

Capítulo 8

De la sombra al algoritmo: la transformación cognitiva de la inteligencia*

DOI: <https://doi.org/10.25062/9786287818712.08>

Carlos Enrique Álvarez Calderón

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo explora la evolución histórica y epistemológica de la actividad de inteligencia, desde sus raíces empíricas en la observación y el espionaje, hasta su configuración contemporánea como sistema cognitivo adaptativo. A partir de una metodología histórico-analítica, se interpreta la inteligencia como una forma de conocimiento estratégico que ha acompañado la transformación de la guerra, pasando del dominio físico al informacional y, finalmente, al cognitivo. Se argumenta que la inteligencia no solo produce información, sino marcos de interpretación que orientan la acción, constituyendo así una epistemología aplicada del poder. Se identifican tres momentos decisivos: la institucionalización moderna del espionaje como práctica racional del Estado; la profesionalización y tecnologización durante la Guerra Fría, y la actual hibridación entre inteligencia, ciberespacio e inteligencia artificial. En la era de las guerras de quinta generación, la inteligencia se redefine como un proceso complejo de *sensemaking* reflexivo, donde los algoritmos complementan, pero no sustituyen, el juicio humano. Se concluye que la verdadera revolución de la inteligencia no es técnica, sino cognitiva: consiste en aprender a comprender cómo el acto de conocer transforma la realidad misma que busca dominar.

Palabras clave: ciberinteligencia; complejidad; epistemología; guerra cognitiva; inteligencia estratégica; poder informacional

* Capítulo de libro resultado del proyecto de investigación "Desafíos y nuevos escenarios de la seguridad multidimensional a nivel nacional, regional y hemisférico en el decenio 2015-2025", del grupo de investigación Centro de Gravedad de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado como A por MinCiencias (código COL0104976). Los puntos de vista expresados pertenecen a su autor y no necesariamente reflejan el pensamiento de esta institución.

Carlos Enrique Álvarez Calderón

Candidato a doctor en Estudios Estratégicos, Seguridad y Defensa, Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia. Magíster en Coaching Ontológico Empresarial, Universidad San Sebastián, Chile. Politólogo y Magíster en Relaciones Internacionales, Pontificia Universidad Javeriana, Colombia. Investigador Asociado MinCiencias y Docente Investigador, Escuela Superior de Guerra “General Rafael Reyes Prieto”. Profesional Oficial de Reserva, Fuerza Aeroespacial Colombiana. Asesor y consultor en seguridad y defensa para instituciones de las Fuerzas Militares de Colombia y a nivel internacional.

Orcid: <https://orcid.org/0000-0003-2401-2789> - Contacto: carlos.alvarez@esdeg.edu.co

Citación APA: Álvarez-Calderón, C. E. (2026). De la sombra al algoritmo: la transformación cognitiva de la inteligencia. En C. E. Álvarez Calderón (Ed.), *El campo de batalla digital: la defensa nacional en la era algorítmica, volumen II. (Guerra cognitiva: la mente como campo de batalla del siglo)* (pp. 555-684). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818712.08>

EL CAMPO DE BATALLA DIGITAL: LA DEFENSA NACIONAL EN LA ERA ALGORÍTMICA. VOLUMEN II. GUERRA COGNITIVA: LA MENTE COMO CAMPO DE BATALLA DEL SIGLO XXI

ISBN IMPRESO (Obra completa): 978-628-7818-65-1

ISBN DIGITAL (Obra completa): 978-628-7818-69-9

ISBN IMPRESO Volumen II: 978-628-7818-67-5

ISBN DIGITAL Volumen II: 978-628-7818-71-2

DOI: <https://doi.org/10.25062/9786287818712>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra “General Rafael Reyes prieto”

Bogotá D.C., Colombia

2026



Introducción

La historia de la inteligencia es, en el fondo, la historia de cómo las sociedades han aprendido a transformar la información en conocimiento útil para sobrevivir, anticiparse y dominar. Desde una perspectiva epistemológica, la actividad de inteligencia constituye un sistema cognitivo aplicado, una interfaz entre el conocimiento y la acción que busca reducir la incertidumbre en entornos de conflicto. En este sentido, la inteligencia no es solo un conjunto de prácticas (espionaje, análisis, contrainteligencia), sino también una arquitectura del saber estratégico. Su evolución refleja cómo la humanidad ha aprendido a observar, clasificar y manipular la información, y cómo ese proceso ha acompañado la transformación de la guerra desde la linealidad física hacia la complejidad informacional.

Floridi (2011) propone que vivimos inmersos en una infosfera, un entorno donde la información constituye el tejido mismo de la realidad. Pero esta concepción tiene raíces profundas en la historia de la inteligencia, que desde los albores de la modernidad funcionó como el primer laboratorio de gestión informacional. Cada avance técnico en espionaje, criptografía o análisis de datos respondió, en el fondo, a una necesidad epistemológica consistente en ampliar la capacidad humana de conocer lo desconocido y de actuar sobre lo incierto. En este sentido, la inteligencia anticipó la revolución cognitiva de la era digital, pues ya desde los siglos XVI y XVII combinaba observación empírica, interpretación contextual y producción de conocimiento situado.

Warner (2002) define la inteligencia como “el conocimiento organizacional destinado a informar la acción en contextos de competencia o amenaza” (p. 16), una formulación que resuena con la noción de Floridi sobre la información como entidad activa. Ambos coinciden en que el valor de la información no reside en

su acumulación, sino en su capacidad de generar sentido y orientar decisiones. Así, la inteligencia puede entenderse como una epistemología aplicada al conflicto militar, en la que cada generación de la guerra (de la pólvora a los algoritmos) ha reformulado la relación entre percepción, conocimiento y poder.

