Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Artículo de Investigación

LA INTELIGENCIA EN EL PUNTO DE MIRA: DE LA TEORÍA CLÁSICA A UN NUEVO ENFOQUE EN LA IMPLEMENTACIÓN EN LA ERA DIGITAL

Paula Castro Castañer
Experta de seguridad en Telefónica S.A
Doctoranda en Ciencias Forenses por la Universidad de Alcalá
Máster en Ciberseguridad y Privacidad por la Universitat Oberta de Catalunya
paula.castroc@edu.uah.es
ORCID: 0009-0008-0315-8387

Recibido 14/02/2025
Aceptado 16/06/2025
Publicado 27/06/2025

Cita recomendada: Castro P. (2025). La inteligencia en el punto de mira: De la teoría clásica a un nuevo enfoque en la implementación en la era digital. *Revista Logos Guardia Civil*, 3(2), p.p. 71-100.

Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

ORCID: 0009-0008-0315-8387

DEDICATORIA

A mi tutor, Hilario, por confiar en mí y apoyarme en todos mis proyectos.

ORCID: 0009-0008-0315-8387

LA INTELIGENCIA EN EL PUNTO DE MIRA: DE LA TEORÍA CLÁSICA A UN NUEVO ENFOQUE EN LA IMPLEMENTACIÓN EN LA ERA DIGITAL

Sumario: 1. INTRODUCCIÓN. 1.1. NOTA METODOLÓGICA. 2. CONCEPTO Y EVOLUCIÓN DE LA INTELIGENCIA. 2.1. TIPOS DE INTELIGENCIA. 2.2. EVOLUCIÓN DE LOS ENFOQUES Y ESTRATEGIAS DE INTELIGENCIA. 3. EL CICLO DE INTELIGENCIA. 4. PROPUESTA DE ACTUALIZACIÓN DEL CICLO DE INTELIGENCIA EN LA ERA DIGITAL: EL MODELO IDEM. 4.1. EJEMPLO PRÁCTICO DE LA IMPLEMENTACIÓN DEL MODELO IDEM. 5. CONCLUSIONES 6. REFERENCIAS BIBLIOGRÁFICAS.

Resumen: Este artículo aborda la evolución de la inteligencia en el ámbito de la Defensa y Seguridad, desde los enfoques tradicionales hasta su adaptación a la era digital, estableciendo una propuesta que responda a algunas de las limitaciones señaladas en la literatura sobre el ciclo clásico de inteligencia. Para ello se exploran conceptos clave como la definición del concepto de inteligencia, los diferentes tipos de inteligencia e incluso el tradicional ciclo de inteligencia y sus fases. Además, se presenta una revisión de la evolución y de los diferentes enfoques que se han ido adoptando a lo largo de la historia en materia de inteligencia. Por último, se propone un modelo de inteligencia, denominado IDEM, con fases flexibles y que combine el talento del analista humano y el procesamiento automatizado de grandes volúmenes de datos para garantizar una inteligencia proactiva, adaptativa y de calidad ante las complejas amenazas cibernéticas transnacionales.

Abstract: This article addresses the evolution of intelligence in the field of Defence and Security, from traditional approaches to its adaptation in the digital age, proposing an approach that responds to some of the limitations identified in the literature regarding the classical intelligence cycle. Key concepts such as the definition of the concept of intelligence, different types of intelligence, and the traditional intelligence cycle and its phases are explored. Additionally, a review of the evolution and various approaches adopted throughout history in intelligence is presented. Finally, a proposed intelligence model called IDEM is introduced, featuring flexible phases and combining the expertise of human analysts with the automated processing of large volumes of data. This aims to ensure proactive, adaptive, and high-quality intelligence in the face of complex transnational cyber threats.

Palabras clave: Amenazas cibernéticas, ciberinteligencia, ciclo de inteligencia, modelo IDEM, enfoque en red

Keywords: Cyber intelligence, cyber intelligence cycle, cyber threats, IDEM model, network approach

ABREVIATURAS

ABI: *Activity-based Intelligence*, Inteligencia Basada en Actividades

CCN-CERT: Centro Criptológico Nacional - *Computer Emergency Response Team*

CESID: Centro Superior de Información de la Defensa

CIA: *Central Intelligence Agency,* Agencia Central de Inteligencia

CIFAS: Centro de Inteligencia de las Fuerzas Armadas

CNI: Centro Nacional de Inteligencia

COMINT: *Communications Intelligence,* Inteligencia de comunicaciones

COP*: Community Policing* o *Community-oriented policing,* Actividad policial orientada a la comunidad

CTI: *Cyber Threat Intelligence*, Ciberinteligencia de amenazas

CYBINT: *Cyber-Intelligence,* Ciberinteligencia

ELINT: *Electronic intelligence*, Inteligencia electrónica

FISINT: *Foreign instrumentation signals intelligence,* Inteligencia de señales de instrumentación extranjera

GEOINT: *Geospatial Intelligence,* Inteligencia geoespacial

HUMINT: *Human Intelligence*, Inteligencia humana

IDEM: Inteligencia Dinámica Enriquecida y Mejorada

IDS: *Intrusion Detection System*, Sistema de Detección de Intrusiones

ILP*: Intelligence-Led Policin*g, Actividad policial basada en la inteligencia

IMINT: *Imagery Intelligence*, Inteligencia de imágenes

ISR: *Intelligence Surveillance and Reconnnaissance),* Inteligencia, vigilancia y reconocimiento

JISR: *Joint Intelligence Surveillance and Reconnnaissance),* Inteligencia, vigilancia y reconocimiento conjuntos

MASINT: *Measurement and Signature Intelligence*, Inteligencia de medidas y firmas

ML: *Machine Learning,* Aprendizaje Automático

NLP: *Natural Language Processing*, Procesamiento de lenguaje natural

OSCE: *Organization for Security and Co-operation in Europe,* Organización para la Seguridad y la Cooperación en Europa

OSINT: *Open-Source Intelligence,* Inteligencia de fuentes abiertas

SCADA: *Supervisory Control and Data Acquisition,* Control de Supervisión y Adquisición de Datos

SECED: Servicio Central de Documentación

SIEM: *Security Information and Event Management*, Gestión de eventos e información de seguridad

SIGINT: *Signal Intelligence*, Inteligencia de señales

SOCMINT: *Social Media Intelligence*, Inteligencia de redes sociales

TCPED: *Tasking, Collection, Processing, Exploitation, Dissemination*, Planteamiento, recogida, tratamiento, explotación y difusión

TTPs: *Threats, Techniques and Procedures*, Tácticas, técnicas y procedimientos

ORCID: 0009-0008-0315-8387

1. INTRODUCCIÓN

En un mundo en el que la Inteligencia Artificial parece acaparar gran parte de la atención y preocupación pública, ¿en qué lugar queda relegada la inteligencia en todas sus otras vertientes? La omnipresencia de la Inteligencia Artificial en los debates contemporáneos a menudo eclipsa la importancia de otros tipos de inteligencia que son fundamentales para el progreso y desarrollo de la humanidad.

La inteligencia humana, en sus múltiples manifestaciones, sigue siendo un pilar insustituible para la prosperidad de la sociedad, más aún en los contextos complejos y cambiantes de esta Era Digital. Una de esas manifestaciones es la inteligencia competitiva que permite obtener recomendaciones accionables a través del procesamiento de información sobre el entorno externo en busca de oportunidades o desarrollos que podrían impactar la posición competitiva de una empresa o país (Lee, 2023). O la inteligencia prospectiva, que, a partir de información pasada y presente, así como de especulaciones futuras, intenta "dibujar" un mapa cognitivo que permita determinar distintas opciones y reducir el nivel de incertidumbre que acompaña a toda decisión (Montero Gómez, 2006).

Es cierto que el crecimiento exponencial de la digitalización, la exposición y la globalización impulsa el origen y la evolución de nuevas formas de inteligencia en respuesta a las nuevas tecnologías y métodos de recopilación de datos, propiciando el nacimiento de inteligencias como la inteligencia de fuentes abiertas (OSINT) o la inteligencia geoespacial (GEOINT), entre otras. Estas disciplinas aprovechan la ingente cantidad de información disponible para proporcionar una visión comprensiva, integrada y detallada de diversos fenómenos. No obstante, la inteligencia no debe limitarse a la recopilación y análisis de datos, sino que también debe integrar consideraciones éticas y evaluar las posibles consecuencias a largo plazo de las decisiones.

En la actualidad la información y la tecnología son vitales para casi todos los aspectos de la vida, por ello la inteligencia desempeña un papel crucial especialmente en el ámbito de la ciberseguridad, ya que la habilidad para anticipar, identificar y mitigar amenazas es esencial para preservar la integridad, confidencialidad y disponibilidad de los sistemas.

Sin embargo, cabe preguntarse: ¿es esta capacidad una realidad en los organismos gubernamentales y privados actuales? ¿Es la inteligencia efectiva en anticipar y mitigar los riesgos crecientes en el ciberespacio? ¿Está el ciclo de inteligencia actualizado para satisfacer las demandas de la Era Digital? Este trabajo se propone realizar un análisis teórico para abordar estas cuestiones y evaluar la efectividad de la inteligencia en el contexto actual.

1.1. NOTA METODOLÓGICA

Para el desarrollo del presente trabajo se ha llevado a cabo una revisión narrativa de la literatura académica y técnica relacionada con la inteligencia en los ámbitos de la defensa y la seguridad, así como con su adaptación al entorno digital. Esta revisión ha servido como base para contextualizar la evolución del concepto, analizar críticamente el ciclo clásico de inteligencia y fundamentar la propuesta del modelo IDEM.

