de un nuevo director, en el año 1995, el General don Félix

Miranda Robredo, al que sucedió un año después el Teniente General Don Javier Calderón (Ruiz, 2005).

El CESID ha sido responsable de los mayores golpes contra la organización terrorista ETA, desarrollando actividades de inteligencia no violentas cuyo objetivo era el conocimiento y la evaluación de los movimientos e iniciativas de apoyo a acciones terroristas nacionales e internacionales dentro de España. Como servicio de inteligencia, el CESID no tenía competencias policiales, sino que sus funciones quedaban limitadas a analizar situaciones que, posteriormente, ponía en conocimiento de los Cuerpos y Fuerzas de Seguridad del Estado, que eran los encargados de perseguir los delitos en defensa de las libertades públicas (Ruiz, 2005).

El CNI, la principal agencia de inteligencia en España, fue creado en mayo de 2002 para sustituir al CESID y cuyo objetivo principal era el de proporcionar al Presidente del Gobierno y al Gobierno de España cualquier información, análisis o propuestas que permitiesen la prevención y de cualquier peligro, amenaza o agresión contra la integridad territorial de España o sus intereses nacionales y la estabilidad de sus instituciones o del Estado de Derecho (Exposición de motivos, LO 11/2002).

Con unos 4.000 efectivos en la actualidad, el CNI mantiene una estructura jerarquizada encabezada por una Dirección (en la actualidad, Doña Paz Esteban), una Secretaría General (en la actualidad, Don Arturo Relanzón) y tres Direcciones - Operaciones, Análisis y Recursos – además de otros órganos de apoyo a la Dirección, así como componentes adicionales en toda España y en el extranjero (CNI, 2021). El CNI desempeña sus funciones y misiones de acuerdo con la Directiva de Inteligencia y en coordinación directa con el resto de las instituciones de inteligencia y seguridad del país, a través de la Comisión Delegada del Gobierno para Asuntos de Inteligencia (Revenga, 2019).

El CNI funciona como agencia de contrainteligencia designada por el Gobierno, así como servicio responsable de la salvaguarda de la información clasificada y seguridad de la información a través del Centro Criptológico Nacional (en adelante, CCN). También se

encarga de la investigación de los refugiados, tarea que comparte con el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (en adelante, CITCO), que depende del Ministerio del Interior (Revenga, 2019).

Desde siempre, los servicios de inteligencia españoles han tenido un fuerte componente de carácter militar, tanto en su estructura, como en sus misiones o la plantilla de personal. El CNI heredó del CESID, una plantilla conformada en su mayor parte por militares y miembros del Cuerpo de la Guardia Civil o de la Policía, algo que se ve justificado por la necesidad de la propia organización de protegerse ante una posible infiltración de cualquier otro servicio de contrainteligencia procedente del extranjero (Díaz, 2005). Sin embargo, en la década de los ochenta se dieron una serie de cambios en esa política de recursos humanos y comenzó a contemplarse la amplia contratación de personal civil, sobre todo mujeres.

A pesar de las reformas emprendidas en los últimos años y del aumento de personal civil, la cultura institucional de la organización continúa teniendo un marcado carácter militar, que se justifica por varios motivos. La primera razón es la indudable tradición militar de sus predecesores inmediatos y otro de los argumentos es que es una unidad organizativa del Ministerio de Defensa desde su origen hasta el año 2011 y que tiene una estructura organizativa típicamente militar y sus miembros están sometidos a un sistema disciplinario muy parecido al de las FAS. Además, se destaca la presencia de una elevada cifra de personal militar, policial y guardias civiles entre el personal, incluyendo muchos de los mandos intermedios y directores, y esta dimensión militar se extiende a varios componentes clave de la cultura del Centro, como los derechos y deberes, los valores e ideales y las obligaciones de su personal (Sánchez, 2019).

Por último, debido al ya referido componente militar de la propia cultura institucional de la organización, es preciso revisar las “Reales Ordenanzas para las Fuerzas Armadas” (Gobierno de España, 2009), en donde se establecen los valores y principios que han de conducir la conducta del personal militar, así como los factores personales y profesionales a las que deben aspira, y que son la igualdad, la dignidad, la solidaridad, el patriotismo, la justicia, la entrega abnegada, la obediencia, el honor o la lealtad.

En 1941 se constituye el Servicio de Información de la Guardia Civil (en adelante, SIGC), con los cometidos principales de vigilancia e información. En sus inicios tuvieron que hacer frente a los maquis que mermaban su capacidad operativa y que hicieron poner en marcha las distintas estrategias de información de este recién nacido servicio español.

A medida que el servicio se va especializando, surgen la ocasión de crear el primer grupo operativo, en plena Guerra Fría, y España se convierte en aliado estratégico de los Estados Unidos, lo que despierta la curiosidad internacional sobre el Estado español. De ese primer grupo operativo, que pasó por distintas nomenclaturas, salieron las primeras hornadas de agentes que se dedicaron íntegramente a la lucha antiterrorista en las décadas más crudas para España, durante la época más sanguinaria de la banda E.T.A.- solo en el año 1980, la banda terrorista asesinó a 91 víctimas. En la actualidad no ha habido demasiada modificación en la estructura y funciones del SIGC, salvo la escisión en el año 2007 de la Jefatura de Información y Policía Judicial (en adelante, JIPJ) que centra su actividad principalmente en la gestión de la información especializada en la seguridad y la lucha antiterrorista (Hernández, 2016).

Por último, dentro del Cuerpo Nacional de Policía se encuentra la Comisaría General de Información, que tiene asignadas como funciones, desde el año 2012, las de captación, recepción y tratamiento de la información que resulte de interés para la seguridad pública (Padilla, 2016). En especial, se centra en la información relativa a la lucha antiterrorista, tanto a nivel nacional como internacional.

Dentro de la Comisaría General de Información se encuentra la sección especializada TEDAX, cuyos agentes intervienen en casos en los que se detecten supuestos artefactos incendiarios o explosivos, del mismo modo que actúan en su recogida, transporte, análisis y estudio de sus componentes y restos de los referidos artefactos o sustancias explosivas (policia.es).

En el ámbito de la inteligencia española, no obstante, es reseñable la carencia de una coordinación por parte de todos los servicios de inteligencia, dada la distinta naturaleza

que los componen, si bien es un aspecto en el que se vienen trabajando en las últimas décadas, dada la necesidad de trabajar en la misma dirección, contra un enemigo común.

2.5. Principales amenazas a las que se enfrentan los servicios de inteligencia en la actualidad (Ciberterrorismo y Ciberseguridad).

El término "ciberterrorismo" combina dos conceptos: "ciber", referido al ciberespacio, y "terrorismo", cuyo significado y alcance se analizará más adelante. Sobre esta base, podemos asumir que el ciberterrorismo es un tipo especial de terrorismo, donde el "lugar" o "medio" en el que se lleva a cabo es el ciberespacio (Conway, 2014). El ciberespacio se considera una red globalmente interconectada de información digital e infraestructuras de comunicación entendida normalmente como Internet y, más ampliamente, como las redes informáticas (Sánchez, 2021).

El concepto de ciberterrorismo suele referirse a un abanico de acciones muy diferentes, desde la simple difusión de propaganda en línea, pasando por la alteración o destrucción de información, hasta la planificación y realización de atentados terroristas mediante el uso de redes informáticas. Por ello, para comprender mejor qué es el ciberterrorismo se delimitará el concepto y lo distinguirá de otros con los que guarda cierta similitud.

Se ha escrito mucho sobre el tema del ciberterrorismo, a pesar de no existir un consenso unánime sobre su alcance y significado. Por así decirlo, para que el ciberterrorismo sea, efectivamente, una forma de terrorismo, debe cumplir con la estructura, el principio de daño y los elementos del terrorismo. En consecuencia, el alcance del ciberterrorismo se basa, como su nombre indica, en el "lugar" en el que se produce o el "medio" a través del cual se lleva a cabo: en el ciberespacio en lugar del mundo físico. Desde este punto de vista, el ciberterrorismo no es un delito autónomo, que deba ser castigado de forma

independiente. Más bien, implica un tipo de terrorismo caracterizado por un método de ejecución único (Pérez, 2020).

Que el ciberterrorismo se defina por su ubicación o por el medio a través del cual se ejecuta puede ser criticado en cierta medida y para hacer frente a estas críticas se puede hacer una comparación con los actos terroristas de secuestro de aviones, como los ataques terroristas del 11 de septiembre en el World Trade Center; o los ataques terroristas con vehículos, como el perpetrado en el paseo marítimo de Niza en 2016. En realidad, el alcance del ciberterrorismo parece seguir la tendencia general de que muchos fenómenos del "mundo real" se reproduzcan en línea (Sánchez, 2015).

Las raíces de la noción de ciberterrorismo se remontan a principios de la década de 1990, cuando el rápido crecimiento del uso de Internet y el debate sobre la emergente "sociedad de la información" provocaron varios estudios sobre los riesgos potenciales a los que se enfrentaba un Estados Unidos altamente interconectado y dependiente de la tecnología. Ya en 1990, la Academia Nacional de Ciencias comenzó un informe sobre la seguridad informática con las siguientes palabras: "Estamos en peligro. Cada vez más, Estados Unidos depende de los ordenadores (…). El terrorista de mañana puede ser capaz de hacer más daño con un teclado que con una bomba". Al mismo tiempo, se acuñó el término prototípico de "Pearl Harbor electrónico", vinculando la amenaza de un ataque informático a un trauma histórico estadounidense (Cruzado, 2011).

Las fuerzas psicológicas, políticas y económicas se han combinado para promover el miedo al ciberterrorismo. Desde una perspectiva psicológica, dos de los mayores temores de la época moderna se dan lugar en el término referido; el miedo a la victimización aleatoria y violenta se combina con la desconfianza y el miedo absoluto a la tecnología informática.

Aunque el ciberterrorismo no implica una amenaza directa de violencia, su impacto psicológico en la sociedad puede ser tan poderoso como el efecto de las bombas terroristas. Tras el 11-S, el discurso sobre seguridad y terrorismo no tardó en dar protagonismo al ciberterrorismo, algo que resultaba comprensible dado que se esperaban

más ataques y la red parecía ofrecer a Al Qaeda oportunidades para infligir enormes daños (Desmedt, 2004).

Pero el nuevo enfoque del ciberterrorismo cuenta también con una dimensión política; los debates sobre la seguridad nacional, incluida la seguridad del ciberespacio, siempre atraen a los poderes políticos y el debate sobre el ciberterrorismo no fue una excepción a este patrón. Por ejemplo, Yonah Alexander, investigador de terrorismo del Instituto Potomac -un grupo de expertos con estrechos vínculos con el Pentágono- anunció en diciembre de 2001 la existencia de una "Red Iraquí". Esta red supuestamente consistía en más de cien sitios web creados en todo el mundo por Irak desde mediados de los años noventa para lanzar ataques de denegación de servicio (DoS) contra empresas estadounidenses - estos ataques hacen que los sistemas informáticos sean inaccesibles, inutilizables o no funcionen (Bendrath, 2003). Cualesquiera que sean las intenciones es evidente que una declaración de este tipo podía respaldar los argumentos que se esgrimían entonces a favor de una política agresiva de Estados Unidos hacia Irak, si bien a día de hoy todavía no ha salido a la luz ninguna prueba de una Red Iraquí.