Durante varios siglos, la inteligencia operó en el umbral entre la observación y la interpretación. En los imperios antiguos y medievales, los espías eran recolectores de datos dispersos; en la modernidad, se convirtieron en traductores de signos y constructores de narrativas. El espionaje dejó de ser una práctica de intuición individual para convertirse en un proceso institucionalizado de análisis, donde la información debía validarse, clasificarse y transmitirse de manera sistemática. Wheeler (2011) señala que entre los siglos XVI y XVIII surgió un tipo de inteligencia imperial que combinaba la exploración geográfica con la observación política, dando origen a una forma de conocimiento totalizante que integraba el mapa, la carta y el rumor. La información dejaba de ser local para convertirse en global, preludiando la emergencia de una conciencia planetaria del poder.

Este tránsito no fue solamente técnico, sino también cognitivo. A medida que los Estados-nación centralizaban sus aparatos de espionaje y diplomacia, también se redefinía el concepto mismo de la "verdad estratégica". Los informes, mapas y cifras se transformaron en instrumentos de interpretación del mundo, y la inteligencia pasó a ser el lenguaje de la racionalidad estatal. En la medida en que los imperios aprendieron a medir, cartografiar y registrar, también aprendieron a controlar. La información se convirtió en una forma de soberanía epistémica, un poder sobre el entorno y sobre la mente.

Desde esta perspectiva, la evolución histórica de la inteligencia puede leerse como una secuencia de transformaciones cognitivas. En la primera generación de la guerra, la inteligencia sirvió para observar y registrar. En la segunda, para analizar y anticipar. En la tercera, para coordinar y sincronizar. y en la cuarta, para influir y manipular percepciones. Cada etapa amplió el campo de la información como dominio de confrontación, hasta convertirla en un teatro cognitivo global donde la verdad misma se volvió un recurso estratégico.

A partir de esta premisa, el presente capítulo se propone responder a una pregunta central: ¿cómo ha evolucionado la inteligencia como forma de conocimiento estratégico y dispositivo de control cognitivo desde sus orígenes empíricos hasta su actual configuración en las guerras de quinta generación? Para responderla, se adopta una metodología histórico-analítica y epistemológica, que combina la reconstrucción documental con la interpretación teórica y la prospectiva estratégica.

Para ello se examina la génesis institucional y tecnológica de la inteligencia como práctica de observación y control, desde los servicios secretos imperiales hasta la Guerra Fría. Luego, se analizan los cambios epistemológicos que acompañaron la transición hacia la era digital, donde la información se convirtió en un campo de batalla simbólico. Finalmente, se exploran las mutaciones contemporáneas de la inteligencia (ciberinteligencia, inteligencia cultural, social y cognitiva), que anuncian una nueva etapa en la evolución del conocimiento estratégico.

Esta aproximación metodológica asume que comprender la inteligencia no implica solo estudiar sus instrumentos o agencias, sino reconocer su dimensión ontológica: la manera en que produce realidad al definir lo que debe conocerse, protegerse o combatirse. En consecuencia, este capítulo aborda la historia de la inteligencia como una genealogía del saber estratégico, donde las prácticas de observación, análisis y manipulación informacional se integran en un mismo proceso evolutivo: la conversión de la información en poder.

Inteligencia como conocimiento estratégico en la infosfera

La historia de la *inteligencia*¹ muestra una constante, el afán humano por conocer mejor que el adversario. Desde los primeros sistemas de observación hasta los actuales algoritmos de vigilancia, la función esencial no ha cambiado. Lo que ha variado es el entorno donde ese conocimiento se produce y las lógicas que lo sustentan. En la actualidad, la práctica de la inteligencia ocurre dentro de un ecosistema informacional total, una infosfera donde datos, percepciones y significados se entrelazan. Comprender la inteligencia exige, por tanto, un marco teórico que permita transitar de la información como insumo al conocimiento como ventaja.

¹ En este capítulo, el término *inteligencia* se emplea en tres planos complementarios. En su sentido más amplio, designa una forma de conocimiento estratégico orientada a reducir la incertidumbre y proporcionar ventaja decisional frente a actores, amenazas o contextos complejos. En un sentido funcional, se entiende como *actividad de inteligencia*, es decir, el conjunto de procesos institucionales mediante los cuales el Estado recolecta, procesa, analiza y difunde información relevante para la seguridad y la defensa nacional, conforme a la Ley Estatutaria 1621 de 2013. Finalmente, en un sentido epistemológico, el término se refiere al *conocimiento de inteligencia*, o sea, al producto analítico resultante de la interpretación crítica de la información y su conversión en comprensión útil para la acción estratégica. Esta triple distinción (ontológica, funcional y epistémica), permite analizar la inteligencia no solo como práctica estatal, sino como disciplina del conocimiento inscrita en la infosfera contemporánea.

La actividad de inteligencia no es solamente una actividad de espionaje ni tan solo un proceso técnico de recolección. Es, ante todo, un modo de conocer orientado a la acción, una epistemología aplicada al poder²; por ello, su valor radica en transformar datos dispersos en comprensión contextual que guíe la toma de decisiones bajo contextos de incertidumbre. En este sentido, la inteligencia se convierte en un subsistema cognitivo del Estado, un dispositivo que convierte información en decisión y decisión en poder.

Por consiguiente, el presente marco teórico aborda la *dimensión epistemológica* de la inteligencia³ desde cuatro ejes complementarios que permiten comprender su complejidad actual. El primero es el eje ontológico, sustentado en la teoría de la información, que explica cómo los datos adquieren sentido dentro de la infosfera. El segundo es el eje epistemológico, centrado en la inteligencia como forma de conocimiento estratégico orientado a la acción. El tercero es el eje metodológico, que examina la transición del modelo lineal del ciclo de inteligencia hacia sistemas adaptativos de producción de conocimiento. Finalmente, el cuarto eje es el cognitivo-estratégico, que explora la interacción entre inteligencia, engaño y GC como expresión contemporánea del poder informacional.