La búsqueda se realizó en bases de datos académicas como Scopus, Google Scholar y Dialnet, además de fuentes institucionales nacionales e internacionales. Se utilizaron

palabras clave en español e inglés tales como "ciclo de inteligencia", "cyber intelligence", "cyber threat intelligence" o "amenazas cibernéticas". Se priorizaron publicaciones recientes (2000-2024) que ofrecieran enfoques teóricos, modelos metodológicos o análisis críticos del proceso de inteligencia. En ocasiones, debido a la falta de bibliografía en fuentes abiertas se consultaron páginas web con renombre o escritas por técnicos especialistas sobre la materia.

Se excluyeron documentos sin respaldo académico o institucional, así como textos que no abordaban específicamente la dimensión estructural o de los procesos de la inteligencia. La literatura seleccionada fue organizada en torno a cinco ejes temáticos: (1) definición del concepto de inteligencia, (2) clasificación de los tipos de inteligencia, (3) evolución histórica y organizativa de los servicios de inteligencia, (4) revisión crítica del ciclo tradicional y (5) propuestas contemporáneas para su adaptación a la era digital.

Este enfoque metodológico ha permitido detectar vacíos teóricos relevantes y servir de base para la elaboración de un modelo actualizado que integre tanto la dimensión humana como las capacidades tecnológicas de la inteligencia en la actualidad.

2. CONCEPTO Y EVOLUCIÓN DE LA INTELIGENCIA

El término inteligencia es un concepto abstracto y complejo de acotar debido a la multitud de enfoques bajo los que puede ser estudiado. Esta dificultad no solo responde a la diversidad de áreas que lo analizan, sino también a los desafíos dentro de un mismo contexto para establecer una única definición.

En el ámbito de la Defensa y Seguridad la mayoría de los autores vinculan el nacimiento de la inteligencia a la aparición de los Estados y las relaciones interestatales. Sin embargo, no existe consenso respecto a su definición se refiere, debido en gran medida a la diferencia de enfoques que adoptan en la práctica los distintos países (Andric & Terzic, 2023). Esta disparidad dificulta tanto el progreso teórico de su estudio como la comprensión profunda de las diversas dimensiones y factores que inciden en su práctica (Payá-Santos, 2023).

En este contexto, una de las primeras clasificaciones fundamentales, la trinidad, fue establecida por Sherman Kent, definiendo tres realidades para este concepto: inteligencia como organización, como proceso y como resultado (Díaz Fernández, 2013).

- **Inteligencia como organización:** hace referencia a los servicios de inteligencia principalmente bajo el amparo de la administración pública como en el caso del Centro Nacional de Inteligencia (CNI) y el Centro de Inteligencia de las Fuerzas Armadas (CIFAS) en España. Estas instituciones tienen entre sus funciones obtener, evaluar, interpretar y difundir inteligencia para proteger y promover los intereses de España, tanto dentro como fuera del país; prevenir, detectar y neutralizar amenazas contra la constitución, los derechos y libertades, la soberanía, la seguridad del Estado, la estabilidad institucional y el bienestar de la población; promover la cooperación con servicios de inteligencia extranjeros y organismos internacionales; interpretar el tráfico de señales estratégicas; coordinar el uso de medios de cifra; garantizar la seguridad de la información clasificada; además de proteger sus propias instalaciones, información y recursos (Jefatura del Estado, 2002).

- **Inteligencia como proceso**: comprende todas las actividades, generalmente englobadas en el denominado ciclo de inteligencia (tratado con mayor profundidad en apartados posteriores), necesarias para cumplir con las demandas de los líderes y que interpretan un entorno, contexto o problema. Estas actividades se consideran un proceso cíclico continuo y van desde la recopilación de información de diversas fuentes, continuando con su posterior análisis y procesamiento, hasta la difusión de los datos de interés a los usuarios finales (Chainey & Chapman, 2013).
- **Inteligencia como producto:** alude al resultado y/o al conocimiento obtenido, en cualquier formato, tras realizar el ciclo de inteligencia. Este producto debe influenciar en la toma de decisiones y estas deben impactar en el contexto interpretado (Chainey & Chapman, 2013).

Recientemente, también se ha propuesto una cuarta dimensión: la **inteligencia como cultura,** definida por Navarro como "el conjunto de iniciativas y recursos que promueven la conciencia de su necesidad y aportan comprensión cívica sobre su realidad" (Payá-Santos, 2023).

Independientemente de la interpretación adoptada, la inteligencia tiene el objetivo de reducir la incertidumbre intrínseca a la condición humana y a la complejidad del mundo contemporáneo en la toma de decisiones para prevenir y evitar cualquier peligro o amenaza (Jordán, 2015).

Para conseguir este cometido, la inteligencia se nutre de conocimientos teóricos relacionados con la política, la economía, las relaciones internacionales, la seguridad, la sociología, la tecnología, la psicología, etc. De ahí que sea imprescindible presentar equipos de expertos de gran calidad en las diferentes materias para abordar los problemas desde múltiples perspectivas y encontrar soluciones más efectivas y con un enfoque trasversal.

El reciente aspecto multidisciplinar de la inteligencia es consecuencia de la ampliación del concepto de seguridad y la creciente complejidad del contexto social donde cada vez son más comunes las amenazas asimétricas y la ciberguerra.

En contraste, una de las cualidades más antigua de la inteligencia es el carácter secreto de sus actividades e información obtenida. No obstante, el crecimiento del uso de fuentes abiertas (OSINT) está cambiando está perspectiva. Además, la globalización y la expansión del uso de Internet también afectan a los conflictos, los cuales cada vez son más transnacionales y requieren la cooperación internacional de los servicios de inteligencia. Aun así, la protección de las fuentes, especialmente las humanas (HUMINT) sigue siendo un principio fundamental, al igual que la necesidad de preservar la discreción en el manejo de la información para evitar contramedidas, desinformación o vulneración de operaciones sensibles.

En definitiva, se podría establecer que la inteligencia engloba el proceso, el producto y la institución que lleva a cabo las diligencias de recopilación, evaluación y procesamiento de información (Knight, 2024) como instrumento de toma de decisiones, con el fin de identificar, advertir y prevenir riesgos y amenazas, reduciendo la incertidumbre (Francisco & Barrilao, 2019). Para lograrlo, estas tareas deben realizarse

de manera intencionada, oportuna, planificada, "secreta" y organizada (Andric & Terzic, 2023).

2.1. TIPOS DE INTELIGENCIA

Existen diversas clasificaciones de la inteligencia, pero una de las más comunes es según el medio en el que se encuentra la información, estableciendo los siguientes tipos (Kamiński, 2019):

- **SIGINT** (*Signal Intelligence*): se obtiene de las interceptaciones de señales independientemente de cómo estas se transmitan. Hay tres subcategorías: la inteligencia de comunicaciones (COMINT), la inteligencia electrónica (ELINT) y la inteligencia de señales de instrumentación extranjera (FISINT). Resulta especialmente relevante en el monitoreo de amenazas digitales y conflictos híbridos.
- **MASINT** *(Measurement and Signature Intelligence)*: basada en la medida de atributos físicos, como emisiones electromagnéticas, propiedades químicas o características acústicas. Se emplea en operaciones militares avanzadas y detección de armas, con el propósito de caracterizar, localizar e identificar a los objetivos.
- **HUMINT** (*Human Intelligence)*: es el método de recopilación de información más antiguo, proveniente de fuentes humanas, ya sea mediante entrevistas, observación directa, infiltración o colaboración de actores locales. Es fundamental en contextos donde las tecnologías no pueden acceder.
- **GEOINT** *(Geospatial Intelligence)* e **IMINT** *(Imagery Intelligence):* inteligencia geoespacial y de imágenes. La primera combina mapas, datos geográficos e información de sensores remotos, mientras que la segunda se centra en el análisis visual de imágenes satelitales, aéreas o de drones.
- **OSINT** *(Open-Source Intelligence)*: inteligencia derivada de la información de dominio público en formato físico, analógico o digital en los diferentes medios de comunicación, como radio, televisión, periódicos, revistas, Internet, bases de datos comerciales, vídeos, gráficos, dibujos, redes sociales, etc. abiertas o informes públicos. Su volumen, accesibilidad y utilidad han aumentado exponencialmente con Internet (Stewart Bertram, 2015).
- **SOCMINT** *(Social Media Intelligence*): en ocasiones, también se menciona como subcategoría de OSINT, centrada en redes sociales. Se emplea para monitorear tendencias, detectar amenazas emergentes, analizar percepciones y rastrear actores específicos (Mahood, 2015).

Sin embargo, otra tipificación muy común es según su finalidad: estratégica, táctica y operacional (Gruszczak, 2018).

- **La inteligencia estratégica:** se enfoca en identificar riesgos, amenazas y oportunidades para apoyar la definición de objetivos y la toma de decisiones, considerando el entorno, actores relevantes, y posibles evoluciones.
- **La inteligencia táctica**: se centra en la planificación y ejecución de operaciones específicas que permitan alcanzar un objetivo de alcance limitado, derivado de los grandes objetivos de la inteligencia estratégica.

- **La inteligencia operativa**: también conocida como inteligencia operacional en el ámbito militar, tiene como propósito permitir la organización y ejecución de actividades para cumplir una misión específica (Jiménez Villalonga, 2018).

La coexistencia y complementariedad entre estas categorías permite construir una inteligencia integral, adaptada a distintos niveles de decisión.