La lucha contra el ciberterrorismo se ha convertido no solo en una cuestión muy politizada, sino también en uno económicamente rentable. Ha surgido toda una industria para hacer frente a la amenaza del ciberterrorismo: los grupos de reflexión han lanzado proyectos elaborados y han publicado distintos *libros blancos* sobre el tema, los expertos han testificado sobre el tema de los peligros del ciberterrorismo ante el Congreso, y las empresas privadas han desplegado apresuradamente consultores de seguridad y programas informáticos diseñados para proteger objetivos públicos y privados (Cruzado, 2011). Por último, también los medios de comunicación se han sumado al coro del miedo al descubrir que el ciberterrorismo es una herramienta llamativa y dramática.

Para comprender mejor lo señalado, hay que tener en cuenta no solo los conceptos de terrorismo y ciberterrorismo, en el sentido mencionado, sino también las nociones de delincuencia informática, ciberdelincuencia y delincuencia común. Cabe señalar que, aunque no todos los autores distinguen entre delincuencia informática y ciberdelincuencia, diferenciarlas puede ser útil a efectos de análisis.

Los delitos informáticos pueden clasificarse en delitos informáticos en sentido amplio y delitos informáticos en sentido estricto. Los delitos informáticos en sentido amplio son delitos tradicionales que se cometen a través de mecanismos informáticos o de internet. Respectivamente, las tecnologías de la información y la comunicación han ampliado los contextos o medios de ejecución de ciertos delitos tradicionales, como el fraude o los abusos sexuales, que ahora también pueden ser cometidos a través de ordenadores o de internet. En consecuencia, el delito informático en sentido amplio también se ha denominado delito cometido "a través" de sistemas informáticos (Clough, 2010).

Los delitos informáticos en sentido estricto, en cambio, son nuevos delitos cometidos hacia los sistemas informáticos o internet. Por lo general, se trata de acciones dirigidas contra el software y, por ello, este fenómeno también ha sido etiquetado como delito cometido contra los sistemas informáticos. Suele incluir delitos como el sabotaje informático (destrucción o inutilización de datos o software), el espionaje informático (acceso u obtención ilegal de datos o software) y el fraude informático (alteración o manipulación de datos o software) (Jijena, 2008).

Los ciberdelitos son delitos informáticos (en sentido amplio o estricto) que se cometen a través de Internet. A diferencia de los delitos informáticos, que se perpetran "a través" o "contra" los sistemas informáticos, los ciberdelitos se realizan siempre en un contexto específico: el ciberespacio. En este sentido, lo que define un ciberdelito no es su comisión a través o contra un sistema informático, sino un lugar o medio específico de perpetración. Ambos conceptos no se excluyen mutuamente y pueden estar presentes juntos; por ejemplo, la difusión de pornografía infantil a través de Internet constituye un ciberdelito y un delito informático en sentido amplio, mientras que la destrucción de datos de sistemas informáticos efectuada en el ciberespacio constituye un ciberdelito y un delito informático en sentido estricto (Cough, 2010).

Por último, los delitos comunes son todos aquellos que no pueden clasificarse como delitos informáticos o ciberdelitos, ni de ninguna otra manera en particular. Por lo tanto, su definición se determina siempre por proceso de eliminación. Por ejemplo, el robo es

un delito común, del mismo modo que el homicidio. Si esos delitos se cometen mediante un dron operado por radiocontrol, no se clasifican como ciberdelitos. El radiocontrol es un sistema cerrado, por lo que queda fuera de Internet. Aunque ambos ejemplos pueden cometerse utilizando tecnología, escapan al fenómeno de la computación o ejecución en el ciberespacio (Gillespie, 2016). Un sujeto que pertenezca a una organización terrorista puede realizar todas las actividades comentadas anteriormente, es decir, delitos informáticos, ciberdelitos o delitos comunes. Sin embargo, para ser calificado como comportamiento terrorista, es necesario que estén presentes la estructura, el principio de daño y los elementos del terrorismo. Para el ciberterrorismo, además, el comportamiento terrorista debe llevarse a cabo "en" o "a través" del ciberespacio. En consecuencia, no todos los ciberdelitos ni delitos informáticos ejecutados por alguien perteneciente a una organización terrorista deben calificarse de terrorismo o ciberterrorismo. Y, ciertamente, no todos los delitos comunes ejecutados por un "terrorista" deben ser considerados como terrorismo o ciberterrorismo (Goodman et al., 2007).

Figura 2. *Los Estados y los grupos que financian suponen la principal amenaza de ciberseguridad para el Centro Criptológico Nacional*

Fuente. Poveda y Torrente (2016)

Tampoco se configura el ciberterrorismo cuando alguien que pertenece a una organización terrorista comete un acto terrorista utilizando tecnologías distintas de las

redes informáticas. Por ejemplo, una organización que pone una bomba en un hospital lleno de pacientes cuyo detonante es un teléfono móvil activado a través de una llamada telefónica. Si esa organización lleva a cabo un atentado de este tipo para desestabilizar el orden constitucional democrático, su comportamiento puede calificarse de terrorismo, pero no de ciberterrorismo, ya que no se ha ejecutado en el ciberespacio ni empleando redes informáticas (Goodman et al.,2007).

Podría decirse que los medios de comunicación han exacerbado la amenaza actual que supone el ciberterrorismo, dado que todavía no se ha registrado ningún caso. Los sistemas informáticos de defensa e inteligencia de los principales estados están protegidos y, por tanto, aislados de Internet; los sistemas gestionados por empresas privadas son más vulnerables a los ataques, pero también más resistentes de lo que se suele suponer; la gran mayoría de los ciberataques son lanzados por piratas informáticos con pocos o ningún objetivo político y sin deseo de causar más que desorden y caos (Jones, 2005).

Las razones por las que se ha expresado tanta preocupación por una amenaza relativamente menor son muchas. En primer lugar, la atracción que ofrece en cuanto a su originalidad o su innovación. En segundo lugar, los medios de comunicación a menudo no distinguen entre *hacking* y ciberterrorismo y exageran la amenaza de este último, razonando a partir de falsas analogías como la siguiente: "Si un niño de dieciséis años puede hacer esto, ¿qué podría hacer un bien financiado?". La ignorancia es un tercer factor: el ciberterrorismo fusiona dos esferas -el terrorismo y la tecnología- que mucha gente, incluida la mayoría de los legisladores y altos funcionarios de la administración, no comprenden del todo y, por tanto, tienden a temer. Además, algunos grupos están ansiosos por explotar esta ignorancia y numerosas empresas tecnológicas, han tratado de atraer subvenciones para la investigación, presentándose como innovadoras en el ámbito de la seguridad informática y, en consecuencia, contribuyentes vitales a la seguridad nacional (Lewis, 2002).

Verton (2003) sostiene que Al Qaeda ha demostrado tener un apetito incesante por la tecnología moderna y proporciona numerosas citas de Bin Laden y otros líderes de Al Qaeda para mostrar su reconocimiento de esta nueva arma cibernética. Tras los atentados

del 11-S, Bin Laden habría hecho una declaración a un editor de un periódico árabe en la que afirmaba que cientos de científicos musulmanes estaban con él y utilizarían sus conocimientos, que abarcaban desde la informática a la electrónica, contra los infieles". El jeque Omar Bakri Muhammad, un partidario de Bin Laden y a menudo el conducto de sus mensajes al mundo occidental, declaró en una entrevista, que Verton recoge en la misma obra, que aconsejaría a quienes dudan del interés de Al Qaeda en las armas cibernéticas que tomen a Osama Bin Laden muy en serio.

Es posible que los futuros terroristas vean un mayor potencial para el ciberterrorismo que los terroristas de hoy. La próxima generación de terroristas está creciendo en un mundo digital, en el que herramientas de piratería informática son cada vez más potentes, más fáciles de usar y más accesibles. El ciberterrorismo también puede resultar más atractivo a medida que los mundos real y virtual están más estrechamente unidos. Por ejemplo, un grupo terrorista podría hacer estallar una bomba en una estación de tren y lanzar un ciberataque contra la infraestructura de comunicaciones, lo que magnificaría el impacto del evento. Paradójicamente, es probable que el éxito de esta lucha contra el terror haga que los terroristas recurran cada vez más a armas no convencionales como el ciberterrorismo y, por tanto, el reto que se plantea es la necesidad de evaluar qué medidas tomar para hacer frente a esta ambigua, pero potencial amenaza del ciberterrorismo, pero hacerlo sin inflar su importancia real ni manipular el miedo que inspira.

Denning (2011) y otros expertos en terrorismo concluyen que, al menos por ahora, los vehículos secuestrados, camiones bomba y armas biológicas parecen suponer una amenaza mayor que el ciberterrorismo. Sin embargo, al igual que los acontecimientos del 11 de septiembre cogieron al mundo por sorpresa, también podría un gran ciberataque. La amenaza del ciberterrorismo puede ser exagerada y manipulada, pero no puede negarse ni ignorarse.

2.6. Principales estrategias de los servicios de inteligencia tras el 11S.

A partir de lo expuesto hasta el momento, se comprende que el creciente flujo de información y comunicación ha permitido una evolución en las organizaciones de

inteligencia. Dentro de las expectativas que abordan las estrategias actuales de los servicios de inteligencia pueden contemplarse las siguientes:

- "El paradigma de la inteligencia nacional acabará por caer en la obsolescencia y se requerirán nuevas instituciones y sistemas de inteligencia.
- Surgirán nuevas competencias y áreas de conocimiento en los estudios de inteligencia.
- Algunas fuentes y métodos importantes utilizados hoy en día perderán su importancia.
- Surgirán nuevos actores en la producción y obtención de inteligencia.
- Con el aumento del entorno competitivo del conocimiento no habrá monopolio intelectual.
- El frágil mundo de la información dará lugar a la importancia de la fiabilidad" (Agrell y Treverton, 2014: 144-145)

Ante este panorama, el avance del siglo XXI que devino del 11S, inició una era de vigilancia, seguimiento y escuchas a través de los medios garantizados por una tecnología enormemente avanzada. Para desarrollar las actuales políticas en materia de terrorismo, los profesionales de la inteligencia debieron desarrollar un sistema que práctico e innovador, a la vez que proporcionaba información con una calidad considerable para incidir en las decisiones. Estas estructuras, en las que la innovación y la creatividad pasan a primer plano, se adaptaron a las nuevas condiciones rápidamente (Agrell y Treverton, 2014).

Empero, las capacidades, funciones, políticas y organizaciones deben responder a las exigencias del cambiante medio de seguridad, un cambio que llega con la necesidad de un personal que investigue el sistema y encuentre perspectivas de futuras alternativas. La amplitud del espectro de precedencia trajo consigo la especialización dentro de los servicios de inteligencia y los métodos de externalización, lo que supuso que el poder se deslizase progresivamente hacia actores no gubernamentales (ONG, grupos terroristas, etc.).