Teoría filosófica de la información como marco ontológico de la inteligencia

La noción moderna de la inteligencia no puede comprenderse sin una reflexión ontológica sobre la información. En la medida en que los Estados, las organizaciones y los individuos dependen cada vez más de los flujos informacionales para orientarse y decidir, la inteligencia se configura como una práctica situada dentro de la *infosfera*⁴, un entramado global de datos, signos y significados que constituye el nuevo entorno ontológico de la humanidad. Luciano Floridi (2010) advierte que la humanidad ya no habita solo un mundo lleno de información, sino que vive en la

² La definición clásica de poder, formulada por Weber (1947) y desarrollada por Dahl (1957), lo entiende como la capacidad de un actor para lograr que otro haga o deje de hacer algo que, en ausencia de esa influencia, no habría hecho. Álvarez et al. (2018) amplía este principio al plano cognitivo al sostener que el poder en la era informacional no solo modifica conductas, sino también percepciones y marcos mentales, configurando la voluntad del otro desde el control del significado y la información.

³ La *dimensión epistemológica* de la inteligencia se refiere al estudio de los fundamentos, métodos y límites del conocimiento que esta produce. Implica comprender cómo la inteligencia transforma información en comprensión significativa y cómo valida la veracidad, pertinencia y utilidad de ese conocimiento para la toma de decisiones. En este sentido, la inteligencia no es solo una práctica técnica o instrumental, sino un proceso cognitivo que busca generar verdad operativa bajo condiciones de incertidumbre.

⁴ Sobre la infosfera, véase el capítulo 7 de este volumen.

información, puesto que los seres humanos son *inforgs*⁵, es decir, organismos informacionales inmersos en un complejo ecosistema de datos que mediatiza toda percepción, relación y decisión.

En este contexto, la inteligencia emerge como el sistema que transforma información en conocimiento significativo para la acción estratégica. Si toda realidad política y militar contemporánea está informacionalmente mediada, entonces la inteligencia no es solo una técnica de obtención de datos, sino un proceso de interpretación semántica y gestión del sentido. La función esencial del analista consiste en separar la señal del ruido, construir significado y otorgar valor epistémico a la información para convertirla en conocimiento estratégico. Como señala Floridi (2011), la información no adquiere valor por su mera existencia, sino por su capacidad para reducir incertidumbre y aumentar la comprensión del agente que la procesa. De ahí que la inteligencia se configure como una práctica epistémica especializada dentro de la arquitectura de la infosfera.

Bajo esta perspectiva, el conocimiento de inteligencia es un producto derivado de tres operaciones encadenadas: 1) la *recolección* (datos), 2) el *procesamiento* (información) y 3) el *análisis* (conocimiento). De ahí que la primera implica observación y acceso⁶; la segunda, clasificación y validación⁷; y la tercera, inferencia y juicio⁸. En este orden de ideas, para Mark Lowenthal (2022) la información es todo lo que se puede conocer, mientras que la inteligencia se refiere a toda información que ha sido recolectada, procesada y analizada para satisfacer las necesidades de los responsables en la toma de decisiones. La distinción parece sencilla, pero

⁵ Sobre los *inforgs*, véase el capítulo 7 de este volumen.

⁶ La recolección de inteligencia consiste en la obtención sistemática de datos provenientes de fuentes humanas, técnicas o abiertas. Su propósito es reunir información relevante para los requerimientos definidos por los niveles político, estratégico u operacional, empleando métodos como la observación directa, la vigilancia electrónica, la interceptación de señales o el análisis de fuentes públicas. En el marco de la Ley 1621 de 2013, la recolección de inteligencia corresponde a la obtención planificada, controlada y legal de información relevante para los fines de seguridad y defensa nacional. Comprende la utilización de medios humanos, técnicos y fuentes abiertas (HUMINT, SIGINT, OSINT, entre otros) autorizados por la ley, con el objetivo de satisfacer los requerimientos de información establecidos por la autoridad competente dentro del proceso de inteligencia.

⁷ El procesamiento comprende el conjunto de actividades mediante las cuales la información recolectada es organizada, depurada y validada para hacerla utilizable. Incluye la traducción, decodificación, clasificación, almacenamiento y verificación de los datos, con el fin de garantizar su confiabilidad antes de ser sometidos al análisis, conforme a los principios de veracidad, necesidad y proporcionalidad señalados en la Ley 1621 de 2013.

⁸ El análisis constituye la fase interpretativa del ciclo de inteligencia. En ella se evalúa, compara e integra la información procesada para generar conocimiento útil que permita comprender situaciones, anticipar escenarios y apoyar la toma de decisiones estratégicas, operacionales o tácticas. De acuerdo con la doctrina de inteligencia militar colombiana, es la etapa en la que los datos se transforman en conocimiento estratégico.

encierra una consecuencia ontológica y es que el dato no tiene existencia significativa fuera del proceso que lo convierte en conocimiento útil (Tabla 1).