2.2. EVOLUCIÓN DE LOS ENFOQUES Y ESTRATEGIAS DE INTELIGENCIA

Numerosos autores sostienen que la inteligencia es tan antigua como la historia de la Humanidad, dado que ocultar información confidencial y descubrir la de los adversarios ha sido siempre una herramienta para alcanzar y mantener el poder. Así lo evidencian civilizaciones como la antigua China con la sabiduría milenaria del maestro Sun Tzu (Navarro Bonilla, 2005) o la Grecia clásica con los procedimientos de transmisión de información secreta de Eneas el Táctico (Vela Tejada, 1993).

En sus orígenes, la inteligencia fue una herramienta al servicio del poder político, con un enfoque eminentemente militar: conocer la fuerza, ubicación y capacidades del enemigo para facilitar la toma de decisiones del líder. Sin embargo, a medida que las sociedades se complejizaban, también lo hicieron sus amenazas, lo que llevó a expandir progresivamente la inteligencia hacia aspectos sociales, económicos o políticos. De tal forma que las actividades de inteligencia cobran un papel crucial con el nacimiento de los Estados y las relaciones entre ellos, con la finalidad de defender y proteger los intereses nacionales (Andric & Terzic, 2023).

No obstante, no fue hasta mediados del siglo XX, especialmente tras las dos guerras mundiales y la Guerra Fría que las potencias globales comenzaron a organizar formalmente sus servicios de inteligencia (Estados Unidos con la CIA, Reino Unido con el MI6 e Israel con el Mossad).

España, aunque con menor protagonismo internacional en este ámbito, también presenta el primer intento de establecer un servicio de inteligencia alrededor de esa época. En 1972 se creó el Servicio Central de Documentación (SECED) y en 1977 el Centro Superior de Información de la Defensa (CESID), pero no fue hasta 2002 que se fundó el actual CNI (Centro Nacional de Inteligencia, 2023).

A partir de ese punto, la revolución tecnológica y la explosión del volumen de información disponible marcaron un cambio radical: la inteligencia dejó de ser un ámbito cerrado y centralizado exclusivamente en el Estado para convertirse en una actividad transversal, dinámica y con implicaciones más allá del plano político-militar. Aunque la esencia de la inteligencia se mantiene, los métodos, los tiempos y los objetivos han experimentado transformaciones profundas. El acceso masivo a datos a través de fuentes abiertas, la aceleración de los flujos informativos y la globalización de las amenazas redujeron el ciclo de vida de la información y pusieron en entredicho el papel central que antes ocupaba el secreto (Payá-Santos, 2023).

A este nuevo contexto se le sumaron los atentados del 11-S que marcaron un punto de inflexión evidenciando la necesidad de identificar y prevenir amenazas asimétricas y transnacionales, desdibujando la clásica distinción entre inteligencia interna y externa, y

empujando a las instituciones policiales a adoptar modelos más analíticos, preventivos y colaborativos (Knight, 2024).

Con la progresiva extensión de la inteligencia hacia otros ámbitos estratégicos, como el policial, que históricamente había funcionado con una lógica reactiva, las funciones policiales comenzaron a evolucionar de forma significativa Su enfoque clásico, centrado en la respuesta a delitos ya consumados o en la atención a solicitudes de servicio, fue cuestionado a medida que los cambios sociales y la creciente complejidad del crimen exigían nuevas formas de intervención (Organización para la Seguridad y la Cooperación en Europa, 2017). A partir de entonces, diversas corrientes filosóficas influyeron en la labor policial como (Gkougkoudis et al., 2022):

- ***Community Policing* o *Community-oriented policing* (COP):** prioriza la cooperación entre ciudadanos y las fuerzas y cuerpos del estado, fomentando la confianza y la prevención (Carter & Fox, 2019).
- ***Problem Solving Policing***: orientada a la identificación y análisis de los problemas subyacentes al delito desde una perspectiva más amplia y trasversal buscando soluciones estructurales y sostenibles (Organización para la Seguridad y la Cooperación en Europa, 2017).
- ***Zero Tolerance Policing*:** respuesta estricta incluso ante delitos menores, basada en las ideas desarrolladas por dos criminólogos estadounidenses, James Q. Wilson y George Kelling, que en 1982 publicaron un artículo titulado "Broken Windows" (Ventanas rotas) (Grabosky, 1999).

No obstante, en las últimas décadas debido a la complejidad de las amenazas y riesgos, muchos académicos y profesionales han señalado que el enfoque holístico más acertado para combatir la globalización del crimen es el de *Intelligence-Led Policing* (ILP) traducido como actividad policial basada en la inteligencia. Este enfoque surgió en la década de 1990 en Reino Unido como una estrategia para mejorar la eficiencia fiscal de los servicios policiales, es decir optimizar la asignación de recursos, la productividad operativa y la calidad de los resultados de las actividades policiales. En sus inicios se implementaba principalmente para combatir la delincuencia grave y organizada, pero desde entonces, ha evolucionado globalmente como un modelo proactivo, impulsado por el análisis de datos y enfocado en prevenir, reducir y desarticular todo tipo de crimen. En Estados Unidos fueron los eventos del 11 de septiembre de 2001 los que finalmente impulsaron su adopción, centrando su enfoque en formas más complejas de criminalidad (Summers & Rossmo, 2019).

ILP es una filosofía proactiva para identificar y prevenir problemas criminales usando información bruta y análisis mixto (cuantitativo y cualitativo), pero no es una táctica puntual, sino un marco flexible, adaptable y sostenible basado en datos objetivos (Carter & Fox, 2019). Sin embargo, su implementación enfrenta dificultades en cuanto a la claridad terminológica y la integración de datos, además de la necesidad de garantizar el respeto a los derechos humanos en la gestión de la inteligencia.

Paralelamente, el modelo Activity-Based Intelligence (ABI) ha ampliado las capacidades de análisis, especialmente ante amenazas emergentes. Con antecedentes en la Guerra Fría, su desarrollo ha sido impulsado por la necesidad de gestionar y analizar enormes volúmenes de datos generados por tecnologías modernas, como los drones y las redes sociales, especialmente en el contexto de la lucha contra el terrorismo. Los métodos

tradicionales de análisis han demostrado ser inadecuados en este nuevo entorno, ya que los analistas pasan demasiado tiempo buscando información y vigilando objetivos conocidos, lo que limita su capacidad para descubrir lo desconocido. ABI mejora este proceso al permitir una correlación en tiempo real de datos provenientes de diversas fuentes, superando las limitaciones de los métodos tradicionales de inteligencia, vigilancia y reconocimiento (ISR, concepto que se explicará más adelante) (Atwood, 2015).

Otro enfoque relevante es el modelo 3i propuesto por Ratcliffe en 2006 basado en tres pilares fundamentales: "interpretar", "influenciar" e "impactar" el entorno criminal. Los analistas deben interpretar activamente el entorno, influir en los decisores quienes, a su vez, utilizan esa inteligencia para diseñar estrategias que afecten el entorno criminal (Budhram, 2015). En 2016 añadió una i más, la de intención, como se puede observar en la Figura 1, destacando la necesidad de claridad y comprensión de los objetivos marcados (Organización para la Seguridad y la Cooperación en Europa, 2017).

Figura 1

El modelo 4-i de Ratcliffe: intención, interpretación, influencia e impacto

Nota: Adaptado de *Guía de la OSCE sobre actividad policial basada en la inteligencia* (p. 24), por OSCE, 2017, OSCE

En suma, la inteligencia ha pasado de ser una actividad altamente secreta y centralizada, a un proceso transversal, interdisciplinar, distribuido y con fuerte apoyo tecnológico. Esta evolución justifica la necesidad de nuevos modelos como IDEM, que integren el análisis humano con el procesamiento automatizado para afrontar amenazas modernas, especialmente en el ciberespacio. Además, esta trayectoria permite observar una creciente convergencia entre las lógicas de seguridad, defensa y tecnología, situando a la inteligencia como un componente clave de la soberanía digital y la resiliencia institucional.

3. EL CICLO DE INTELIGENCIA

Aunque frecuentemente se atribuye a Sherman Kent la formulación científica del método de inteligencia, investigaciones posteriores han demostrado que una metodología rigurosa y un conjunto completo de operaciones (lo que más tarde se denominó ciclo de inteligencia) ya estaban delineados, por ejemplo, durante la Guerra Civil Española (Navarro Bonilla, 2004).

El ciclo de inteligencia aglutina todas las actividades que permiten la transformación de información en bruto en inteligencia y como su nombre indica es de naturaleza cíclica. El ciclo de inteligencia clásico tiene cuatro fases, pero en algunos países se añaden fases diferentes o subfases diferenciadas. Por ejemplo, en España el CCN-CERT establece seis fases para el ciclo de inteligencia: dirección y planificación; recolección; transformación; análisis y producción; difusión y, por último, evaluación (Centro Criptológico Nacional, 2015).