Después del 11S, la evolución de los servicios puso en primer plano cuatro funciones de la inteligencia (Ariely, 2014). Se trata de la inteligencia exterior, la operación clandestina, la contrainteligencia y la inteligencia doméstica. Asimismo, tras los atentados, el gobierno federal solicitó 4.500 millones de dólares para la seguridad de las infraestructuras, y el FBI cuenta ahora con más de mil investigadores cibernéticos. Antes del atentado, George W. Bush, entonces candidato presidencial, advirtió que las fuerzas americanas estaban sobreexplotadas y faltas de fondos, precisamente cuando se enfrentaban a una serie de amenazas y desafíos como serían la proliferación de armas de destrucción masiva, el aumento del ciberterrorismo o la proliferación de la tecnología de misiles. Después de los atentados, el ya presidente Bush creó la Oficina de Seguridad del Ciberespacio en la Casa Blanca y nombró a su antiguo coordinador antiterrorista, Richard Clarke, para dirigirla (Ariely, 2014). Blanco Navarro (2011), a diez años del atentando, llevó adelante un diagnóstico, a partir del cual se derivan una serie de estrategias que fueron aplicadas de manera generalizada por los servicios de inteligencia tras el 11S. Dicho diagnóstico detectaba:

Biblioteca
UNIVERSITAS Miguel Hernández

> Descoordinación entre servicios, entre fuerzas policiales, y entre servicios de inteligencia y policías. Descoordinación en el seno de las propias organizaciones. Ausencia en la Administración de generalistas con visión global, estratégica y de futuro, marcada en parte por la sujeción al desarrollo de un plan a cuatro años, que es el plazo de una legislatura. Falta de medios personales y técnicos para enfrentar los riesgos. Ausencia de colaboración, cooperación internacional. Poco aprovechamiento de la información de fuentes abiertas, información utilizada intensivamente por AQ y grupos terroristas. Rigidez general, organizativa e institucional, burocratización, mucho procedimiento. Necesidad de sistemas menos jerárquicos, más organizados en red, y no únicamente en la ausencia de imaginación (Comisión 11-S). Necesidades legislativas, ya comentadas, y orientadas a facilitar la función de obtención de información por servicios de inteligencia y policiales, en equilibrio y con garantías judiciales para el respeto de los derechos y libertades fundamentales. Un acercamiento global al fenómeno del terrorismo, que implique lucha contra la financiación, control de fronteras e inmigración, vinculaciones con

el crimen organizado nacional y transnacional, control de explosivos y armas de destrucción masiva, etc. (2011: 19-20).

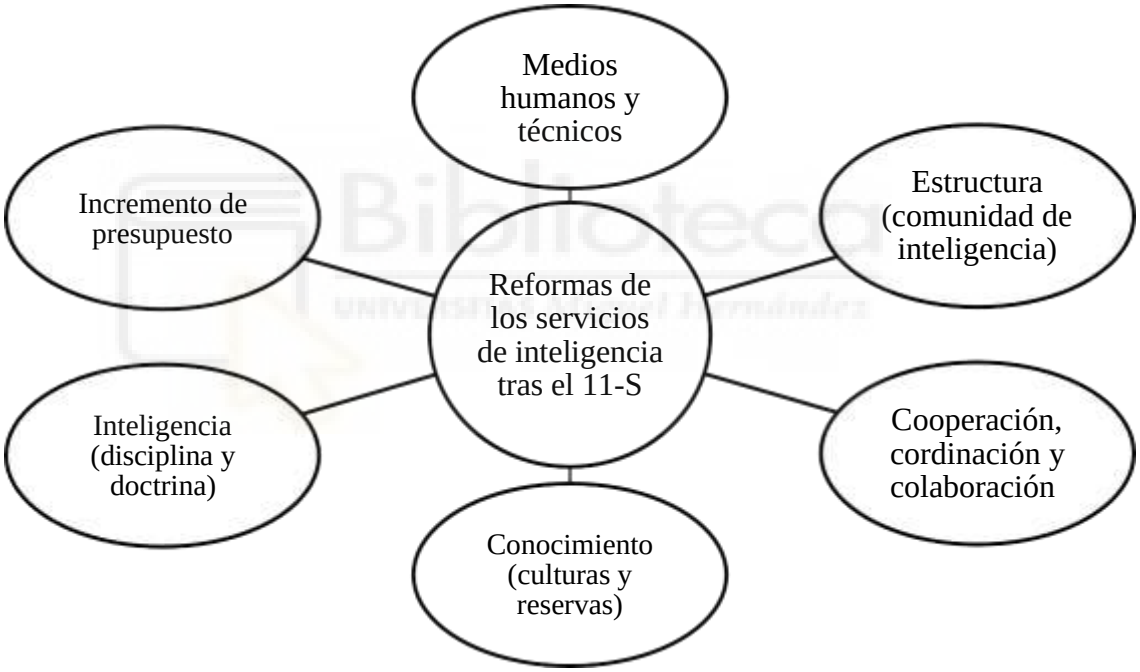
De estas mismas cuestiones se derivan las medidas oportunas para una actuación efectiva (Blanco Navarro, 2011):

1. Incrementos presupuestarios. Incrementos de un 30 % en las asignaciones presupuestarias para los servicios de inteligencia.
2. Medios humanos y tecnológicos. "Medidas también generalizadas en los servicios de inteligencia han ido orientadas a incrementos cuantitativos en sus efectivos. Estas han aumentado sus plantillas entre un 20 % y un 40 %" (2011: 21).
3. Estructuras. "Los graves fallos de detección, análisis, coordinación y difusión de información de Inteligencia, puestos de manifiesto tras los grandes atentados de la década, han obligado a reformar las estructuras para la lucha contra el terrorismo" (2011: 23). Esto es, se crearon "instituciones públicas o privadas, órganos, agencias y servicios de inteligencia e información de un Estado que trabajan, de forma conjunta o separada, para aportar conocimiento que facilite la toma de decisiones en el ámbito de la seguridad y defensa" (2011: 23).
4. Esfuerzos en materia de cooperación, colaboración y coordinación. "Continuos son los esfuerzos en materia de cooperación, colaboración a nivel internacional. Una de las fórmulas más habituales es mediante el intercambio de información en materia de terrorismo, de crimen organizado, de blanqueo de capitales y financiación del terrorismo. Igualmente, las estructuras diseñadas permiten un intercambio de información, de procedimientos, incluso de culturas, entre miembros de diferentes Cuerpos a nivel nacional e internacional. También se han desarrollado programas de colaboración con el sector de la seguridad privada, bajo el principio básico de hacer de la seguridad una cuestión de todos. Finalmente, también se detecta un incremento de proyectos de colaboración entre instituciones públicas y privadas, con participación de la Universidad, y con la finalidad de mejorar procedimientos y tecnologías al servicio de la inteligencia" (2011: 32-33).

5. Reformas en el ámbito del conocimiento. Desarrollo de la noción de cultura de inteligencia como el "conjunto de conocimiento que la sociedad debe tener sobre la necesidad, la función y la finalidad de un Servicio de Inteligencia, de manera que perciba como propias las cuestiones relacionadas con su seguridad, su libertad y la defensa de sus intereses" (2011: 33).

6. Hacia una disciplina o doctrina de inteligencia. Se destacan líneas de investigación, estudios y trabajo en las que se produce la interacción de estos servicios con espacios académicos para mejorar el producto de inteligencia y la seguridad nacional.

Figura 3. *Reformas de los servicios de inteligencia tras el 11-S*



Fuente. Blanco Navarro (2011).

Estas estrategias serán las que se tomarán como eje para el trabajo y desarrollo y discusión de los resultados de la revisión sistemática.

3. JUSTIFICACIÓN DEL ESTUDIO, PREGUNTA DE INVESTIGACIÓN, OBJETIVOS E HIPÓTESIS

3.1. Justificación.

Dado que toda investigación nace de una inquietud inicial, resulta justo identificar la inquietud de la que parte este estudio y que es la de analizar un campo sobre el que no se ha investigado demasiado, que es el de las estrategias que los servicios de inteligencia españoles desarrollan en su lucha contra el terrorismo.

La experiencia española en la lucha contra el terrorismo representa una buena guía de estrategias, acciones y decisiones que se pueden aplicar a la lucha contra el terrorismo actual. Pese a las evidentes diferencias existentes entre los orígenes y los rasgos del terrorismo de grupos como ETA o GRAPO y organizaciones como ISIS, todos ellos comparten una característica común: el ejercicio del terror como medio para la consecución de sus objetivos.

El atentado terrorista del 11-S produjo un cambio en el paradigma mundial en cuanto a la lucha contra el terrorismo, y conllevó a que por parte de la Comunidad de Inteligencia se llevara a cabo una profunda reestructuración de sus políticas y estrategias. En este trabajo se analizarán algunas de estas estrategias, haciendo una revisión sistemática de los estudios en los que se reflejan las mismas, tras el atentado del 11S.

3.2. Pregunta de investigación

La pregunta de investigación de la que parte el presente estudio es: ¿se han adaptado los servicios de inteligencia a los nuevos desafíos actuales en materia de terrorismo tras el 11S?

3.3. Objetivos

Enlazando con la pregunta de investigación, se plantean como objetivos a perseguir los que siguen a continuación.

3.3.1. Objetivo General

- Analizar la estructura y las estrategias de los servicios de inteligencia en la lucha contra el terrorismo.

3.3.2. Objetivos Específicos

- Abordar la situación de los principales servicios de inteligencia nacionales e internacionales, realizando una revisión sistemática de las estrategias aplicadas después del 11S.

Biblioteca
UNIVERSITAS Miguel Hernández

3.4. Hipótesis

En este punto cabe definir cuál es la hipótesis del presente estudio; la cual sería que, "los servicios de inteligencia siguen en constantes evolución y adaptación, y pese al cambio de paradigma tras el 11S, siguen evolucionando para responder a las nuevas amenazas".

4. METODOLOGÍA

4.1. Diseño de investigación

El desarrollo de esta investigación se realizará a partir de una revisión sistemática, conformándose, así, como un estado de la cuestión. De acuerdo con Hurtado de Barrera (2000), este tipo de investigación se aplica cuando las descripciones existentes son insuficientes, se encuentran dispersas, o ha acontecido la aparición de un nuevo contexto. El alcance es descriptivo, cuya importancia radica en que constituye la base y el punto de partida para los tipos de investigación de mayor profundidad. Esto quiere decir que, a partir de la exploración y descripción de las modificaciones en la estructura y las estrategias de los servicios de inteligencia de España en la lucha contra el terrorismo luego del caso 11S como objeto de estudio, se podrán abrir nuevas líneas de investigación para conocer y evaluar sus perspectivas futuras.

Por su parte, Arias (2006) define el diseño de la investigación como "la estrategia que adopta el investigador para responder al problema planteado" (2006: 30). El diseño corresponde así a un tipo de revisión sistemática de la literatura, cuyo objetivo se centra en examinar la evidencia empírica sobre la temática en cuestión, y cuya base o fuente de datos está constituida por información especializada, formalizada en artículos de investigación. Esta misma información se analiza desde un enfoque cualitativo, puesto que "se trata de captar el núcleo de interés y los elementos clave de la realidad estudiada, facilitándose de esta manera el entendimiento de los significados, los contextos de desarrollo y los procesos" (Tonon, 2011: 2).