Tabla 1. *Arquitectura cognitiva de la información y su transformación en conocimiento estratégico*

Nivel	Naturaleza	Operación cognitiva	Propósito en inteligencia	Riesgos/ Vulnerabilidades	Autores clave
Dato	Hecho bruto, fragmentado y no interpretado	Observación / recolección	Capturar señales del entorno	Ruido, sobrecarga informacional, datos falsos	Floridi (2010); Lowenthal (2022)
Información	Dato contextualizado, organizado y validado	Clasificación / validación	Reducir incertidumbre inicial	Sesgos de selección, manipulación, desinformación	Johnson (2010); McDowell (2009)
Conocimiento	Información integrada en marcos interpretativos	Análisis / inferencia	Comprender la situación estratégica	Sesgos cognitivos, modelos erróneos, sobreinterpretación	Floridi (2011); Kent (1965)
Inteligencia estratégica	Conocimiento orientado a la decisión	Síntesis / juicio estratégico	Guiar la acción y anticipar escenarios	Fallas de alerta, politización, errores de estimación	Kent (1965); Herman (1996); Lowenthal (2022)
Decisión / Sabiduría estratégica	Aplicación del conocimiento bajo incertidumbre	Acción / evaluación adaptativa	Generar ventaja estratégica	Rigidez decisional, mala adaptación, error estratégico	MacGaffin y Oleson (2015)

Fuente: Elaboración propia

La Tabla 1 muestra que la inteligencia constituye el punto más alto de una jerarquía semántica donde los datos se transforman en conocimiento útil mediante los procesos de la interpretación y la validación. Cada nivel agrega un valor epistémico distinto y exige una operación cognitiva específica. En ese sentido, la inteligencia no se define por la cantidad de información acumulada, sino por la calidad del significado que logra construir a partir de ella. En la práctica de la inteligencia, el dato no es, sino que deviene en función del contexto y del propósito.

Esta idea es coherente con la reflexión de Loch Johnson (2010), quien sostiene que la inteligencia nacional debe entenderse ante todo como una forma de información organizada y dirigida a la toma de decisiones políticas. Johnson (2010) afirma que la inteligencia “es información relevante para los intereses de seguridad nacional que ha sido sistemáticamente recolectada y analizada para orientar a los decisores en entornos de incertidumbre” (p. 5). De este modo, la diferencia entre

información y conocimiento estratégico radica en el proceso de transformación que agrega valor y contexto a los datos. La inteligencia, por tanto, no es sinónimo de secreto, sino de pertinencia, ya que su función principal es producir información procesada (es decir, conocimiento), que permita actuar.

Esta perspectiva permite entender que la práctica de la inteligencia, en su forma más fundamental, consiste en reducir la *ambigüedad*⁹. Según Johnson (2010), la información sin análisis es tan inútil como el análisis sin información confiable; ambas dimensiones son inseparables, y el ciclo que las une constituye el núcleo epistémico de la comunidad de inteligencia. Floridi (2011) coincide en este punto cuando afirma que el conocimiento no surge del volumen de datos, sino del proceso semántico que convierte la información en comprensión significativa

El vínculo entre teoría de la información e inteligencia se refuerza al observar cómo los sistemas nacionales de seguridad y defensa se estructuran como redes de procesamiento informacional. Johnson (2010) describe a la comunidad de inteligencia estadounidense como un organismo distribuido de conocimiento en el que múltiples agencias recolectan, procesan y analizan información con distintos enfoques y prioridades, pero con un propósito común, orientado a dotarle al Estado de una conciencia situacional extendida. Desde esta óptica, la inteligencia cumple una función cognitiva sistémica, debido a que constituye la memoria y el sentido del aparato estatal.

La visión de Sir Richard Dearlove (2010) complementa este argumento al enfatizar la dimensión social de la información, ya que, en su opinión, seguridad nacional y percepción pública son hoy por hoy inseparables. La inteligencia, concebida tradicionalmente como un conocimiento secreto destinado a los gobiernos, ha pasado a operar también en un entorno mediático donde la información circula sin control y la opinión pública termina influyendo en la legitimidad de las políticas de seguridad. En este nuevo escenario, la información no es solo un insumo técnico, sino un elemento de ansiedad social que condiciona el valor político del conocimiento. Dicho de otra manera, la infosfera ha diluido la frontera entre inteligencia y comunicación pública, lo que obliga a repensar la gestión informacional del Estado en clave cognitiva y ética.

⁹ En el contexto de la actividad de inteligencia, la *ambigüedad* se refiere a la presencia simultánea de múltiples interpretaciones posibles de un hecho o situación debido a información incompleta, contradictoria o incierta. Reducir la ambigüedad implica transformar datos confusos o dispersos en conocimiento claro y coherente que permita orientar la toma de decisiones bajo condiciones de incertidumbre.

Floridi (2015) proporciona el marco filosófico para comprender este desafío, ya que, si la información constituye el tejido ontológico de la realidad social en el presente, entonces la manipulación informacional equivale a una forma de poder. La ética de la información, por ende, se convierte en parte de la doctrina de seguridad. Defender la integridad semántica del entorno informacional es proteger la autonomía interpretativa de los ciudadanos y de las instituciones. Por esta razón, la actividad de inteligencia, al operar sobre información crítica y sensible, asume una responsabilidad epistémica al producir conocimiento verdadero frente a la desinformación, el engaño y el ruido.

En este sentido, el marco informacional de Floridi se traduce en términos operativos en lo que Johnson (2010) llama "la responsabilidad analítica" del sistema de inteligencia. No basta con recolectar datos, ni con producir informes; se trata de generar interpretaciones rigurosas, imparciales y contextualizadas que contribuyan al interés público. Este principio ético, conocido en la comunidad como *speaking truth to power*, implica que el analista debe mantener independencia intelectual frente a presiones políticas y mediáticas, preservando la calidad epistémica del conocimiento producido.

Por ende, la función estratégica de la inteligencia consiste en transformar un volumen caótico de información en una narrativa coherente que guíe la acción. Esa narrativa, al condensar significados, otorga ventaja, por lo que el valor de la actividad de la inteligencia reside en la calidad de su inferencia y no en la cantidad de sus datos. Las operaciones exitosas del pasado (desde la ruptura del código *Enigma* hasta la operación *Jaque*), ejemplifican este principio en el que lo decisivo no fue acumular más información, sino interpretar mejor la ya disponible. En la práctica, la diferencia entre la información y la inteligencia se mide por la capacidad de ver antes y comprender mejor.