- En la primera fase, denominada **dirección y planificación** se establecen el qué y el cómo, es decir, los requisitos del producto de inteligencia que se quiere obtener y las acciones que se deberán llevar a cabo para obtenerlo. Debe quedar claro el tema de estudio, el alcance, los objetivos, el plazo de entrega y el tipo de informe para que el trabajo en el resto de las fases sea eficiente y se obtengan resultados de mayor calidad y en consonancia con las normas jurídicas nacionales e internacionales (Organización para la Seguridad y la Cooperación en Europa, 2017).
- En la siguiente etapa, **recolección,** se recopilan los datos en bruto, por ejemplo, de las fuentes que se han mencionado anteriormente (SIGINT, MASINT, HUMINT, GEOINT, IMINT, OSINT). Este proceso es complejo, ya que los analistas deben establecer el equilibrio exacto entre recolectar todos los datos necesarios y suficientes sin caer en la sobrecarga de información redundante. Para ello deben conocer la existencia, pertinencia, accesibilidad y fiabilidad de las fuentes seleccionadas, así como las limitaciones legales y los requisitos de autorización (Organización para la Seguridad y la Cooperación en Europa, 2017). Además, la validez y la exactitud de la información deberán ser evaluadas antes de proseguir con el resto de los pasos del ciclo de inteligencia.
- En la fase de **transformación** se convierten los datos en bruto recabados en la anterior etapa en conjuntos estructurados como bases de datos, referencias bibliográficas, etc., transformando la información en aquellos formatos necesarios para continuar con el ciclo y obtener inteligencia. Esta etapa implica catalogar, priorizar y referenciar la información recogida.
- La cuarta fase, de **análisis y producción**, está compuesta por las actividades mediante las que se integra, evalúa, analiza y prepara la información transformada de cara a obtener el producto final. Dentro de esta etapa se pueden establecer dos subfases: en la primera se deben integrar los datos obtenidos de diferentes fuentes para establecer hipótesis e identificar un patrón de inteligencia; la segunda implicaría interpretar los datos, es decir, ir más allá de la información obtenida, refutando o respaldando las hipótesis preestablecidas (Organización para la Seguridad y la Cooperación en Europa, 2017). Generalmente en esta fase se obtiene lo que se denomina *actionable intelligence,* producto de inteligencia que satisface los requisitos definidos en la fase de dirección y planificación y, por tanto, las necesidades del consumidor. Este producto a su vez puede ser de muchos tipos, como un análisis de tendencias, una evaluación a largo plazo, una inteligencia actual, estimativa o de avisos, etc. (Centro Criptológico Nacional, 2015).
- En la etapa de **difusión** se entrega el producto final al consumidor que lo ha solicitado y en caso de ser necesario, y jurídicamente admisible, también se compartirá con otros actores interesados.
- La última fase corresponde a la **evaluación** que permite retroalimentar continuamente todas las fases anteriores del ciclo de inteligencia con los

> resultados obtenidos, permitiendo ajustar y refinar tanto las actividades individuales como el ciclo en su conjunto. Esto resulta especialmente útil para satisfacer de manera óptima las necesidades cambiantes de inteligencia.

Sin embargo, muchos expertos cuestionan este modelo tradicional de inteligencia y una de las críticas manifestadas es la excesiva simplificación de este modelo en comparación con la gran complejidad que realmente presenta el proceso de obtención de inteligencia. Robert Clark señala que este término "se ha convertido en un concepto teológico: nadie cuestiona su validez", a pesar de no establecer los pasos precisos a seguir (Phythian et al., 2013).

Además, Arthur Hulnick señala que la noción de que los clientes de inteligencia orientan a los productores al inicio del ciclo es incorrecta, ya que los clientes a menudo esperan ser alertados por el sistema de inteligencia, por lo que el proceso de recopilación mayoritariamente está impulsado por la necesidad de llenar lagunas en los datos y no por las orientaciones políticas (Pothoven et al., 2023).

Por otro lado, no en todos los casos se acude a los órganos de obtención de datos, muchas veces se consultan directamente las bases de datos existentes y alimentadas durante años para preparar un informe. O puede que sí se soliciten nuevos datos en bruto a los equipos que los recolectan, pero no se suele plantear una nueva demanda de inteligencia a nivel de cliente (Jordán, 2011).

En cuanto a la fase de análisis, no se crítica en sí su definición dentro del ciclo de inteligencia, si no que se manifiesta que es la etapa en la que más errores se cometen, no por falta de información, sino más bien por lo contrario, por sobrecarga de datos que inducen a que informaciones relevantes sean ignoradas o inadecuadamente interpretadas por los analistas (Jordán, 2016). Los analistas han de ser conscientes de sus propios procesos mentales y errores potenciales, evitando caer en simplificaciones cognitivas involuntarias y por supuesto en sesgos. Además, en algunos casos, como en situaciones de crisis, llegan los datos directamente en bruto, sin pasar por esta fase.

En referencia a la fase de difusión, en ocasiones tampoco se pasa por ella, ya que no todos los análisis elaborados llegan a los consumidores. Muchos no son leídos por los destinatarios y se guardan directamente en la base interna. Otras muchas veces los clientes ya tienen las decisiones tomadas e ignoran la inteligencia que no las respalda.

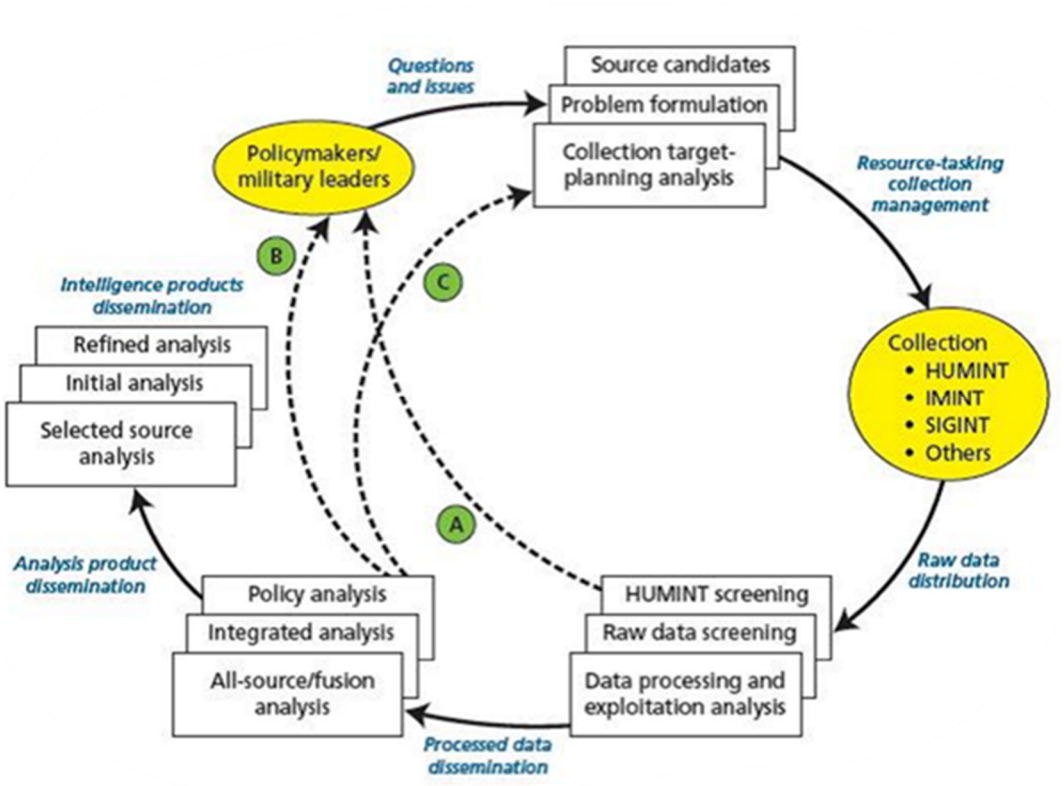
También, en relación con el ciclo de inteligencia de manera general, se critica su definición como una secuencia de fases que finalmente se dispone de manera circular, cuando es un proceso más dinámico, donde todas las fases se retroalimentan entre sí, pudiendo avanzar y retroceder en cualquier dirección dentro del ciclo. Y también se señalan los problemas organizativos, de mando y flujo de información que propician falta de flexibilidad en la acción y comunicación, ralentizando los procesos de toma de decisiones (Organización para la Seguridad y la Cooperación en Europa, 2017).

Referentes como Peter Gill y Mark Phythian argumentan que el concepto del ciclo de inteligencia ha quedado obsoleto debido a los avances tecnológicos, la revolución de la información y los cambios en las amenazas y objetivos. Por lo que proponen reemplazarlo con una "red de inteligencia" que refleja mejor las complejas interacciones entre selección de objetivos, recogida y análisis, y que destaca los factores contextuales

que influyen en el proceso y pueden ser afectados por sus resultados (Pothoven et al., 2023).