En este apartado se procede, entonces, con el desarrollo y exposición de la metodología utilizada para llevar a cabo el presente escrito. En la actualidad la información científica que circula ha aumentado de manera exponencial, por lo tanto, se reconoce que el procedimiento de búsqueda debe realizarse de acuerdo a ciertas fases o etapas, bajo criterios de inclusión y exclusión, para promover un entendimiento y desarrollo eficiente (Gómez-Luna, et al., 2014).

4.2. Fuentes de información

Para la búsqueda de la bibliografía pertinente se tuvieron en cuenta diversos materiales formalizados, revisados y referenciados correctamente en revistas de divulgación científica o de investigaciones alojadas en bases de datos, repositorios de universidades y sitios webs. Dentro de estos, se hizo foco en aquellos documentos que enfatizan en la evolución de la estructura y estrategias de los servicios de los diferentes servicios españoles de inteligencia en relación con la lucha contra el terrorismo a partir del caso 11S. Así, se utilizaron bases de datos y repositorios de investigaciones, tales como Dialnet, Redalyc, Scielo y Research Gate. Google Académico fue el principal motor de búsqueda para la localización de documentos alojados en otras bases de datos diversas. Además, se han consultado distintas revistas especializadas como "Revista de análisis y prospectiva" o "*International Journal of Intelligence, Security, and Public Affairs*" así como los fondos públicos del Centro Nacional de Inteligencia. De esta manera, las principales fuentes de información se obtuvieron de internet.

Biblioteca
UNIVERSITAS Miguel Hernández

4.3. Criterios de inclusión y exclusión

Las palabras claves seleccionadas fueron: "Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España" (con sus correspondientes en lengua inglesa). Se emplearon los operadores booleanos "OR" y "AND" con el objetivo de definir las relaciones oportunas entre los conceptos de búsqueda. Se emplearon artículos escritos en español e inglés.

De este modo, como criterios de inclusión se establece: el año de publicación (entre el 2002 y el 2022, es decir, luego del 11S y hasta la actualidad), que relacionen las palabras claves determinadas, y que estuvieran escritos en español o en inglés. Estos últimos fueron traducidos utilizando la herramienta de traducción de archivos DocTranslator. Como criterios de exclusión se determina que no pueden formar parte de la revisión sistemática aquellos artículos escritos antes del 2001, en idioma diferente al español o inglés, y que no se vincule o responda con las exigencias de la temática expuesta.

4.4. Estrategias de búsqueda

Para esta revisión se aplicaron las siguientes estrategias de búsqueda. En primera instancia, se estableció el objeto de la investigación para poder responder a la conformación del estado actual de la cuestión. A partir de ello se establecieron los criterios de inclusión y exclusión para los artículos académicos, se seleccionaron las palabras clave y se llevó a cabo la búsqueda. Una vez realizados esos primeros pasos, se definió la información que era de interés para responder a los objetivos planteados y se seleccionaron los artículos. Posteriormente, se analizó e interpretó su información, para habilitar las discusiones y conclusiones pertinentes.

Los resultados de la búsqueda se plasman a continuación en una tabla, en la cual se indican los artículos identificados tras la búsqueda en las diferentes bases de datos, los artículos seleccionados tras aplicar los criterios de inclusión, los artículos excluidos, los artículos seleccionados para leer el resumen y comprobar su relevancia, los que han sido seleccionados y excluidos tras leer el resumen y, finalmente, los artículos seleccionados.

Biblioteca
UNIVERSITAS Miguel Hernández

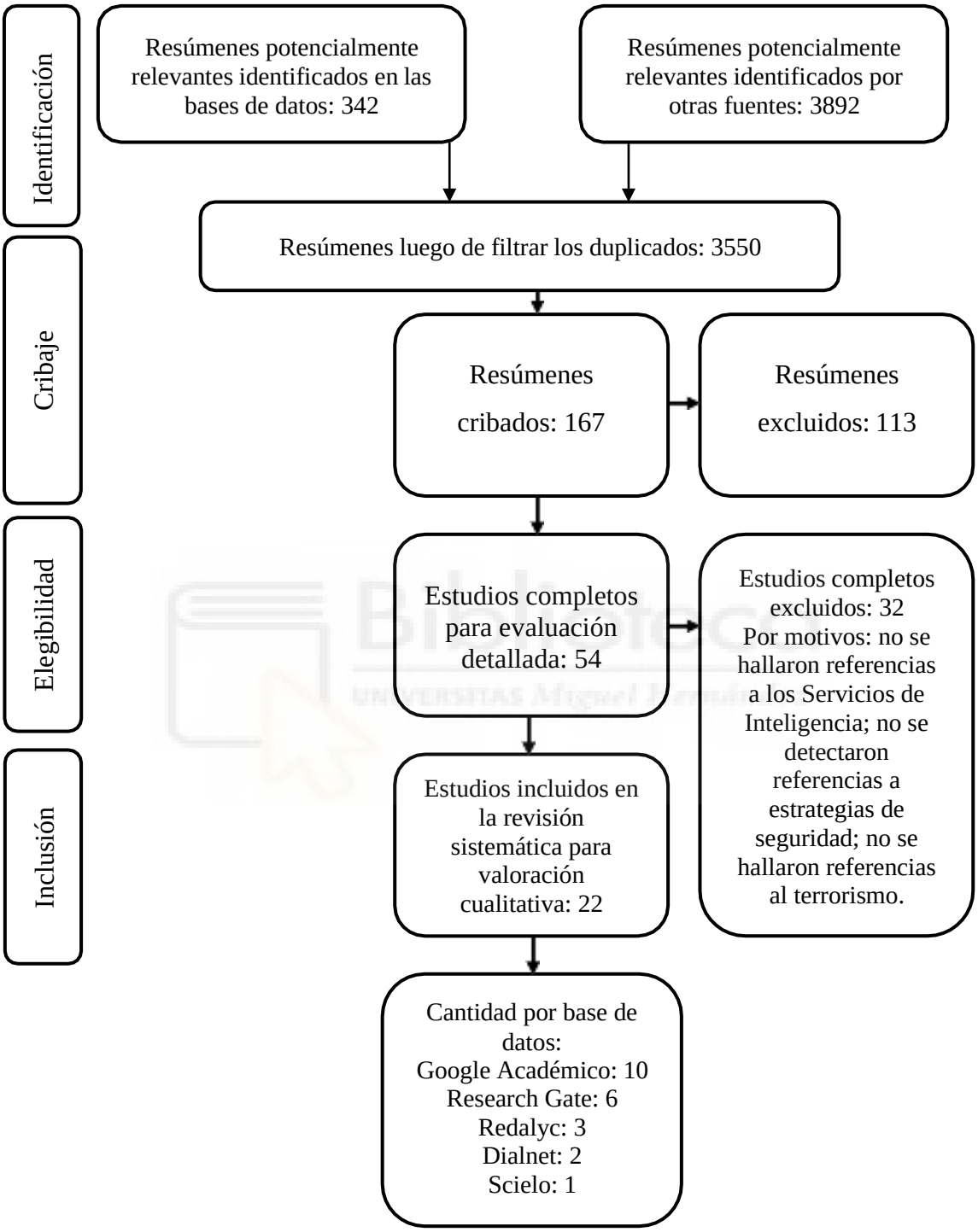
4.4.1. Descripción del proceso de búsqueda (PRISMA)

Tabla 1. *Fases de búsqueda y selección de artículos*

Fase	Artículos
Identificación de estudios	3550 artículos
Cribaje	167 artículos
Elegibilidad	54 artículos
Inclusión	22 artículos

Fuente. Elaboración propia (2022).

Figura 4. *Diagrama de flujo PRISMA (fases de la revisión sistemática)*



Fuente. Elaboración propia (2022).

Como se puede observar, hubo 32 artículos que fueron excluidos de la investigación debido a que, luego de su lectura, no lograron hallarse referencias a los servicios de inteligencia, no fue posible detectar estrategias que hicieran referencia a mejoras en la seguridad y no se hallaron referencias al terrorismo, teniendo en cuenta el 11S o el terrorismo global actual. Por estos motivos, los artículos no eran de utilidad para responder al objetivo de investigación, es decir, no permitían analizar la estructura y las estrategias de los servicios de inteligencia en la lucha contra el terrorismo. Es así que, posterior a la lectura, fueron seleccionados 22 artículos.

4.5. Organización de la información

La información ha sido organizada de acuerdo a las estrategias de Blanco Navarro (2011) que fueron expuestas previamente en el marco teórico. Este modo de organización fue seleccionado debido a que el artículo de Blanco Navarro (2011) analiza las transformaciones producidas a nivel mundial en los servicios de inteligencia pasados diez años del atentado del 11S como hito terrorista. En este sentido, plantea un diagnóstico sobre dichas transformaciones y detecta las estrategias que fueron aplicadas de forma generalizada por los mencionados servicios. Brevemente, se traen a colación las estrategias:

1. Incrementos presupuestarios. Incrementos en las asignaciones presupuestarias para los servicios de inteligencia.

2. Medios humanos y tecnológicos. Mejoras tecnológicas y aumento de personal en los servicios de inteligencia.

3. Estructuras. Reformas estructurales y tecnológicas en los edificios públicos y privados.

4. Esfuerzos en materia de cooperación, colaboración y coordinación. Mejoras en las relaciones internacionales y colaboración entre distintos organismos.

5. Reformas en el ámbito del conocimiento. Desarrollo de la noción de cultura de inteligencia como el "conjunto de conocimiento que la sociedad debe tener sobre la necesidad, la función y la finalidad de un Servicio de Inteligencia" (2011: 33).

6. Hacia una disciplina o doctrina de inteligencia. Se destacan líneas de investigación, estudios y trabajo en las que se produce la interacción de estos servicios con espacios académicos para mejorar el producto de inteligencia y la seguridad nacional.

Biblioteca
UNIVERSITAS Miguel Hernández

5. RESULTADOS

5.1. Artículos seleccionados

Tabla 2. *Selección de artículos para la revisión sistemática*

Art.	Base de datos	Año	Título	Autores	Palabras clave[1]	Estrategias[2]
1	Google Académico	2002	"Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información"	Esteban Navarro, M.A. y Navarro Bonilla, D.	"Servicios inteligencia", "Estrategias de seguridad", "Terrorismo", "España"	5, 6

[1] Las palabras claves expresadas en esta tabla responden a las seleccionadas para la revisión sistemática y se indican aquellas en las que existen coincidencia explícita o temática. Esto es, no se utilizan necesariamente todas las que aparecen indicadas en los artículos seleccionados. Asimismo, aunque no en todos aparezca "estrategias de seguridad" como palabra clave, estas son detectables en la totalidad de los artículos, por lo que son válidos para incluirse en la revisión sistemática.

[2] Estas son: 1. Incrementos presupuestarios; 2. Aumento de medios humanos y tecnológicos; 3. Mejoras en las estructuras; 4. Esfuerzos en materia de cooperación, colaboración y coordinación; 5. Reformas en el ámbito del conocimiento; 6. Disciplina o doctrina de inteligencia (Blanco Navarro, 2011).