Si la infosfera constituye el entorno donde la información circula y se disputa, la inteligencia actúa como un sistema nervioso que dota de coherencia a ese flujo. Su eficacia depende tanto de la calidad de sus insumos como de la arquitectura cognitiva que los procesa. La teoría filosófica de la información de Floridi (2011; 2015), en este sentido, proporciona la ontología¹⁰ que les faltaba a las teorías de

¹⁰ En este contexto, la ontología se refiere al estudio del ser o de la naturaleza fundamental de un fenómeno. Aplicada a la actividad de inteligencia, implica indagar qué es en su esencia, cómo existe dentro del ecosistema informacional y qué relaciones mantiene con los datos, el conocimiento y la acción. No se trata de un aspecto técnico, sino de una reflexión filosófica sobre el modo de ser de la inteligencia en el marco de la sociedad de la información.

la inteligencia, al ofrecer un marco conceptual que explica su naturaleza como fenómeno emergente de la interacción entre los datos, el significado y la acción. En este punto, Terry Quist (2022) aporta una reflexión decisiva al sostener que la inteligencia no puede entenderse únicamente como una técnica de obtención o análisis de información, sino como una práctica filosófica aplicada que combina ontología, epistemología y ética. En su opinión, “no existe una filosofía única de la inteligencia” (p. 778), pero la aplicación del pensamiento filosófico es indispensable para comprender qué es la inteligencia, por qué se ejerce y cuáles son sus límites.

Además, en un mundo saturado de información, la ventaja no proviene de acumular más datos, sino de producir conocimiento más pertinente, más confiable y más oportuno. Por lo tanto, la filosofía aporta el andamiaje conceptual que permite al analista examinar los supuestos ontológicos y normativos que guían su trabajo: qué se considera “real”, qué se asume como “verdadero” y qué se entiende por “riesgo” o “justificación”. Así, mientras la teoría de la información proporciona el sustrato ontológico (el ser informacional del mundo), la filosofía introduce la reflexión crítica sobre el sentido y la finalidad del conocimiento que la inteligencia produce. Según Quist (2022), la falta de este examen filosófico conduce a lo que denomina *shadow thinking*, es decir, la tendencia a reificar metáforas y confundir construcciones analíticas con realidades objetivas, fenómeno que oscurece la comprensión del entorno estratégico. De ahí que, más allá de procesar datos, la inteligencia deba cultivar una conciencia ontológica sobre los marcos de pensamiento que estructuran su práctica y condicionan sus juicios.

La reflexión de Quist (2022) también coincide con la noción de *ontología social* propuesta por Pili (2020). Muchas de las entidades que analiza la inteligencia (por ejemplo, la figura del enemigo, la amenaza o el riesgo), no existen de forma natural, sino como construcciones sociales sostenidas por creencias colectivas y prácticas institucionales. Desde esta óptica, la infosfera no solamente contiene datos, sino representaciones compartidas que configuran la realidad política y estratégica. Reconocer este carácter construido del objeto de estudio permite a la inteligencia evitar la proyección cognitiva o especular (*mirror imaging*)¹¹ y comprender

¹¹ La “proyección cognitiva” (*mirror imaging*) es una distorsión analítica común en los procesos de inteligencia que consiste en atribuir al adversario los mismos valores, motivaciones y modos de razonamiento que posee el propio analista o su comunidad política. Este sesgo proyectivo genera una ilusión de simetría cognitiva que impide comprender las lógicas culturales, ideológicas o estratégicas del otro. Según Quist (2022), el problema de la *proyección cognitiva* deriva de la dificultad epistemológica de acceder a la mente ajena y del uso inconsciente del propio marco de referencia para inferir intenciones o comportamientos del adversario. Reconocer y neutralizar este sesgo es fundamental para evitar errores de estimación y mejorar la comprensión ontológica del entorno estratégico.

que cada actor interpreta el mundo desde un marco ontológico distinto. En consecuencia, la información no solo describe el mundo, también lo crea, y el papel del analista consiste en descifrar esas estructuras simbólicas para dotar al Estado de una comprensión más lúcida del entorno semántico en el que actúa¹².

En resumen, la teoría filosófica de la información ofrece el fundamento ontológico de la actividad inteligencia moderna al situarla como práctica cognitiva dentro de la infosfera. Al comprender que los seres humanos y las instituciones son inforgs que operan en redes de datos interdependientes, se reconoce que el poder ya no se ejerce solo sobre territorios físicos, sino sobre territorios semánticos, en los cuales la inteligencia es la disciplina que explora, defiende y administra esos territorios del significado; por consiguiente, de su capacidad para mantener la integridad informacional del Estado depende no solo la seguridad material, sino también la soberanía cognitiva de las naciones.

En este punto, la reflexión ontológica sobre la información se transforma en una reflexión epistemológica sobre el conocimiento. Es decir, si la teoría de la información permite entender *qué* es la inteligencia y *en qué* entorno existe, la teoría del conocimiento estratégico busca explicar *cómo* conoce y *para qué* conoce. La inteligencia no solo habita la infosfera, sino que actúa dentro de ella mediante procesos de observación, interpretación y anticipación. La transición del dato al conocimiento y de la información a la decisión exige un marco que dé cuenta de las condiciones bajo las cuales se produce conocimiento útil, confiable y oportuno. De ahí que la epistemología de la inteligencia se oriente hacia el estudio de sus métodos, sesgos y límites, es decir, hacia el modo en que convierte la información en poder.