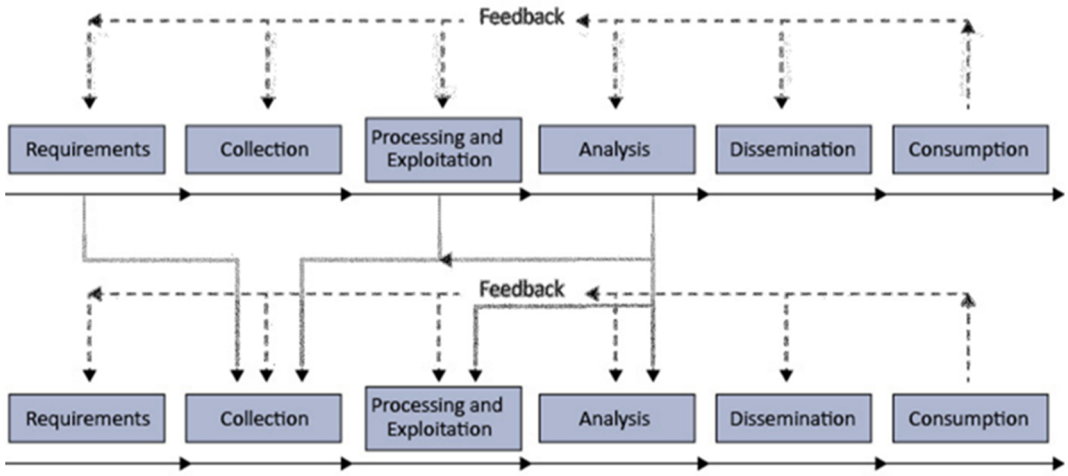
Por otra parte, diversos autores han intentado capturar la complejidad del ciclo de inteligencia en esquemas alternativos al tradicional. Como se puede observar en la Figura 2, Treverton y Gabbard proponen un enfoque más realista que incluye atajos entre fases, mostrando que hay pasos que en ocasiones no se realizan, como por ejemplo que la información no analizada puede llegar directamente a los decisores. Mark Lowenthal presenta un ciclo compuesto por retroalimentaciones constantes, donde nuevas necesidades y ambigüedades reactivan el proceso, haciéndolo más dinámico y con numerosos niveles, como se puede ver en la Figura 3. Y Robert M. Clark introduce el concepto *Target-Centric Intelligence*, un modelo colaborativo y orientado al objetivo, donde todos los participantes construyen juntos una imagen compartida del asunto de interés de la inteligencia, representado en la Figura 4 (Jordán, 2016).

Figura 2
Enfoque de Treverton y Gabbard



Nota: Tomado de *Una revisión del ciclo de Inteligencia* (p. 4) por J. Jordán, 2016, *Análisis GESI (Grupo de Estudios En Seguridad Internacional),* 2.

Figura 3
Proceso multi-estrato Mark Lowenthal



Nota: Tomado de *Una revisión del ciclo de Inteligencia* (p. 5) por J. Jordán, 2016, *Análisis GESI (Grupo de Estudios En Seguridad Internacional),* 2.

Figura 4
Target-Centric Intelligence de Robert M. Clark

Nota: Tomado de *Una revisión del ciclo de Inteligencia* (p. 6) por J. Jordán, 2016, *Análisis GESI (Grupo de Estudios En Seguridad Internacional),* 2.

Por último, también han surgido propuestas como el concepto JISR de la OTAN, (por sus siglas en inglés, Inteligencia, vigilancia y reconocimiento conjuntos en castellano). Este término hace referencia al conjunto integrado de capacidades de inteligencia y operaciones que sincroniza e integra la planificación y ejecución de todas las capacidades de recolección de información con su procesamiento, explotación y difusión. Este concepto surge de la necesidad de mejorar la compartición de información e inteligencia para prevenir crisis, amenazas terroristas, actividades criminales

transnacionales y ciberamenazas (Gruszczak, 2018). La inteligencia, vigilancia y reconocimiento (ISR) siempre han sido actividades esenciales de las operaciones militares, pero se dividían según los niveles de mando (estratégico, operativo y táctico), o según las diversas disciplinas de inteligencia, dependiendo del tipo y complejidad de las fuentes de información involucradas. En el contexto actual esta división limita el uso óptimo de los especialistas de inteligencia, agencias, fuentes y actividades. Por ello, se propone el modelo JISR donde las actividades de inteligencia, vigilancia y reconocimiento funcionan como una sola unidad, integrándose en todos los niveles y dominios (Ministry of Defence, 2023).

No obstante, el modelo JISR presenta el mismo proceso que el ISR, el cual está formado por 5 fases: planteamiento, recogida, tratamiento, explotación y difusión (TCPED por sus siglas en inglés). La principal diferencia con el ciclo de inteligencia tradicional es que este proceso no se plantea de manera lineal ni circular, sino que se ejecutan las diferentes etapas dinámicamente, de forma secuencial, simultánea o independiente, en función del resultado requerido. No obstante, en este modelo, el proceso ISR sí que suele alinearse con la fase de recolección del ciclo de inteligencia, y los resultados de esta recolección se incorporan en la etapa de procesamiento, además de apoyar el ciclo de decisión.

Sin embargo, este enfoque también enfrenta varias limitaciones. Primero, puede haber una falta de recursos suficientes para satisfacer todos los requisitos, especialmente debido a la alta demanda y baja disponibilidad de ciertas capacidades de recolección. También existen problemas técnicos como limitaciones en el poder computacional y el ancho de banda, que afectan la capacidad para procesar y difundir resultados. Los adversarios pueden interferir mediante ataques a las capacidades de ISR, camuflaje, ocultación y desinformación. Además, el acceso a ISR puede estar limitado por barreras físicas, cognitivas, virtuales, legales y políticas (Ministry of Defence, 2023).

Por ello, la inteligencia como proceso en la actualidad debería alejarse de los modelos lineales y cíclicos tradicionales para adoptar estructuras más fluidas y en red, capaces de responder de manera ágil a las amenazas emergentes y aprovechar el vasto volumen de datos disponibles (Jiménez Villalonga, 2018).

4. PROPUESTA DE ACTUALIZACIÓN DEL CICLO DE INTELIGENCIA EN LA ERA DIGITAL: EL MODELO IDEM

El ciclo clásico de inteligencia ha sido durante décadas la columna vertebral de la inteligencia como proceso. En su momento, esta representación secuencial tuvo sentido, ya que facilitaba la estandarización, la formación de analistas y la gestión de las operaciones. Sin embargo, el modelo presenta importantes limitaciones cuando se traslada a contextos actuales marcados por la complejidad, la incertidumbre y el ritmo acelerado de cambio, especialmente en dominios como el ciberespacio.

En este entorno altamente dinámico, la inteligencia ha adquirido una relevancia crítica como instrumento para comprender y anticipar amenazas, particularmente en el ámbito digital. A medida que las organizaciones expanden su presencia en el ciberespacio para maximizar su visibilidad y alcance, también aumentan su superficie de exposición a posibles ataques. Esta transformación obliga a repensar el papel de la inteligencia más

allá de su formulación clásica, adaptándola a las particularidades de un entorno descentralizado, interconectado y en constante evolución.

Sin embargo, esta adaptación no es sencilla. La proliferación de términos y enfoques refleja tanto la juventud del campo como su rápida expansión. En algunos marcos conceptuales, se utiliza el término ciberinteligencia o CYBINT como un subtipo de COMINT (Jiménez Villalonga, 2018), pero también podría considerarse como un tipo de inteligencia superior que abarca y coordina actividades de OSINT, SIGMINT, SOCMINT e incluso HUMINT (Portillo, 2019).

En el contexto europeo es más común hablar de la ciberinteligencia de amenazas (CTI por sus siglas en inglés), que hace referencia a la aplicación sistemática de inteligencia para identificar, analizar y mitigar amenazas que afectan el ciberespacio. Según Gartner (Lee, 2023), la CTI se basa en conocimientos fundamentados en evidencias, que proporcionan contexto, mecanismos, indicadores y consejos prácticos sobre amenazas emergentes o existentes.

Es por eso por lo que la CTI desempeña un papel crucial, ayudando a las organizaciones a desarrollar una estrategia de seguridad proactiva que les permita entender y anticipar las tácticas, técnicas y procedimientos (TTPs, *Threats, Techniques and Procedures)* de los adversarios. Así mismo, facilita la identificación de amenazas desde su origen y la respuesta efectiva a incidentes antes de que puedan causar daños significativos.

No obstante, a la hora de implementar investigaciones o sistemas de trabajo en este ámbito, persiste una ausencia de ciclos metodológicos específicos y ampliamente aceptados para estructurar el proceso de recolección y análisis de ciberinteligencia. En consecuencia, se tiende a recurrir al ciclo de inteligencia tradicional o a alguno de los enfoques alternativos existentes. Pero como se ha señalado, todos ellos presentan limitaciones importantes para su aplicación efectiva en entornos digitales.

El **modelo clásico** es rígido y secuencial; el **modelo propuesto por Treverton y Gabbard** permite cierta flexibilidad, pero carece de retroalimentación clara; el **modelo Target-Centric** plantea un ciclo continuo más cercano al objetivo, aunque sin una estructura realmente flexible entre fases; y el **enfoque multinivel de Lowenthal** introduce dinamismo, pero mantiene una cierta linealidad y las conexiones bidireccionales entre fases no se entienden del todo.

Tabla 1

Tabla comparativa de los diferentes modelos para representan la inteligencia como proceso

	Modelo clásico	Modelo de Treverton y Gabbard	Modelo de Mark Lowenthal	Modelo Target-Centric
Estructura	Lineal o cíclica (fases sucesivas en círculo)	Semilineal (con posibles "atajos")	Multinivel (con capas activas según necesidad)	Cíclica (centrada en el objetivo)
Inicio del proceso	Por requerimiento del consumidor	Similar al clásico, pero admite reiniciar desde fases intermedias	Desde nuevas necesidades que reactiven fases anteriores	Desde el análisis del objetivo (desde análisis anteriores o desde nuevas necesidades e informaciones)
Fases principales	Dirección y planificación, recolección, transformación, análisis y producción, difusión, evaluación	Similares a las del modelo clásico, pero sin orden estricta ni mención a la retroalimentación	Mismas que el clásico, en capas con ciclos internos y *feedback* continuo	Requisitos y *gaps*, recogida, análisis y difusión, se entrelazan en torno al objetivo
Interacción entre fases	Limitada (retroalimentación al final)	Media (lineal con atajos)	Alta (continua y simultánea)	Media (ciclos conectados por el objetivo)
Flexibilidad y adaptabilidad	Baja (modelo rígido y secuencial)	Media (cierta fluidez, pero mantiene fases definidas)	Alta (orientado a reformular continuamente el proceso)	Media: (dinamismo entorno al objetivo)
Difusión de la inteligencia	Al final del proceso	Puede ser omitida o adelantada si el producto lo requiere	Puede producirse en diferentes niveles y momentos, según el ciclo interno activado	Final del proceso, tras la fase de producción
Retroalimentación	Al final del proceso	No aparece referenciada explícitamente	En todas las fases	No aparece referenciada explícitamente

Es por ello que en este trabajo se propone el modelo de inteligencia IDEM (Inteligencia Dinámica Enriquecida y Mejorada) con un enfoque en red, no lineal y altamente adaptativo, en el que las fases del proceso de inteligencia no se suceden de manera secuencial, sino que interactúan de forma dinámica, flexible y continua, permitiendo una retroalimentación constante entre fases y equipos de trabajo.