2	Google Académico	2004	"Del 11-S al 11-M: el papel de España en la Unión Europea"	Closa, C.	"Estrategias de seguridad", "11S", "Terrorismo", "España" (y Unión Europea).	4, 5
3	Google Académico	2005	"La Formación de la Comunidad de Inteligencia Española: Un proceso en marcha"	Galvache Valero, F.	"Servicios inteligencia", "España"	3, 4
4	Google Académico	2005	"Servicios de inteligencia y lucha antiterrorista"	Jordán Enamorado, J.	"Servicios inteligencia", "Terrorismo", "España"	3, 5
5	Research Gate	2006	"Legislación antiterrorista comparada después de los atentados del 11 de septiembre y su incidencia en el ejercicio de los derechos fundamentales"	Álvarez Conde, E. y González, H.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España"	5, 6
6	Redalyc	2007	"La cooperación entre servicios de inteligencia en el marco de la Unión Europea: ¿cooperación trasnacional o multinacional?"	Díaz, G.	"Servicios inteligencia", "Terrorismo", "España" (y Unión Europea).	2, 3. 4

7	Dialnet	2009	"Inteligencia y terrorismo internacional: un panorama de cambios"	López Espinosa, M.A.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España"	1, 2, 3, 4, 5, 6
8	Research Gate	2010	"Reservas de Inteligencia: hacia una Comunidad ampliada de Inteligencia"	Arcos, R. y Antón, J.	"Servicios inteligencia", "Estrategias de seguridad", "Terrorismo", "España"	1, 2, 4
9	Google Académico	2011	"La seguridad interior en la UE: diez años después del 11-S"	Sorroza Blanco, A.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España" (y Unión Europea).	1, 2, 4
10	Dialnet	2011	"El frenesí legislativo después del 11-S, ¿derechos humanos versus seguridad nacional?"	Martínez Mulero, I.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España" (y Unión Europea).	5, 6
11	Research Gate	2011	"Seguridad, desarrollo y lucha contra la pobreza tras el 11-S: los	Sanahuja, J.A.	"Estrategias de seguridad", "11S", "Terrorismo", "España"	4, 5

			Objetivos del Milenio y la "securitización" de la ayuda"			
12	Dialnet	2011	"¿Son los Servicios de Inteligencia un factor de estabilidad en España?"	Camacho Barrientos, J.	"Servicios inteligencia", "Estrategias de seguridad", "España"	2, 3
13	Google Académico	2012	"La adaptación de los servicios de inteligencia al terrorismo internacional"	Díaz, A.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España"	1, 2, 3, 4, 5
14	Redalyc	2013	"La lucha contra el terrorismo en la estrategia de Seguridad Nacional"	Alonso, A.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España"	1, 2, 3, 4, 5, 6
15	Dialnet	2014	"Recursos humanos y servicios de inteligencia: diez aspectos clave del nuevo estatuto de personal del CNI de 2013"	Bosch, X.	"Servicios inteligencia", "Estrategias de seguridad", "España"	1, 2, 4

16	Dialnet	2016	"El debate entre libertad y seguridad, a través de la legislación antiterrorista aprobada tras el 11-S"	Carrasco Durán, M.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo"	1, 2, 5
17	Scielo	2016	"La lucha antiterrorista y el nuevo sistema de seguridad internacional tras el 11 de septiembre: ¿una consecuencia lógica?"	Garrido, A.P.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo"	1, 2, 3
18	Google Académico	2017	"La reciente evolución de la estrategia antiterrorista, test de la estrategia global de seguridad de la UE"	Ramón Chornet, C.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España" (y Unión Europea).	4, 5, 6
19	Dialnet	2019	"El papel de España frente al terrorismo internacional y la seguridad exterior (2001-2017)"	Iturriaga Barco, D.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España"	1, 4, 5

20	Google Académico	2019	"Seguridad y terrorismo: cambios en las estrategias de seguridad de España, Francia y Reino Unido ante la emergencia del Estado Islámico"	Ubierna, M.V.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España"	1, 2, 5, 6
21	Google Académico	2020	"Secreto de Estado y servicios de inteligencia"	García Novoa, E.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España"	5, 6
22	Google Académico	2021	"Los servicios de inteligencia y la lucha antiterrorista"	Romay-Ventas, I.	"Servicios inteligencia", "Estrategias de seguridad", "11S", "Terrorismo", "España"	3, 5

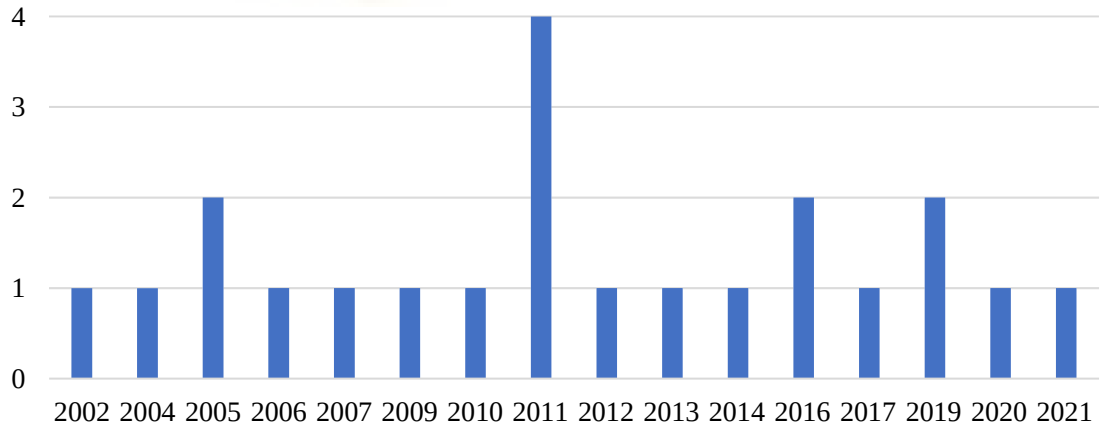
Fuente. Elaboración propia (2022).

5.2. Análisis de los artículos

En este punto se hace relevante exponer las características de los artículos analizados en la revisión sistemática. Por consiguiente, se procede a describir la muestra de estudio. En primera instancia, se expuso anteriormente que 10 artículos fueron obtenidos utilizando Google Académico como base de datos principal. Dialnet fue la segunda base que mayores resultados obtuvo (6 artículos), mientras que Scielo que la que menor cantidad de artículos considerables arrojó (1 artículo).

Con respecto al año de publicación, como se evidencia en el siguiente gráfico, el año 2011, a diez años del atentado del 11S, es el que mayor producción teórica al respecto tuvo, mientras que los demás años se mantuvieron relativamente estable. A 20 años del mencionado atentado, a producción teórica no tuvo crecidas significativas, mientras que en el corriente año no se detectaron artículos o publicaciones que fuesen de relevancia para responder a los objetivos planteados en el presente escrito.

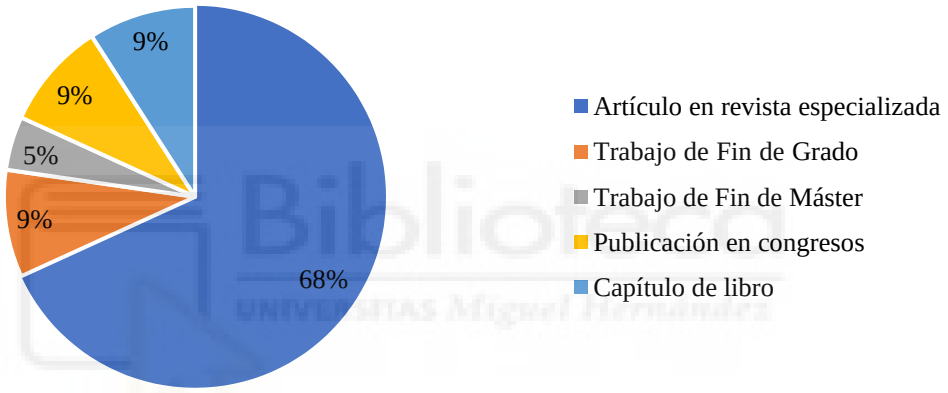
Figura 5. *Año de publicación*



Fuente. Elaboración propia (2022).

Por otro lado, las publicaciones halladas fueron mayoritariamente artículos de revistas. Los trabajos de investigación de grado o máster fueron escasos, al igual que las publicaciones de congresos y capítulos de libros. Asimismo, no se plasma un gráfico sobre la metodología de los artículos porque el 100 % responde a investigaciones y revisiones de índole teórica. Es así que la muestra total se encarga de analizar legislaciones existentes, establecer comparativas a partir de documentos, y llevar adelante revisiones de la literatura sobre la temática.

Figura 6. *Tipo de publicación*

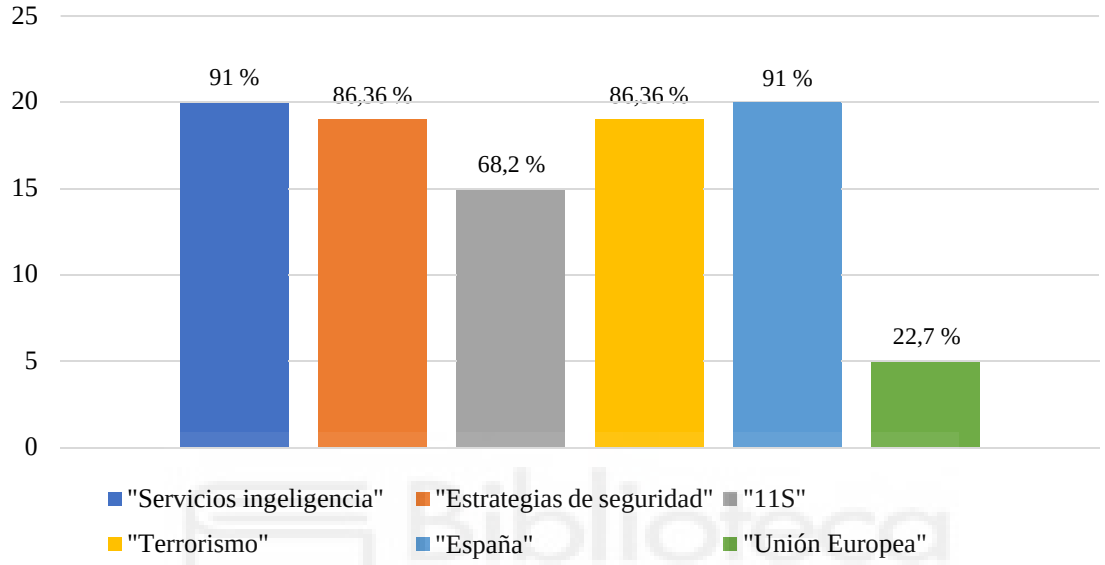


Fuente. Elaboración propia (2022).

Asimismo, fue importante detectar la aparición de las palabras clave seleccionadas para la revisión. Como se observa, el 91 % de los artículos tienen como objeto de estudio los servicios de inteligencia, al igual que están contextualizados en España en particular, aunque cinco de los mismos también hacen referencia al panorama de la Unión Europea. Asimismo, el 86,36 % de las publicaciones refieren a las estrategias de seguridad, pudiéndose inferir en el 13,64 % restante. El 68,2 % de la muestra explicita la situación del atentado del 11S y el 86,36 % se vincula con distintas modalidades del terrorismo. De esta manera queda en evidencia la notoria relevancia de los artículos seleccionados para llevar adelante el análisis de la estructura y las estrategias de los servicios de inteligencia

en la lucha contra el terrorismo en España, como así también para abordar la situación de los principales servicios de inteligencia internacionales.