Teoría del conocimiento estratégico en inteligencia

La inteligencia, en su forma más pura, constituye una epistemología aplicada al poder. Nace de la necesidad de conocer mejor que el adversario y de transformar la incertidumbre en decisión; en términos filosóficos, puede considerarse como una disciplina del conocimiento orientada a la acción estratégica. Sherman Kent (1965) fue uno de los primeros en formular con claridad esta idea al definir la inteligencia como “el conocimiento que nuestros líderes deben poseer para salvaguardar la

¹² Quist (2022) denomina “ontología social” al estudio de cómo las instituciones y comunidades de inteligencia generan y sostienen creencias compartidas que configuran su realidad operativa. En este marco, incluso la noción de enemigo es una categoría construida que existe porque se cree en ella. Esta lectura coincide con la concepción de Floridi (2010) sobre la infosfera como territorio semántico, donde los significados son entidades reales que influyen en la conducta política y estratégica.

seguridad nacional” (p. 3). Con ello estableció un principio fundacional, en cuanto que la inteligencia no es solamente información ni mera actividad burocrática, sino un proceso cognitivo que permite al Estado anticipar y orientar sus actos en un entorno complejo.

La teoría del conocimiento estratégico se estructura, por tanto, sobre la relación entre información, interpretación y poder decisional. El conocimiento de inteligencia no busca la verdad absoluta, sino la comprensión suficiente para actuar. Por ende, su fin no es teórico, sino pragmático, ya que busca reducir la *fricción*¹³ y aumentar la coherencia entre los medios, fines y contextos. En este sentido, Whitesmith (2022) sostiene que el analista no trabaja en un régimen de verdad verificable, sino en un sistema de justificación razonada, en donde la validez del conocimiento depende de la calidad argumentativa y de la coherencia inferencial más que de su correspondencia empírica con la realidad. En otras palabras, la inteligencia no busca la verdad ontológica, sino la justificación pragmática que permita tomar decisiones informadas bajo condiciones de incertidumbre¹⁴. Michael Herman (1996) lo expresa al afirmar que “la inteligencia es un poder en sí mismo” (p. 2), porque influye directamente en la conducta del Estado y en su posición en el sistema internacional; de ahí que las comunidades de inteligencia funcionen como sistemas de conocimiento que administran la incertidumbre y producen ventaja política, militar o económica frente a los demás actores.

Kent (1965) propuso distinguir entre tres funciones del conocimiento estratégico: la recopilación, el análisis y la estimación. La primera busca información relevante; la segunda, evaluarla críticamente; la tercera, derivar conclusiones y pronósticos que guíen la acción. El eje unificador es el juicio analítico, entendido como el arte de inferir a partir de información incompleta. Este enfoque reconoce que toda decisión en política exterior o seguridad nacional se toma bajo condiciones de ambigüedad. Por eso la inteligencia no puede aspirar a la certeza, sino a la probabilidad informada. Lowenthal (2022) sigue esta línea de pensamiento al definir la

¹³ El término *fricción* proviene de la teoría de la guerra de Carl von Clausewitz y designa el conjunto de factores imprevisibles que interfieren entre la planificación racional y la ejecución real de una acción. Incluye desde errores humanos y fallas logísticas hasta incertidumbres psicológicas y contingencias del entorno. En el ámbito de la inteligencia, la fricción se manifiesta en la distancia entre la información disponible y la comprensión efectiva que de ella se obtiene, afectando la coherencia entre los medios, los fines y el contexto estratégico. La función del conocimiento de inteligencia, por tanto, no es eliminar la fricción (lo cual es imposible), sino reducir su impacto mediante la anticipación, el análisis crítico y la adaptación continua (Clausewitz, 1984).

¹⁴ El modelo clásico de conocimiento como “creencia verdadera justificada”, reinterpretado en el campo de la inteligencia, sostiene que la verdad absoluta resulta inalcanzable; lo que otorga valor epistémico al análisis es la justificación racional y verificable del proceso de inferencia (Whitesmith, 2022).

inteligencia como el producto de la información que ha sido procesada y analizada para satisfacer las necesidades de los responsables de la formulación de políticas. En su planteamiento, la información constituye la materia prima, mientras que la inteligencia es el resultado de su transformación a través del análisis. El valor del conocimiento estratégico se mide, entonces, por su relevancia y su impacto en la toma de decisiones. Este proceso de conversión epistemológica (de datos a significado, de información a conocimiento útil), distingue a la inteligencia de otras formas de saber.

El propósito esencial de la *inteligencia estratégica*¹⁵ es reducir la incertidumbre del entorno para los tomadores de decisiones de política pública. Este principio, formulado por Kent (1965) y reafirmado por Lowenthal (2022), atraviesa toda la práctica contemporánea. Como sostiene Richards Heuer (1999), el analista de inteligencia trabaja con fragmentos de información, señales débiles y datos contradictorios, por lo que su desafío es construir una interpretación coherente que sea útil y creíble. Sin embargo, el proceso analítico está sujeto a los límites cognitivos de quien lo realiza, debido a que los sesgos de confirmación, la disponibilidad heurística o la tendencia a percibir patrones ilusorios pueden distorsionar los juicios más experimentados. Por ello, Heuer propone desarrollar “métodos estructurados de análisis” que ayuden a contrarrestar estos sesgos y a mejorar la calidad epistémica del conocimiento producido¹⁶.

En esta misma línea, Whitesmith (2022) ha planteado que la justificación analítica constituye el núcleo epistemológico del conocimiento de inteligencia. La verdad, en este contexto, se sustituye por *verosimilitud suficiente*, y el elemento

¹⁵ Sherman Kent (1965) definió la inteligencia estratégica como el conocimiento que los líderes nacionales necesitan para salvaguardar la seguridad y orientar la política exterior del Estado. A diferencia de la inteligencia militar, centrada en la planificación y ejecución de operaciones militares, la inteligencia estratégica busca comprender las capacidades, intenciones y tendencias políticas, económicas y tecnológicas de otros actores, con el fin de anticipar riesgos y oportunidades a largo plazo. Para Kent, esta forma de conocimiento no se limita al ámbito castrense, sino que constituye un instrumento de gobierno y de formulación de políticas nacionales.