Mientras que el modelo tradicional comienza con la **dirección y planificación,** donde se establecen los requisitos de inteligencia en función de las necesidades del decisor, el modelo IDEM propone iniciar con una fase de **identificación y priorización de amenazas** en tiempo real. Una de las críticas más reiteradas al ciclo tradicional es su escasa flexibilidad ya que una vez definidos los objetivos, el proceso tiende a seguir una trayectoria fija, lo que resulta ineficaz en el contexto actual, donde las amenazas evolucionan de forma rápida y no siempre están alineadas con las necesidades previamente establecidas. Por ello, el objetivo de esta fase debe ser detectar y priorizar amenazas emergentes de manera proactiva, sin depender exclusivamente de las directrices iniciales de los consumidores, que a menudo no llegan a tiempo o directamente no se formulan. Esta fase se convertiría en un propio proceso dinámico y continuo,

alimentado por la monitorización constante, el reconocimiento en tiempo real de patrones de amenazas emergentes y la capacidad de reorientar rápidamente los esfuerzos de inteligencia conforme surgen nuevas amenazas o cambios en las condiciones (Dahj, 2022).

La siguiente fase, la **recolección**, sigue siendo fundamental en la inteligencia como proceso, ya que sin datos e información no se puede obtener conocimiento accionable. En el modelo clásico, uno de los mayores desafíos ha sido filtrar de manera efectiva grandes volúmenes de datos para evitar tanto la saturación informativa como la pérdida de información crítica. En la Era Digital, esta tarea se ha vuelto aún más compleja debido al aumento exponencial de la cantidad de fuentes y datos disponibles, impulsado por las nuevas tecnologías, la globalización, y la corta vida útil de la información. IDEM aborda esta complejidad mediante el uso de tecnologías avanzadas como el *machine learning* (ML) y la inteligencia artificial, que permiten una recolección continua y exhaustiva automatizada. A pesar de gestionar volúmenes significativamente mayores, estas herramientas hacen posible filtrar, priorizar y enriquecer la información en tiempo real, garantizando así su relevancia y utilidad.

En esta propuesta, no tiene sentido establecer una fase específica para la **transformación** de los datos como se plantea en el modelo clásico. Gracias a tecnologías avanzadas, como el procesamiento de lenguaje natural (NLP por sus siglas en inglés*)* y herramientas de análisis de *big data*, la conversión de datos en bruto en información relevante y contextualizada puede producirse en múltiples etapas del proceso de forma simultánea. Esto permite que los datos sean procesados, estructurados y analizados en paralelo, facilitando una respuesta ágil ante nuevas informaciones o variaciones en el entorno.

Además, la separación entre la **transformación** y el **análisis** puede llevar a una falta de integración y a una pérdida de contexto durante la transición. Por esta razón, IDEM sustituye estas dos fases del modelo clásico por una única etapa de **contextualización y enriquecimiento** que pone el foco en situar los datos en su contexto, interpretar su relevancia y entender la conexión con otros eventos y patrones. De esta manera el análisis puede actualizarse y ajustarse continuamente conforme emergen nuevos datos y surgen nuevas preguntas, desarrollando una capacidad de adaptación continua. Asimismo, es esencial procesar e integrar la información obtenida de múltiples fuentes de datos ya que facilitan una interpretación más profunda y eficiente, especialmente en el contexto actual de amenazas híbridas. A diferencia del enfoque tradicional, y también de los sistemas ISR clásicos, que establece un proceso individual para cada tipo de fuente (OSINT, HUMINT, SIGINT, COMINT, etc.) (Ministry of Defence, 2023), IDEM propone un modelo interconectado y multisensor, más eficaz en la detección y análisis de fenómenos complejos, tal y como sugiere la doctrina de JISR del Departamento de Defensa de EE. UU., abordada en el apartado 2.2

En cambio, en el modelo IDEM sí se mantiene una etapa específica para la **producción** de inteligencia accionable. Mientras que, en el ciclo tradicional, el análisis y producción se centran en generar informes y recomendaciones que ayuden para la toma de decisiones, IDEM aboga por productos no solo reactivos, sino también predictivos, que permitan anticipar eventos y tendencias o evaluar impactos que faciliten el ajuste de las estrategias y decisiones en tiempo real. El énfasis aquí está en la inteligencia como apoyo a decisiones dinámicas, no como producto cerrado.

Paralelamente al desarrollo de todas estas fases, es indispensable la fase de **retroalimentación** definida en el tradicional ciclo de inteligencia, pero reinterpretándola como un proceso trasversal. Para asegurar una mejora continua y un proceso más eficiente, es crucial que se saquen puntos de mejora o debilidades a lo largo de cada una de las fases. Esto permitirá considerar estas observaciones no solo en los pasos siguientes, sino también en investigaciones futuras, en lugar de esperar hasta obtener el producto final de inteligencia, como ocurre en el modelo tradicional.

Por último, en el ciclo tradicional la **difusión** se reserva para el final del proceso, una vez producido el informe de inteligencia. IDEM rompe con esta lógica, planteando una difusión modular y progresiva, , no solo compartiendo inteligencia como tal, sino también aquellas amenazas reconocidas y clasificadas en la fase de identificación y priorización, o los datos recopilados de las diferentes fuentes disponibles o incluso aquellos datos contextualizados y enriquecidos en diferentes formatos. Evidentemente, esta difusión temprana debe gestionarse de forma cuidadosa, garantizando la protección de las fuentes para evitar contramedidas y desinformación por parte de los objetivos y proteger a las fuentes humanas (HUMINT). Sin embargo, el carácter transnacional de los delitos actuales exige la cooperación internacional de los diferentes servicios de inteligencia y, por tanto, la compartición oportuna y no tardía de información entre ellos para obtener unos resultados más eficaces.

Ahora bien, pese a las capacidades técnicas que ofrece la automatización, el papel del analista humano sigue siendo esencial en cada una de las etapas anteriormente descritas. Las herramientas automatizadas operan dentro de unos parámetros y algoritmos definidos por sus programadores, que son los verdaderamente capaces de interpretar la información en un contexto más amplio, considerando factores culturales, políticos y situacionales. Además, los modelos predictivos carecen de la flexibilidad cognitiva para manejar ambigüedades, contradicciones o excepciones y pueden fallar ante entradas erróneas, datos sesgados o situaciones no previstas.

Los analistas, por el contrario, son capaces de adaptarse, innovar y reajustar sus enfoques en respuesta a nuevos paradigmas, mientras que los modelos de inteligencia artificial necesitan una gran cantidad de datos de entrenamiento para poder desarrollar nuevas metodologías de análisis y no son capaces de aplicar enfoques creativos si surgen nuevas problemáticas. Esta capacidad de los humanos, de colaborar entre equipos, discutir interpretaciones, reestructurar estrategias en función del *feedback* recibido es esencial para la implementación exitosa de estrategias de inteligencia (Jordán, 2011).

Tabla 2
Tabla comparativa del modelo clásico y de la propuesta de modelo IDEM

	Modelo clásico	Modelo IDEM (propuesta propia)
Estructura	Lineal o cíclica (fases sucesivas en círculo)	Modular, dinámica y en red (circunferencias concéntricas e interconectadas)
Inicio del proceso	Por requerimiento del consumidor	Proactivo, sin requerimiento previo
Fases principales	Dirección y planificación, recolección, transformación, análisis y producción, difusión, evaluación	Identificación y priorización, recolección, contextualización y enriquecimiento, producción de inteligencia, retroalimentación y difusión
Interacción entre fases	Limitada (retroalimentación al final)	Alta: fases interactivas y bidireccionales
Flexibilidad y adaptabilidad	Baja (modelo rígido y secuencial)	Muy alta (fases simultaneas y reajustables)
Difusión de la inteligencia	Al final del proceso	Transversal y continua desde fases tempranas del proceso
Retroalimentación	Al final del proceso	Constante: en todas las fases
Tecnología aplicada	No contemplada explícitamente	Integración de tecnologías avanzadas (IA, ML, NLP, *big data*)
Participación humana	Central, pero jerárquico	Combinación sinérgica entre analista humano y herramientas automatizadas
Aplicabilidad en entornos digitales	Limitada	Alta (orientado a amenazas cibernéticas y escenarios complejos)