Figura 7. *Palabras clave*



Fuente. Elaboración propia (2022).

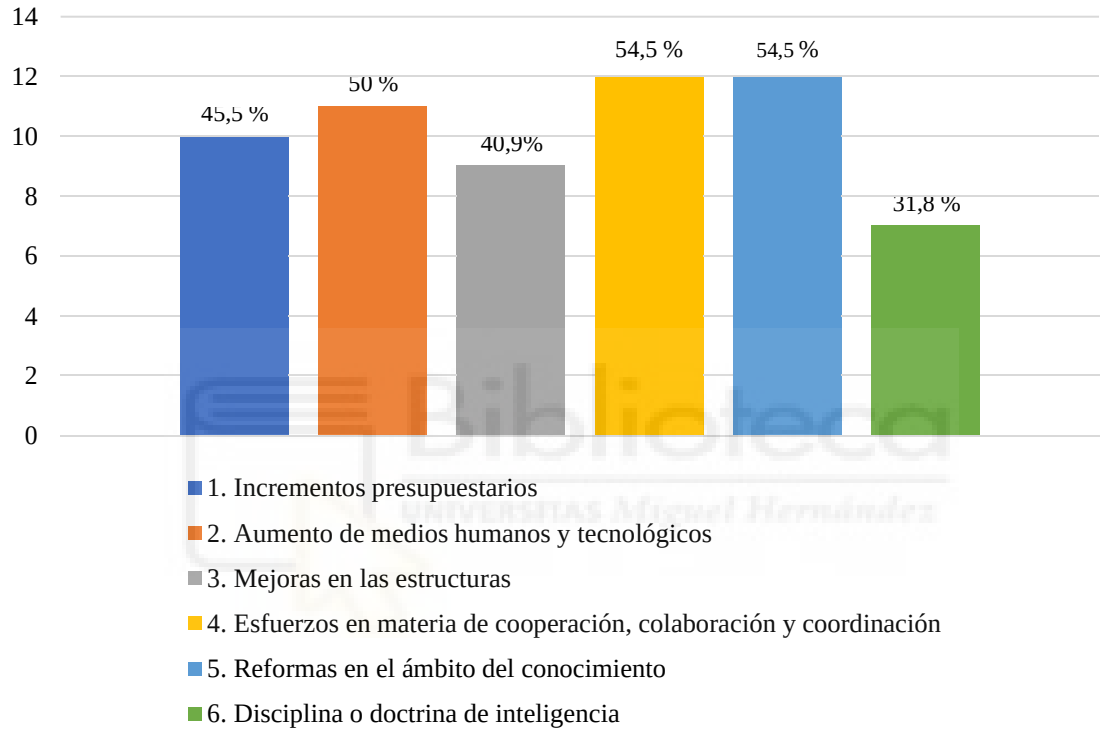
Ahora bien, el foco de esta revisión está puesto en la detección de las estrategias de seguridad aplicadas dentro de los servicios de inteligencia para optimizar la lucha contra el terrorismo. Estas mismas estrategias se vinculan directamente con las estructuras de estos servicios, puesto que hacen referencia tanto a recursos materiales como humanos y económicos destinados a generar mejoras constantes. Asimismo, se centra en revelar la evolución y transformaciones en este ámbito luego del atentado del 11S en Estados Unidos. Las estrategias limitadas responden a las propuestas por Blanco Navarro (2011). Estas son:

1. Incrementos presupuestarios.
2. Aumento de medios humanos y tecnológicos.
3. Mejoras en las estructuras.
4. Esfuerzos en materia de cooperación, colaboración y coordinación.

5. Reformas en el ámbito del conocimiento.
6. Disciplina o doctrina de inteligencia.

De acuerdo con ello, la revisión sistemática ha sido de utilidad para determinar cuáles de estas estrategias han sido las más relevantes, tal y como se indica en el siguiente gráfico.

Figura 8. *Estrategias de seguridad de los Servicios de Inteligencia luego del 11S*



Fuente. Elaboración propia (2022).

El gráfico expuesto permite evidenciar que tanto los esfuerzos en materia de cooperación, colaboración y coordinación, al igual que las reformas en el ámbito del conocimiento, fueron las estrategias que mayor relevancia presentaron. Los artículos indican que, debido al atentado del 11S, se estableció un cambio de paradigma en materia de relaciones regionales e internacionales, al igual que la necesaria redefinición de las conceptualizaciones en torno a la seguridad y las estrategias. Es por ello que, estos puntos, como se observa, presentan un mayor porcentaje.

Empero, el aumento de recursos y de presupuesto destinado a los servicios de inteligencia y la seguridad también es de notoria relevancia, seguido de las mejoras en las estructuras. Sin embargo, es necesario destacar que las primeras tres estrategias se entrelazan directamente, ya que el incremento del presupuesto se destina a generar mejoras, tanto de recursos humanos como materiales.

Finalmente, puede observarse que, en menor medida, aparece la idea de generar una doctrina de inteligencia. No obstante, las nuevas informaciones y reformas en el ámbito del conocimiento implica, necesariamente, una optimización de la disciplina, por lo que, igualmente, se vinculan de manera directa.

De esta manera puede comprenderse que, a partir del 11S, las estrategias que se aplicaron en materia de seguridad y servicios de inteligencia fueron múltiples, pero todas responden necesariamente a la prevención de riesgos, a la optimización y mejora de los recursos, al fortalecimiento de las relaciones regionales e internacionales, y la divulgación de información e investigaciones de notoria importancia para seguir mejorando en estas cuestiones.

Poniendo en relación el año de publicación con las estrategias de seguridad, para corroborar si en ciertos períodos fue más importante alguna en particular, puede determinarse que no existe una relación directa. Esto se indica a partir de la siguiente información:

Tabla 3. *Relación año de publicación y estrategia abordada*

Año de publicación	Estrategias
2002	5, 6
2004	4, 5
2005	3, 4, 5
2006	5, 6

2007	2, 3, 4
2009	1, 2, 3, 4, 5, 6
2010	1, 2, 4
2011	1, 2, 3, 4, 5, 6
2012	1, 2, 3, 4, 5
2013	1, 2, 3, 4, 5, 6
2014	1, 2, 4
2016	1, 2, 3, 5
2017	4, 5, 6
2019	1, 2, 4, 5, 6
2020	5, 6
2021	3, 5

Fuente. Elaboración propia (2022).

Lo que puede observarse es que, en el 2009, 2011 y 2013, los artículos seleccionados hicieron referencia a todas las estrategias mencionadas por Blanco Navarro (2011), mientras que en el 2012 y 2019 lo hicieron parcialmente. Por lo que puede determinarse que el año 2011 fue el más prolífico respecto al análisis de las transformaciones en los servicios de inteligencia con relación al área de seguridad, no solo por mayor cantidad de artículos publicados sobre el tema, sino también por llevar adelante un abordaje más profundo. En el resto de las publicaciones, en esta línea, se detecta un menor tratamiento sobre las estrategias de seguridad, pero, tal y como se indicó en el gráfico 8, fueron tenidas en cuenta de forma bastante equitativa, por lo tanto, puede determinarse que es posible cumplir con los objetivos propuestos en la presente investigación.

6. DISCUSIÓN

La última década ha presentado grandes avances con respecto a la promoción de acciones enfocadas en la Comunidad de Inteligencia como una entidad que se entrelaza con cuestiones referentes a la seguridad y la lucha contra posibles amenazas externas como son los hechos de terrorismo (Rueda, 2015). Las organizaciones y agencias del Estado que forman parte de esta Comunidad trabajan tanto independiente como dependientemente con el fin de proteger la seguridad del país. En el caso de España existen, como se expuso, el CNI o los servicios creados a tal efecto dentro del Cuerpo Nacional de Policía o el Cuerpo de la Guardia Civil (Díaz, 2006; Revenga, 2019).

El 11S fue un hecho que puso en evidencia la importancia de actualizar y mejorar los servicios de seguridad, provocando un cambio de paradigma (Agrell y Treverton, 2014). De ello, Blanco Navarro (2011) expuso una serie de estrategias que fueron aplicadas en la primera década, tanto internacionalmente como en España en particular. Fueron numerosos los autores que hicieron referencia a la importancia de incrementar los presupuestos, aumentar y mejorar los medios humanos y tecnológicos, aumentar los esfuerzos de colaboración y cooperación internacional, llevar adelante reformas en cuestiones del conocimiento y promover una disciplina de la seguridad e inteligencia, en lo cual se destacan las múltiples líneas de investigación, estudios y trabajos que se vinculan con estos servicios en pos de mejorar los productos de seguridad nacional e inteligencia (Esteban Navarro y Navarro Bonilla, 2002; Closa, 2004; Díaz, 2007; López Espinosa, 2009; Sorroza Blanco, 2011; Alonso, Garrido; 2016; Ubierna, 2019; García Novoa, 2020; entre otros).

Es importante destacar que los avances tecnológicos, tal y como señalan los artículos de la revisión sistemática, han posibilitado la mejora en la comunicación y el transporte, como así también aumentar la vigilancia y seguimiento a grupos potencialmente peligrosos que puedan atentar contra la seguridad del país. Para el desarrollo de las actuales políticas en materia de terrorismo, los profesionales de la inteligencia fueron desarrollando un sistema práctico e innovador para proporcionar información de calidad considerable. Estas estructuras, en las que la innovación y la creatividad pasan a primer

plano, se fueron adaptando a las nuevas condiciones rápidamente (López Espinosa, 2009; Alonso, 2013; Ramón Chornet, 2017).

Las capacidades, funciones, políticas y organizaciones se transformaron para responder a las exigencias del cambiante medio de seguridad, un cambio que llegó con la necesidad de un personal que investigue el sistema, encuentre perspectivas de futuro alternativas en lugar del mero *statu quo*, entre otros puntos de importancia. La amplitud del espectro de precedencia trajo consigo la especialización dentro de los servicios de inteligencia y los métodos de externalización, lo que supuso que el poder se deslizase progresivamente hacia actores no gubernamentales. Es así que, después del 11S, la evolución de los servicios puso en primer plano cuatro funciones de la inteligencia: la inteligencia exterior, la operación clandestina, la contrainteligencia y la inteligencia doméstica (Ariely, 2014). Estas se relacionan con las estrategias de mejora en materia de seguridad, posicionándose como las actividades más significativas que los servicios modernos para prevenir los ataques a sus Estados.

Desde lo expuesto en el marco teórico y en estrecha relación con la revisión sistemática de la literatura, puede detectarse que los servicios de inteligencia, a raíz de los avances tecnológicos y las características del terrorismo global actual (mediado por ciberataques y atentados contra la información) han debido, indefectiblemente, realizar mejoras en todas las esferas. De alguna manera, la actualidad está atravesada por una lucha de poder en la que la información y el conocimiento son los principales objetivos. Así, el presente siglo XXI implica una vigilancia constante y una protección de la información. Después del 11S, la evolución de los servicios puso en primer plano las funciones de la inteligencia. La contrainteligencia, el contraterrorismo, la lucha contra los estupefacientes y contra el armamento se posicionan como las actividades más significativas que los servicios modernos que están llevándose a cabo para prevenir múltiples y diversos ataques. Es así que, en la estructuración de los servicios de inteligencia, la colaboración de los analistas y los responsables de la toma de decisiones hizo que la inteligencia se haya ido politizando (Ubierna, 2019).