¹⁶ Heuer (1999) advierte que los analistas de inteligencia, al igual que cualquier ser humano, están sujetos a limitaciones cognitivas derivadas de la estructura misma del pensamiento. Los *sesgos de confirmación* llevan a aceptar preferentemente la información que valida las hipótesis previas y a desestimar aquella que las contradice. La *heurística de disponibilidad* induce a sobrevalorar la probabilidad de un evento según la facilidad con que se recuerdan casos similares, lo que puede generar percepciones distorsionadas de riesgo o frecuencia. A su vez, la *tendencia a percibir patrones ilusorios* impulsa a ver coherencia o causalidad donde solo existe coincidencia, reforzando narrativas analíticas erróneas. Para Heuer, estos mecanismos inconscientes no son fallas de razonamiento individuales, sino propiedades universales del procesamiento humano de la información; por ello propone el uso de métodos estructurados de análisis que obliguen a cuestionar hipótesis, buscar evidencia contradictoria y explicitar supuestos, con el fin de minimizar los errores sistemáticos en la estimación de inteligencia.

decisivo pasa a ser la solidez justificativa, basado en la trazabilidad del razonamiento, la consistencia de las inferencias y la transparencia metodológica¹⁷. Así, la fortaleza del análisis no depende del acceso a la verdad, sino del grado en que sus conclusiones pueden ser racionalmente defendidas frente a la duda y la ambigüedad. En este punto, la inteligencia se revela no solo como un sistema técnico, sino como una práctica cognitiva colectiva. La comunidad de analistas se convierte en un laboratorio epistemológico donde se ponen a prueba hipótesis, se contrastan fuentes y se evalúan probabilidades. La teoría del conocimiento estratégico, en consecuencia, no puede desligarse de la psicología del análisis. La objetividad absoluta es inalcanzable, pero la intersubjetividad rigurosa (es decir, el acuerdo racional entre analistas informados), puede acercarse a una comprensión razonable de la realidad.

Herman (1996) amplía esta concepción al destacar que el valor de la inteligencia depende tanto de su producción como de su recepción. El conocimiento estratégico se completa solo cuando el decisor lo incorpora a su razonamiento y lo traduce en acción. En muchos casos, la falla no radica en la calidad del análisis, sino en la voluntad política de aceptarlo. y la historia ofrece numerosos ejemplos, desde las advertencias ignoradas antes de Pearl Harbor hasta las evaluaciones de la Agencia Central de Inteligencia (CIA) durante Vietnam que chocaron con las percepciones optimistas del Pentágono; de allí surge una paradoja central, y es que la inteligencia puede ser epistémicamente correcta y, sin embargo, políticamente ineficaz si los líderes la desatienden (Álvarez, 2023).

En la práctica, la inteligencia produce dos tipos de capital cognitivo. El primero es la ventaja de decisión (*decision advantage*), entendida como la capacidad de actuar antes y con mayor conocimiento que el adversario. El segundo es la confianza de decisión (*decision confidence*), la seguridad epistemológica que permite ejecutar una acción sin dudar de su fundamento. En este sentido, MacGaffin y Oleson (2015) sostienen que ambos componentes son interdependientes, ya que la ventaja sin confianza conduce a la parálisis, y la confianza sin ventaja puede derivar en error o arrogancia estratégica. Según Whitesmith (2022), la confianza no surge de

¹⁷ El concepto de *verosimilitud suficiente* proviene de la filosofía de la ciencia y ha sido adaptado al campo de la inteligencia para describir el grado de aproximación razonable entre una hipótesis y la realidad observable. No implica una verdad definitiva, sino una plausibilidad argumentada que permite la acción informada. En contextos de incertidumbre (como los que enfrenta la inteligencia estratégica), la verosimilitud reemplaza la verdad como criterio operativo; es decir, una afirmación es suficientemente verosímil cuando está sustentada por evidencia coherente, contrastada y justificable dentro de los límites de la información disponible. Así, el conocimiento de inteligencia no se mide por su correspondencia empírica, sino por la solidez racional de su justificación y su utilidad práctica para la toma de decisiones (Whitesmith, 2022).

la certeza sino de la comprensión, ya que el decisor confía porque entiende cómo y por qué se llegó a una conclusión; la confianza, por ende, es una convicción epistémica derivada de la transparencia justificativa del proceso analítico.

En consecuencia, la inteligencia eficaz no solo otorga información superior, sino que consolida la certeza racional de que esa información es confiable, y esta doble dimensión también se aprecia en la experiencia histórica. Por ejemplo, durante la Segunda Guerra Mundial, el desciframiento de los códigos alemanes y japoneses proporcionó una ventaja decisoria al permitir anticipar movimientos y ajustar estrategias. En contraste, los fracasos de inteligencia previos al ataque terrorista del 11 de septiembre de 2001 demostraron cómo la ausencia de coordinación y la interpretación deficiente pueden convertir la abundancia de datos en una carga y no en un recurso. En ambos la lección es inequívoca: el conocimiento estratégico no depende del volumen de información, sino de la capacidad institucional y cognitiva para interpretarla correctamente.