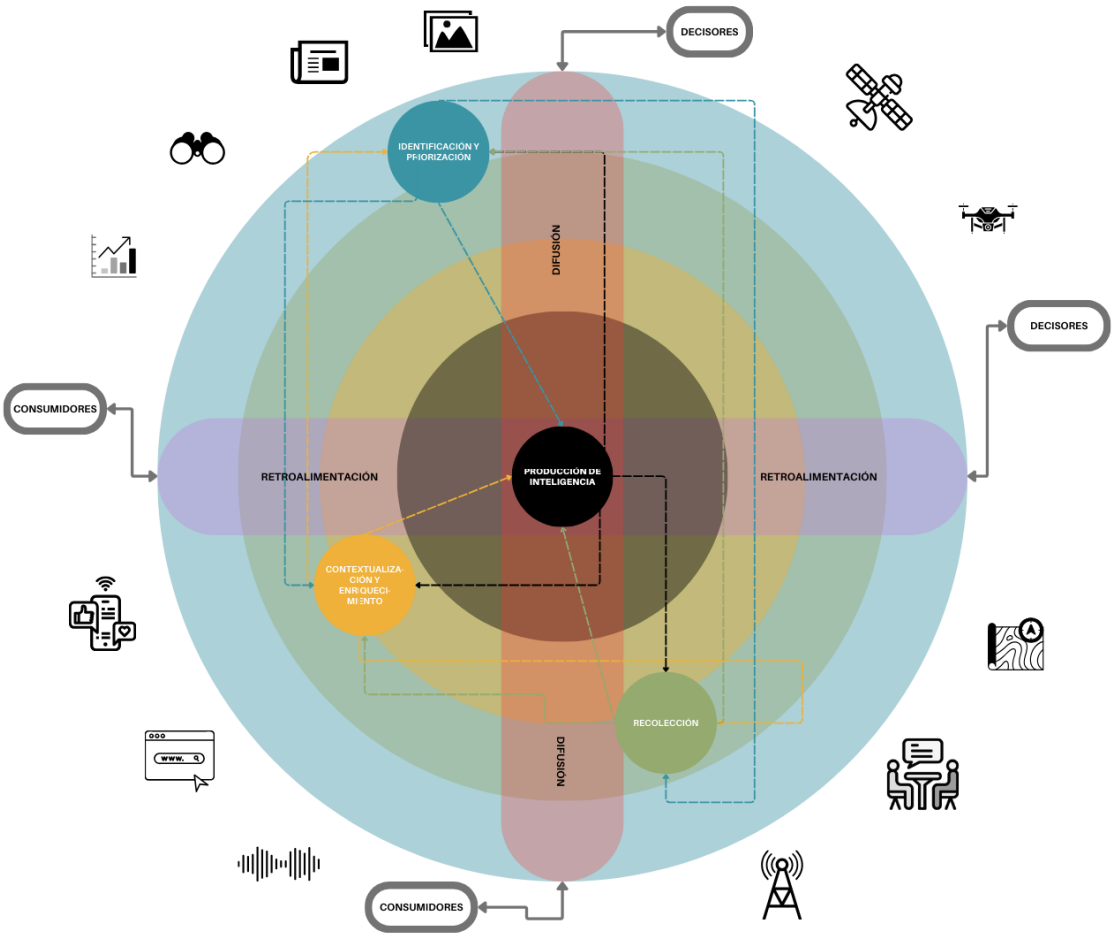
A continuación, se presenta un esquema representativo del modelo IDEM, en el que las diferentes fases se disponen como circunferencias concéntricas. Esta disposición refleja, por un lado, la proximidad creciente al producto final de inteligencia a medida que se avanza hacia el centro, y por otro, y la naturaleza constante de todas las etapas, ya que las fases más internas están contenidas dentro de las exteriores. No obstante, el modelo no establece un recorrido lineal, no es necesario transitar por todas las etapas para poder alcanzar el centro. Este carácter dinámico se representa mediante flechas que indican los posibles flujos de entrada y salida entre las diferentes fases, permitiendo transiciones directas y bidireccionales según las necesidades del contexto.

Perpendicular a estas circunferencias y perpendiculares también entre sí, se integran dos elementos clave representados como rectángulos transversales. El primero representa la fase de retroalimentación, trasversal a todas las fases y oportuna para la mejora continua de todo el ciclo. El segundo simboliza la fase de difusión también colateral a todas las etapas y esencial para obtener productos más completos y resultados más eficaces.

En la parte externa del esquema se sitúan los consumidores y decisores. Su número y relevancia dependerá tanto de las necesidades de inteligencia que se precisen como del impacto esperado de los análisis realizados. Estas figuras se representan mediante flechas bidireccionales, que indican su doble función, establecer el objetivo y los criterios de inteligencia, al mismo tiempo que recibir retroalimentación o productos de inteligencia que les faciliten la toma de decisiones.

Asimismo, se incorporan iconos de diferentes fuentes de información, apoyando así la estrategia de recolectar, contextualizar y enriquecer los datos obtenidos por diferentes fuentes para realizar un proceso de inteligencia más completo, trasversal y eficaz.

Figura 5
Modelo de inteligencia IDEM



Nota: Elaboración propia, Paula Castro Castañer, 2024

La combinación de la adaptabilidad, experiencia, juicio crítico y talento humano con la capacidad de las máquinas para procesar grandes volúmenes de datos crea una sinergia que garantiza una toma de decisiones más efectiva, multidisciplinar, informada y flexible, asegurando una mayor calidad y relevancia de la inteligencia generada.

4.1. EJEMPLO PRÁCTICO DE LA IMPLEMENTACIÓN DEL MODELO IDEM

Un ejemplo práctico que ilustraría la utilidad de aplicar este modelo de inteligencia es en caso de que un proveedor de energía nacional detectará una anomalía en sus sistemas de control SCADA. En esta situación, no existe aún un incidente confirmado ni una solicitud explícita por parte de los decisores (ya que probablemente no tienen conocimiento todavía de esta situación), lo que implica que la activación del proceso de inteligencia se origina de manera proactiva y autónoma, a partir de señales identificadas en el entorno operacional. No obstante, el equipo interno de inteligencia activa el modelo IDEM para anticipar si se trata de una amenaza real o una falsa alarma.

Desde el IDS llega una alerta automática de tráfico anómalo hacia servidores de respaldo, lo cual da inicio a la fase de identificación y priorización. Esta alerta, aunque preliminar, es suficiente para que el equipo interno de inteligencia clasifique la amenaza como prioritaria, considerando el potencial impacto que un compromiso de esta naturaleza podría representar para una infraestructura crítica del país. Como consecuencia, se decide despriorizar temporalmente investigaciones abiertas sobre campañas de hacktivismo y vigilancia geopolítica de bajo impacto, así como otras tareas de monitorización rutinaria en foros y canales oscuros. Esta reorientación permite concentrar esfuerzos humanos y tecnológicos en una única hipótesis de trabajo: una posible intrusión avanzada dirigida.

La recolección se activa simultáneamente desde múltiples fuentes internas (logs, SIEM, registros de autenticación) y externas (feeds de ciberinteligencia, bases de datos de indicadores de compromiso, alertas de entidades colaborados o proveedores de inteligencia). Durante esta etapa, al surgir indicios que sugieren motivaciones económicas detrás del posible ataque, como, por ejemplo, la extracción de datos de mercado en lugar de información operativa, el proceso regresa brevemente a la fase de identificación con el propósito de reformular la hipótesis inicial. Este retorno permite que el análisis se oriente ahora hacia la posibilidad de un caso de espionaje económico industrial en desarrollo, modificando consecuentemente el enfoque del resto de las actividades del proceso de inteligencia.

En la fase de contextualización y enriquecimiento se procede a integrar los datos recopilados con información histórica de incidentes previos y con el análisis de tendencias en el sector energético. Se emplean técnicas de análisis de comportamiento, atribución de TTPs y minería de datos históricos. Estas metodologías facilitan la detección de patrones y coincidencias con campañas anteriormente atribuidas a actores estatales o grupos intermediarios, es decir, entidades que operan como delegados o agentes indirectos de otros actores con intereses geopolíticos o económicos.

La producción de inteligencia se distribuye en distintos formatos adaptados a las necesidades específicas de cada tipo de destinatario. Esto incluiría alertas tácticas dirigidas a los equipos de ciberseguridad responsables de la respuesta inmediata, informes estratégicos orientados a los altos responsables del sistema energético, y recomendaciones preventivas destinadas a otros operadores del sector para fortalecer su postura de defensa.

Es importante destacar que esta producción y difusión de inteligencia se realiza de manera continua y en paralelo con el desarrollo de la investigación, sin esperar a la obtención de una "conclusión definitiva". Este enfoque permite una respuesta temprana y dinámica frente a amenazas emergentes puesto que otros actores relevantes del sector energético al recibir estos productos podrían reportar incidentes similares en sus redes, lo que permitiría reabrir ciclos de análisis y reajustar la priorización de amenazas a escala nacional.

Además de la retroalimentación externa por parte de actores relevantes que permite ajustar hipótesis y prioridades a partir de señales del entorno, también se incorpora una fase de retroalimentación continua interna orientada a la mejora del propio proceso de inteligencia. Por ejemplo, durante la fase de contextualización, el equipo de inteligencia detecta que ciertos indicadores clave de compromiso (IoCs) no fueron

priorizados inicialmente por los sistemas automatizados de alerta. Esta observación se documenta y se canaliza hacia el equipo responsable de ajustar los umbrales de sensibilidad del SIEM, lo que permite refinar los criterios de detección para futuros casos similares. Finalmente, al concluir el ciclo, se realiza una revisión interna del desempeño del modelo IDEM en este caso específico, evaluando métricas como el tiempo de respuesta, la precisión de las hipótesis iniciales y la utilidad de los productos generados. Esta evaluación alimenta una base de conocimiento interna que permite ajustar metodologías, herramientas y flujos de trabajo, asegurando que el modelo evolucione de forma adaptativa y basada en la experiencia acumulada.