De estas cuestiones puede considerarse que, entonces, la revisión sistemática de la literatura ha sido suficiente para dar respuesta a las interrogantes planteadas en la presente investigación y dar por cumplimentados los objetivos propuestos.

Sin embargo, pueden presentarse algunas limitaciones al respecto. En primer lugar, el alcance descriptivo de las revisiones sistemáticas requieren, indefectiblemente, estudios más profundos. Además de ello, limitar la búsqueda al idioma español e inglés deja de lado un universo teórico por explorar, que sería importante analizar. Por otro lado, con respecto a posibles líneas de investigación, por ejemplo, podría pensarse en estudios de casos particularizados, comparaciones entre distintos organismos, etc., para corroborar el nivel de aplicación de las estrategias de seguridad desarrolladas en este trabajo. Otra investigación podría conformarse igualmente como una revisión, pero que incorpore artículos previos al 2001 para establecer una comparativa de los servicios de inteligencia y sus estrategias de seguridad antes y después del 11S.

De esta forma, puede determinarse que, si bien los objetivos de la presente investigación han logrado cumplimentarse, el objeto de estudio no se ha agotado. Es por ello que se estima la relevancia de seguir profundizando en las cuestiones de seguridad, especialmente teniendo en cuenta el contexto tecnologizado y globalizado de la actualidad, en el que la información circula exponencialmente por las redes y cualquier fallo en estos sistemas pone en riesgo la estabilidad mundial.

7. CONCLUSIONES

El objetivo de la presente investigación se enfocó en analizar la estructura y las estrategias de los servicios de inteligencia en la lucha contra el terrorismo, con el fin de responder a la interrogante enfocada en las adaptaciones de los servicios de inteligencia españoles e internacionales a los nuevos desafíos actuales en materia de terrorismo. De ello se hipotetizó que los servicios de inteligencia siguen en constantes evolución y adaptación y, pese al cambio de paradigma tras el 11S, siguen evolucionando para responder a las nuevas amenazas.

De esta forma, los servicios de inteligencia son de importancia para informar a los responsables políticos de cuestiones de importancia, proteger información confidencial, propiciar la cobertura se seguridad global, para resolver conflictos de productividad entre la inteligencia humana y la tecnológica, para el establecimiento de bancos de datos, para reunir la inteligencia para cubrir el vacío de información antes de las prioridades, en la producción y capacidades en función de las necesidades, para la gestión eficiente de presupuestos y, especialmente, para la seguridad general contra acciones terroristas y ciberterroristas.

Gracias al desarrollo del marco teórico y normativo, la búsqueda de antecedentes y la revisión sistemática de la literatura puede concluirse que la hipótesis ha sido corroborada. En este sentido, fueron múltiples las estrategias aplicadas a mejorar y optimizar los servicios de inteligencia en materia de seguridad.

Con los trágicos acontecimientos del 11 de septiembre de 2001 en Estados Unidos, los atentados del 7 de julio de 2005 en Londres, los atentados del 10 de marzo de 2010 en el metro de Moscú, el aumento de los grupos extremistas en varias regiones, la actualidad del conflicto Ucrania-Rusia, y demás atentados contra la seguridad nacional, puede determinarse la importancia de la actuación de los servicios de inteligencia y las estrategias de seguridad en esta materia. En definitiva, las políticas antiterroristas modernas y proactivas se pueden resumir en atacar al terrorista y sus activos a través de medios convencionales. Y las políticas más defensivas que han surgido a lo largo de los

años incluyen erigir barreras tecnológicas como, por ejemplo, detectores de metales o equipos de detección de bombas en los aeropuertos con el objetivo de fortificar los objetivos potenciales y asegurar las fronteras. Si bien es teórico, analítico y descriptivo, la evidencia expuesta pone en evidencia los esfuerzos de los servicios de inteligencia para mejorar la seguridad, quienes han definido diversos mecanismos comunes de lucha contra el terrorismo a través de acciones defensivas y preventivas.

No obstante, actualmente siguen mejorando y adecuándose a las nuevas tecnologías e innovaciones. Por consiguiente, 20 años después del 11S, los avances han sido numerosos, pero no han cesado. Se espera que en los próximos años, junto a nuevos avances, estos servicios sigan mejorando para responder a las necesidades de la sociedad, como así también para responder frente a amenazas cada vez más sofisticadas, como es el ciberterrorismo y los ciberataques.

Biblioteca
UNIVERSITAS Miguel Hernández

8. BIBLIOGRAFÍA

Adaev, V. (2021). Concept Of Information Security Of The Russian Federation. *Ways Of Implementation,* 1(6), 38-44.

Agrell, W. y Treverton, G. (2014). *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy.* Oxford Scholarship. DOI:10.1093/acprof:oso/9780199360864.001.0001

Almenara, V. (2006). *La adquisición de información para la seguridad y defensa del estado. Servicios españoles de inteligencia (1968-1981).* Universidad de Málaga.

Alonso, A. (2013). La lucha contra el terrorismo en la estrategia de Seguridad Nacional. *UNISCI Discussion Papers,* 35, 223-248. Recuperado de https://www.redalyc.org/pdf/767/76731410012.pdf

Álvarez, T. (2019). Introducción a la actividad de Inteligencia. *Congreso de la asociación de Constitucionalistas de España "Seguridad y Libertad"*, 1-20.

Álvarez Conde, E. y González, H. (2006). Legislación antiterrorista comparada después de los atentados del 11 de Septiembre y su incidencia en el ejercicio de los derechos fundamentales. *Elcano Newsletter*, 7. Recuperado de https://www.researchgate.net/publication/28105083_Legislacion_antiterrorista_comparada_despues_de_los_atentados_del_11_de_septiembre_y_su_incidencia_en_el_ejercicio_de_los_derechos_fundamentales

Aranda, E. (2004). Servicios de Inteligencia: un estudio comparado. *Cuadernos de estrategia.* Ministerio de Defensa.

Arcos, R. y Antón, J. (2010). Reservas de Inteligencia: hacia una Comunidad ampliada de Inteligencia. *Inteligencia y Seguridad,* 8, 11-38. Recuperado de https://www.researchgate.net/publication/276044211_Reservas_de_Inteligencia_hacia_una_Comunidad_ampliada_de_Inteligencia

Arias, F.G. (2012). *El Proyecto de Investigación. Introducción a la metodología científica.* Episteme. Recuperado de

https://www.academia.edu/23573985/El_proyecto_de_investigaci%C3%B3n_6ta_Edici%C3%B3n_Fidias_G_Arias_FREELIBROS_ORG

Ariely, G. (2014). Cyberterrorism. En Chen, T., Jarvis, L., Macdonald, S (auts). *Adaptive Responses to Cyberterrorism*. (175-195). Springer.

Bebler, A. (2015). Crimea and the Russian-Ukrainian Conflict. *Romanian Journal of European Af airs*, 15(1), 35-54.

Bendrath, R. (2001). The Cyberwar Debate: Perception and Politics in U.S. Critical Infrastructure Protection. *Information & Security*, 7, 80–103.

Bergman, R. (2018). The Secret History Of Mossad, Israel'S Feared And Respected Intelligence Agency. [online] Newstatesman.com.

Blanco Navarro, J.M. (2011). Seguridad e inteligencia: 10 años después del 11-S. *Documento Marco.* IEEE. Recuperdo de https://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM09-2011SeguridadInteligencia.pdf

Boltaina, X. (2012). El personal del Centro Nacional de Inteligencia: su vínculo jurídico como "empleado público" y la afectación de sus derechos y deberes. *Inteligencia y seguridad: Revista de análisis y prospectiva*, 11, 183-212.

Bosch, X. (2014). Recursos humanos y servicios de inteligencia: diez aspectos clave del nuevo estatuto de personal del CNI de 2013. *Inteligencia y Seguridad*, 15, 77-103. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=5568424

Camacho Barrientos, J. (2011). ¿Son los Servicios de Inteligencia un factor de estabilidad en España? *Derecom*, 5. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=7680423

Carrasco Durán, M. (2016). El debate entre libertad y seguridad, a través de la legislación antiterrorista aprobada tras el 11-S. En Pérez Francesch, J.L. y Molinares Hassan, V. (Coords.), *En defensa del estado de derecho: estudios sobre las tensiones entre la seguridad y la libertad en el mundo de hoy* (43-66). Universidad del Norte. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=8321278

Carter, D.L. y Carter, J.G. (2009b). The intelligence fusion process for state, local and tribal law enforcement. *Criminal justice and behavior*, 36 (12), 1323–1339

Carter. J.G. (2019). Community Policing and Intelligence-Led Policing: An Examination of Convergent or Discriminant Validity. *Policing: An International Journal, 1*-31

Clough, J. (2010). *Principles of Cybercrime*. New York: Cambridge University Press.

Closa, C. (2004). Del 11-S al 11-M: el papel de España en la Unión Europea. *Elcano Newsletter*, 3. Recuperado de http://biblioteca.ribei.org/id/eprint/611/

Collina, C. (2019). Cooperating with a Vertical Partner: Central Power and Regional Governors in Putin's Russia. En *Russia on the Eve of Election.* EU-Russia Centre.

Conway, M. (2014). Cyberterrorism. En Chen, T., Jarvis, L., Macdonald, S (auts.). *Reality Check: Assessing the (Un)Likelihood of Cyberterrorism*, 103-121. Springer.

Corvalán, L. (2011). Las acciones encubiertas norteamericanas entre el 4 de septiembre y el 4 de noviembre de 1970, según el informe Church y otros documentos desclasificados por los EE.UU. *Universidad Academia de Humanismo Cristiano. Tiempo Histórico*, 2, 117-132

Cruzado, J. A. (2011). *Delitos Informáticos y Ciberterrorismo: Fundamentos de Investigación.* Instituto Tecnológico Superior de Libres.

Denning, D. (2011). 10 Years After September 11, A Social Science Research Council Essay Forum. En Whither Cyber Terror? Springer

Desmedt, I. (2004). Análisis científico del Ciberterrorismo. *Novática: Revista de la Asociación de Técnicos de Informática*, 172, 33-37.

Dezcallar, J. (2002). Los servicios de inteligencia: una herramienta indispensable. En M. A. Aguilar y J. M. Ridao (Eds.), *El terrorismo: una amenaza del siglo XXI.* XIV Seminario Internacional de Defensa. Asociación de Periodistas Europeos.

Díaz, A. (2012). La adaptación de los servicios de inteligencia al terrorismo internacional. *Elcano Newsletter*, 52. Recuperado de http://biblioteca.ribei.org/id/eprint/1007/

Díaz, A.M. (2001). La función de los servicios de inteligencia. De Cueto, C. y Jordán J. (Coords). *Introducción a los Estudios de seguridad y defensa.* Ed. Linares.

Díaz, A.M. (2006). *Los servicios de inteligencia españoles. Desde la Guerra Civil hasta el 11-M - Historia de una transición.* Alianza.