Esta dinámica de retroceso, reformulación y acción simultánea que permite el modelo IDEM sería impracticable con el modelo clásico del ciclo de inteligencia, ni en muchos de los modelos propuestos en la literatura revisada, donde los procesos son más rígidos, lineales y dependientes de la iniciativa de los decisores.

5. CONCLUSIONES

La inteligencia, entendida como organización, proceso, producto e incluso cultura, desempeña un papel clave en la gestión de la incertidumbre en entornos volátiles, interconectados y marcados por crecientes amenazas híbridas. Su carácter multidisciplinar y la diversidad de enfoques utilizados por diferentes países y disciplinas dificultan una definición única y una clasificación cerrada de sus tipos, pero también reflejan su riqueza conceptual y la necesidad de cooperación y adaptación constante.

El ciclo clásico de inteligencia, aunque valioso en su momento por aportar estructura y estandarización, presenta limitaciones significativas para enfrentar los retos contemporáneos, especialmente en el ámbito digital. La naturaleza dinámica y descentralizada del ciberespacio, así como el volumen y la velocidad de los datos, requieren modelos más flexibles y adaptativos. El modelo IDEM propuesto en este trabajo responde a esa necesidad mediante una estructura modular, no lineal y en red, donde las fases interactúan de forma simultánea y se retroalimentan constantemente.

Este nuevo enfoque reorganiza las etapas del ciclo tradicional y añade elementos clave como la identificación proactiva de amenazas, la contextualización integrada con el análisis, la difusión temprana y transversal de inteligencia, y la incorporación sistemática de retroalimentación. Además, integra tecnologías avanzadas como la inteligencia artificial o el aprendizaje automático para optimizar la gestión de grandes volúmenes de datos y mejorar la capacidad predictiva.

No obstante, la tecnología por sí sola no basta. El juicio humano, la capacidad crítica, la creatividad analítica y el conocimiento contextual siguen siendo imprescindibles. La sinergia entre analistas y sistemas automatizados garantiza una inteligencia más eficaz, precisa y útil para la toma de decisiones.

En definitiva, la inteligencia del siglo XXI debe ser ágil, multidisciplinar y colaborativa. Solo a través de enfoques híbridos, abiertos al aprendizaje y a la mejora continua, será posible anticipar y mitigar eficazmente las amenazas emergentes. El modelo IDEM es un paso en esa dirección: una propuesta adaptativa y realista para afrontar los desafíos que impone la era digital a los sistemas de inteligencia contemporáneos.

La realidad del contexto actual sigue presentando desafíos y dificultades significativas para anticipar y mitigar de manera efectiva las amenazas contemporáneas, en especial aquellas que se manifiestan en el ciberespacio, puesto que es difícil mantenerse al día y por delante de los ciberdelincuentes. Por ello, es necesario que la comunidad de inteligencia siga investigando y desarrollando estrategias que disminuyan las debilidades actuales, promoviendo la concienciación de la cultura de inteligencia, la difusión de información y la cooperación internacional.

6. REFERENCIAS BIBLIOGRÁFICAS

Andric, J., & Terzic, M. (2023). Intelligence cycle in the fight against terrorism with usage of OSINT data. Journal of Information Systems & Operations Management, 17(1). https://doi.org/10.1080/2158379X.2021.1879572

Atwood, C. P. (2015). Activity-Based Intelligence Revolutionizing Military Intelligence Analysis. Joint Force Quarterly, 77. https://ndupress.ndu.edu/Media/News/Article/581866/activity-based-intelligence-revolutionizing-military-intelligence-analysis/

Budhram, T. (2015). Intelligence-led policing: A proactive approach to combating corruption. South African Crime Quarterly, 52. https://doi.org/10.17159/2413-3108/2015/i52a30

Carter, J. G., & Fox, B. (2019). Community policing and intelligence-led policing: An examination of convergent or discriminant validity. Policing: An International Journal, 42(1), 43–58. https://doi.org/10.1108/PIJPSM-07-2018-0105

Centro Criptológico Nacional. (2015). CCN-STIC-425 Ciclo de Inteligencia y Análisis de Intrusiones.

Centro Nacional de Inteligencia. (2023). Origen de los Servicios de Inteligencia. https://www.cni.es/sobre-el-cni/nuestra-historia

Chainey, S., & Chapman, J. (2013). A problem-oriented approach to the production of strategic intelligence assessments. Policing: An International Journal of Police Strategies & Management, 36(3), 474–490. https://doi.org/10.1108/PIJPSM-02-2012-0012

Dahj, J. N. M. (2022). Mastering Cyber Intelligence. Packt Publishing Ltd.

Díaz Fernández, A. M. (2013). El papel de la inteligencia estratégica en el mundo actual. Cuadernos de Estrategia, 162, 35–66. https://dialnet.unirioja.es/servlet/articulo?codigo=4275959

Francisco, J., & Barrilao, S. (2019). Servicios de Inteligencia, secreto y garantía judicial de los derechos. Teoría y Realidad Constitucional, 309–340.

Gkougkoudis, G., Pissanidis, D., & Demertzis, K. (2022). Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police. Digital, 2, 143–163. https://doi.org/10.3390/digital2020009

Grabosky, P. N. (1999). Zero tolerance policing. Australian Institute of Criminology, 102(Trends & issues in crime and criminal justice).

Gruszczak, A. (2018). NATO's intelligence adaptation challenge. https://www.globsec.org/what-we-do/publications/natos-intelligence-adaptation-challenge

Jefatura del Estado. (2002). Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia.

Jiménez Villalonga, R. (2018, November 26). Tipos de Inteligencia. https://global-strategy.org/tipos-de-inteligencia/

Jordán, J. (2011). Introducción al análisis de inteligencia. 2340-8421, 2, Art. 2. https://www.seguridadinternacional.es/resi/index.php/revista

Jordán, J. (2015). Introducción a la Inteligencia en el ámbito de Seguridad y Defensa. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 26, Art. 26. https://www.seguridadinternacional.es/resi/index.php/revista

Jordán, J. (2016). Una revisión del ciclo de Inteligencia. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 2. https://www.seguridadinternacional.es/resi/index.php/revista

Kamiński, M. A. (2019). Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community. Security Dimensions, 32(32), 82–105. https://doi.org/10.5604/01.3001.0014.0988

Knight, T. C. (2024). Five Thousand Candles: Optimizing Information Sharing Policies for Homeland Security A dissertation. American Public University System.

Lee, M. (2023). Cyber Threat Intelligence (1st ed.). John Wiley & Sons, Inc.

Mahood, L. M. E. K. (2015). SOCMINT: following and liking social media intelligence [Canadian Forces College]. https://www.cfc.forces.gc.ca/254-eng.html

Ministry of Defence. (2023). Intelligence, Surveillance and Reconnaissance.

Montero Gómez, A. (2006). Inteligencia Prospectiva de Seguridad (24; Área: Seguridad y Defensa). https://www.realinstitutoelcano.org/publicaciones/

Navarro Bonilla, D. (2004). El Ciclo de Inteligencia y sus límites. Cuadernos Constitucionales de La Cátedra Fadrique Furió Ceriol, 48, 51–66. https://dialnet.unirioja.es/servlet/articulo?codigo=2270935

Navarro Bonilla, D. (2005). Información, espionaje e inteligencia en la monarquía hispánica (Siglos XVI-XVII). Revista de Historia Militar, Extraordinario, 13–40. https://bibliotecavirtual.defensa.gob.es/BVMDefensa/es/catalogo_imagenes/grupo.do?path=309075

Organización para la Seguridad y la Cooperación en Europa. (2017). Guía de la OSCE sobre actividad policial basada en la inteligencia (Departamento de Amenazas Transnacionales Unidad de Asuntos Policiales de carácter estratégico, Ed.; Vol. 13).

Payá-Santos, C. A. (2023). El desempeño de la inteligencia en España en el ámbito público, empresarial y académico. Revista Científica General José María Córdova, 21(44), 1029–1047. https://doi.org/10.21830/19006586.1222

Phythian, M., Warner, M., Gill, P., Richards, J., Davier, P. H. J., Gustafson, K., Ridgen, I., Brantly, A., Sheptycki, J., Strachan-Morris, D., Omand, D., & Hulnick, A. S. (2013). Understanding the Intelligence Cycle (M. Phythian, Ed.).

Portillo, I. (2019). Conociendo que es la Ciberinteligencia y el Cyber Threat Intelligence. https://www.ginseg.com/ciberinteligencia/conociendo-que-es-la-ciberinteligencia-y-el-cyber-threat-intelligence/

Pothoven, S., Rietjens, S., & de Werd, P. (2023). Producer-client paradigms for defense intelligence. Defence Studies, 23(1), 68–85. https://doi.org/10.1080/14702436.2022.2089658

Stewart Bertram. (2015). The Tao of Open Source Intelligence. IT Governance Publishing.

Summers, L., & Rossmo, D. K. (2019). Offender interviews: implications for intelligence-led policing. Policing, 42(1), 31–42. https://doi.org/10.1108/PIJPSM-07-2018-0096

Vela Tejada, J. (1993). Tradición y originalidad en la obra de Eneas El Táctico: La génesis de la historiografía militar. Minerva. Revista de Filología Clásica, 7, 79–92. https://doi.org/https://doi.org/10.24197/mrfc.7.1993