Díaz, G. (2007). La cooperación entre servicios de inteligencia en el marco de la Unión Europea: ¿cooperación trasnacional o multinacional? *UNISCI Discussion Papers*, 13, 43-51. Recuperado de https://www.redalyc.org/pdf/767/76701304.pdf

Díaz, G. (2016). El papel de la inteligencia en la lucha contra el terrorismo salafista yihadista. *Revista CIDOB d'Afers Internacionals*, 116, 207-228

Díaz-Caneja, J.M. (2016). La cooperación de inteligencia en la Unión Europea. *Pre-bie3*, 6.

Ehrman, J. (2009). *What are We Talking About When We Talk about Counterintelligence?* Center for the study of intelligence [Online] Cia.gov.

Espona, R.J. (2010). Los servicios de inteligencia en los países post-soviéticos. *Inteligencia y Seguridad 8, 7*3-90.

Esteban Navarro, M.A. y Navarro Bonilla, D. (2002). Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información. *El profesional de la información*, 12(4), 269-281. Recuperado de http://eprints.rclis.org/24076/

Esteban, M. A. (2004). Necesidad, funcionamiento y misión de un Servicio de Inteligencia para la Seguridad y la Defensa. En D. Navarro, F. et al. (eds.) *Estudios sobre inteligencia: fundamentos para la seguridad internacional (Cuadernos de Estrategia no 127)*, 60-87. Instituto Español de Estudios Estratégicos.

Estevens, J. (2020). Building intelligence cooperation in the European Union. *JANUS.NET*, 11(2), 90-105.

Federal Security Service (FSB). [online]

Galeotti, M. (2015). *Spetsnaz: Russia's Special Forces.* Osprey Publishing, 8-11.

Galvache Valero, F. (2005). La Formación de la Comunidad de Inteligencia Española: Un proceso en marcha. *Arbor,* 180(709), 183–205. Recuperado de https://arbor.revistas.csic.es/index.php/arbor/article/view/502

García Novoa, E. (2020). *Secreto de estado y servicios de inteligencia*. Universidad de Salamanca. Recuperado de https://gredos.usal.es/handle/10366/144886

Garrido, A.P. (2016). La lucha antiterrorista y el nuevo sistema de seguridad internacional tras el 11 de septiembre: ¿una consecuencia lógica? *Foro internacional*, 56(4), 941-976. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-013X2016000400941

Gillespie, A. (2016). *Cybercrime: Key Issues and Debates*. London: Routledge.

Gobierno de España (1995). Real Decreto 1324/1995 por el que se establece el Estatuto del personal del CESID. *Boletín Oficial del Estado*, 198, 25845 - 25856.

Gobierno de España (2002). Ley 11/2002 reguladora del CNI. *Boletín Oficial del Estado*, 109, 16440.

Gobierno de España (2004). Real Decreto 327/2004 por el que se modifica el Estatuto del personal del CNI. *Boletín Oficial del Estado*, 51, 9342 - 9351.

Gómez-Luna, E; Fernando-Navas, D; Aponte-Mayor, G. y Betancourt-Buitrago, L. (2014). Metodología para la revisión bibliográfica y la gestión de información de temas científicos, a través de su estructuración y sistematización. *Revista Dyna*, 81(184), abril, 158-163. Recuperado de https://www.redalyc.org/articulo.oa?id=49630405022

González, J.L. (2016). Servicios de inteligencia y contraterrorismo. Guillermo Portilla (dir.) *Terrorismo y contraterrorismo en el siglo XXI: un análisis penal y político criminal*, 115-135.

González-García, A. y Girao, F.J. (2020). Capacidades prospectivas y de defensa en la lucha contra el Ciberterrorismo. *Relaciones Internacionales*, 28, 58.

Gonzálvez, J. (2021). Opciones estratégicas de Rusia desde la óptica del neorrealismo ofensivo. *Revista de Estudios en Seguridad Internacional*, 7(2), 145-166.

Goodman, S. et al. (2007). Cyberspace as a medium for terrorists. *Technological Forecasting and Social Change*, 74(2), 193-210.

Hernández, J- (2016). El servicio de información de la Guardia Civil (SIGC). 75 años de Historia. *Cuadernos de la Guardia Civil*, 75 Aniversario, 8-30

Hurtado de Barrera, J. (2000). *Metodología de la Investigación.* Quirón. Recuperado de https://ayudacontextos.files.wordpress.com/2018/04/jacqueline-hurtado-de-barrera-metodologia-de-investigacion-holistica.pdf

Iturriaga Barco, D. (2019). El papel de España frente al terrorismo internacional y la seguridad exterior (2001-2017). *El reinado de Juan Carlos I (1975-2014): actas VI Congreso Internacional de Historia de Nuestro Tiempo*, 321-327. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6912983

James, A. (2014). Forward to the past: reinventing intelligence-led policing in Britain. *Police Practice and Research*, 15(1).

Jiménez, R. (2005). El CNI: al servicio de España y de los ciudadanos. *Arbor CLXXX*, 709, 153-181.

Jordán Enamorado, J. (2005). Servicios de inteligencia y lucha antiterrorista. *Arbor*, 180(709), 227–246. Recuperado de https://arbor.revistas.csic.es/index.php/arbor/article/view/505

Kesavan, K. (2020) *India'S 'Act East' Policy And Regional Cooperation*. [online] Observer Research Foundation.

Kolbe, P.R., et al. (2022). The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict.. *Harvard Business Review*, 18 Feb. 2022

Lewis, J. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic and International Studies* [En línea].

Lista, F. (2004). Cooperación europea en materia de Inteligencia. Estudios sobre Inteligencia: fundamentos para la seguridad internacional. *Cuadernos de Estrategia,* núm. 127. IEEE-CNI, Ministerio de Defensa.

López Espinosa, M.A. (2009). Inteligencia y terrorismo internacional: un panorama de cambios. *Cuadernos de estrategia*, 141, 197-239. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=3077934

Marrin, S. (2012). Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful. I*ntelligence and National Security*, 27 (3), 398–422.

Martín, J.M. (2019). La comunidad de inteligencia española, presente y futuro. *XIX CEMFAS*, 175-214.

Martínez, J.A. (2012). El reclutamiento de personal en el Centro Nacional de Inteligencia (CNI). *Papeles del Psicólogo*, 33(3), 202-210

Martínez Mulero, I. (2011). El frenesí legislativo después del 11-S, ¿Derechos humanos versus seguridad nacional? *Revista Aequitas*, 1, 71-81. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=3819449

McCrum, R. (2010) MI6: The History Of The Secret Intelligence Service, 1909-1949 By Keith Jefery. Book Review. [online] The Guardian.

Murphy, J. (2014). India's Secret Wars Part 3: Research And Analysis Wing (RAW) SOFREP. [online] SOFREP.

Navarro, D. (2014). Espionaje, seguridad nacional y relaciones internacionales. *Colección de estudios internacionales*, 14, 1-45

Ofek, R., 2015. *"Operation Opera": Intelligence Behind-The-Scenes.* Israel Defense. [online] Israeldefense.co.il.

Pérez, A. (2020). Ciberterrorismo, ¿una nueva amenaza? *Bie3: Boletín IEEE,* 19, 386-400

Ramón Chornet, C. (2017). La reciente evolución de la estrategia antiterrorista, test de la estrategia global de seguridad de la UE. *Anuario Español de Derecho Internacional*, 33, 103-126. Recuperado de https://revistas.unav.edu/index.php/anuario-esp-dcho-internacional/article/view/16915

Ratcliffe, J.H. (2008) *Intelligence-led policing.* Cullompton

Real Decreto 436/2002, de 10 de mayo, por el que se establece la estructura orgánica del Centro Nacional de Inteligencia. BOE 2002 (113)

Revenga, M. (2019). El control del Centro Nacional de Inteligencia: una perspectiva comparada. *Revista Española de Derecho Constitucional*, 116, 13-44.

Richards, J. (2012). Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy. *Intelligence and National Security* 27 (5), 761- 80.

Romay-Ventas, I. (2021). *Los servicios de inteligencia y la lucha antiterrorista.* Universidad Internacional de La Rioja. Recuperado de https://reunir.unir.net/handle/123456789/11529

Rueda, F. (2011). Así desnudan su intimidad los candidatos a espía. *Tiempo*, 25 de marzo de 2011.

Rueda, F. (2015). Cooperación y competencia de los servicios de inteligencia en los conflictos actuales. *Ábaco*, 2 (85),110- 117.

Ruiz, C. (2002). Servicios de inteligencia y seguridad del Estado constitucional. Tecnos.

Ruiz, C. (2005). El CESID: Historia de un intento de modernización de los Servidos de Inteligencia. *Arbor CLXXX*, 709, 121-150

Sanahuja, J.A. (2011). Seguridad, desarrollo y lucha contra la pobreza tras el 11-S: los Objetivos del Milenio y la "securitización" de la ayuda". *Documentación social*, 136, 25-42. Recuperado de https://www.researchgate.net/publication/301822142_Seguridad_desarrollo_y_l

ucha_contra_la_pobreza_tras_el_11-S_los_Objetivos_del_Milenio_y_la_securitizacion_de_la_ayuda

Sánchez, G. (2015). El ciberterrorismo: de la web 2.0 al internet profundo. *Abaco: revista de cultura y ciencias sociales,* 85, 100-108.

Sánchez, J.F. (2019). *Inteligencia y seguridad como objeto constitucional: el CNI y la comunidad de inteligencia ante los nuevos retos de la sociedad del riesgo*. Centro de Estudios Políticos e Internacionales.

Sánchez, M. (2021). Repensando el concepto de ciberterrorismo. *Bie3: Boletín IEEE,* 21, 406-420.

San Felipe, C. (2013). The fight of the Israeli Intelligence Services against the Palestinian suicidal terrorism during the Intifada of Al Aqsa (years 2001-2006). *Revista Enfoques,* XI, 103-127.

Seaboyer, A. y Giler, K. (2019). Russian Special Forces and Intelligence Information Effects.

Shoham, D. y Liebig, M. (2016) The intelligence dimension of Kautilyan statecraft and its implications for the present. *Journal of Intelligence History,* 15 (2), 119-138

Sorroza Blanco, A. (2011). La seguridad interior en la UE: diez años después del 11-S. *Elcano Newsletter*, 127. Recuperado de http://biblioteca.ribei.org/id/eprint/2120/

Thomas, G. (2006). *Mossad: la historia secreta.* Barcelona: Plaza & Janés.

Tonon, G. (2011). La utilización del método comparativo en estudios cualitativos en ciencia política y ciencias sociales: diseño y desarrollo de una tesis doctoral. *Revista Kairos,* mayo (27), 1-12. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=3702607

Ubierna, M.V. (2019). *Seguridad y terrorismo: cambios en las estrategias de seguridad de España, Francia y Reino Unido ante la emergencia del Estado Islámico.* Universidad Torcuato Di Tella. Recuperado de https://repositorio.utdt.edu/handle/20.500.13098/11233

Yuen, D. (2014). *Deciphering Sun Tzu: How to Read the Art of War*. Oxford University Press.

Zamir, M. (2019). The role of MI6 in Egypt's decision to go to war against Israel in May 1948. *Intelligence and National Security*, 34(6), 775-799.

Biblioteca
UNIVERSITAS Miguel Hernández