Gill (2010) contribuye a esta visión epistemológica al situar la inteligencia dentro de un campo de teorías que buscan explicar cómo se produce, valida y aplica el conocimiento en contextos de seguridad. Propone distinguir entre tres enfoques: el empírico, centrado en la descripción y clasificación de prácticas; el normativo, orientado a la ética y la rendición de cuentas; y el analítico, que examina la inteligencia como forma de conocimiento. En este último enfoque, la inteligencia no es simplemente una actividad instrumental, sino un sistema cognitivo con su propio método y racionalidad. Gill subraya que entender la inteligencia como teoría del conocimiento implica reconocer su carácter interpretativo, debido a que los analistas no descubren verdades ocultas, sino que construyen narrativas plausibles basadas en evidencia incompleta. Este reconocimiento epistemológico de la inteligencia la aproxima más a las ciencias sociales que a las naturales, pues según Peter Gill (2010), el contexto y la subjetividad son ineludibles.

James Wirtz (2010), por su parte, aborda la relación entre teoría, fuentes y métodos dentro de los estudios en inteligencia, advirtiendo que la producción de conocimiento en inteligencia se enfrenta a un dilema metodológico permanente. La información disponible suele ser fragmentaria, clasificada o intencionalmente manipulada, lo que obliga a construir inferencias a partir de lagunas y ambigüedades. En su análisis, la inteligencia se asemeja a una forma de investigación aplicada que combina elementos de la historia, la sociología y la ciencia política con métodos empíricos y analíticos propios. Wirtz enfatiza que la validez del conocimiento de inteligencia depende de la triangulación de fuentes, la verificación

cruzada y la capacidad del analista para mantener un equilibrio entre escepticismo y creatividad.

Estos aportes refuerzan la idea de que la actividad de la inteligencia opera bajo un régimen epistemológico distinto al de la ciencia convencional. Si el científico parte de la premisa de la repetibilidad y la transparencia, el analista de inteligencia trabaja con lo irrepetible y lo oculto. Su conocimiento no es verificable en sentido experimental, pero sí evaluable en términos de coherencia, plausibilidad y eficacia decisoria. Por eso Gill (2010) propone hablar de una “ciencia práctica de la incertidumbre”, una disciplina cuyo objeto es transformar lo desconocido en lo parcialmente comprendido y lo incierto en lo manejable.

La confianza decisoria también se construye mediante la conrainteligencia. Saber que las propias fuentes son seguras y que la información no ha sido comprometida refuerza la fiabilidad del conocimiento. En este sentido, la conrainteligencia cumple una función epistémica al filtrar la información contaminada, detectar el engaño y validar la consistencia del análisis. Dicho de otra manera, la inteligencia sin conrainteligencia es conocimiento sin certeza. Kent (1965) ya intuía esta interdependencia cuando subrayó que “la inteligencia efectiva depende tanto de la protección de nuestras fuentes como de la penetración de las ajenas” (p. 141). Heuer (1999) añade otro elemento decisivo, relacionado con la importancia del aprendizaje organizacional. Los errores analíticos, lejos de ocultarse, deben convertirse en insumos para mejorar los modelos mentales y las metodologías. La inteligencia es, en este sentido, un sistema adaptativo que evoluciona mediante la revisión crítica de sus fallas. Esta lógica de mejora continua la conecta con la teoría de los sistemas complejos, en el que cada ciclo de análisis reconfigura la red cognitiva institucional y la prepara para nuevos desafíos.

En síntesis, la teoría del conocimiento estratégico concibe la inteligencia como una forma de razonamiento aplicado que combina método, juicio y ética. Gill (2010) la define como el puente entre el conocimiento científico y el conocimiento práctico del Estado, mientras que Wirtz (2010) la describe simplemente como la disciplina que enseña a razonar en la oscuridad; en ambos casos, el valor del conocimiento no radica en su certeza, sino en su capacidad para iluminar la acción. Por consiguiente, las lecciones de Kent, Heuer, Herman, Lowenthal, MacGaffin y Oleson convergen en una misma premisa, y es que el conocimiento es poder solo si es conocimiento confiable. La inteligencia, entendida como epistemología aplicada, traduce esa premisa en práctica institucional. y allí donde la información es infinita, la ventaja estratégica pertenece a quien sabe pensar mejor (Tabla 2).

Tabla 2. Principales enfoques teóricos del conocimiento estratégico en inteligencia

Autor	Enfoque principal	Aporte teórico	Limitación reconocida	Tipo de conocimiento generado
Kent (1965)	Epistemología racional-positivista	Inteligencia como conocimiento objetivo para la acción estatal	Supone certeza racional bajo incertidumbre	Conocimiento anticipatorio
Heuer (1999)	Psicología cognitiva	Identifica sesgos y propone métodos estructurados de análisis	Riesgo de sobre corrección analítica o rigidez metodológica	Conocimiento heurístico
Herman (1996)	Sociología del poder	Vincula inteligencia con influencia política y legitimidad institucional	Subestima los factores cognitivos individuales	Conocimiento político
Gill (2010)	Epistemología interpretativa	Reivindica la inteligencia como práctica de interpretación social y contextual	Dificultad de verificación empírica	Conocimiento contextual
Wirtz (2010)	Metodología interdisciplinar	Triangulación de fuentes y validación cruzada	Reconoce opacidad empírica estructural	Conocimiento empírico verificado
Lowenthal (2022)	Política pública/gestión	Inteligencia como interfaz entre análisis, decisión y rendición de cuentas	Enfoque excesivamente institucionalista	Conocimiento aplicado

Fuente: Elaboración propia

La Tabla 2 muestra cómo la teoría del conocimiento estratégico ha transitado de la objetividad racional de Kent (1965) hacia una epistemología pragmática e interpretativa en la que el valor del conocimiento depende tanto del rigor metodológico como del juicio humano. Cada enfoque, desde el análisis cognitivo hasta la interpretación contextual, revela una faceta complementaria de la inteligencia como ciencia práctica de la incertidumbre.

La evolución de las teorías del conocimiento estratégico ha tenido también un impacto decisivo en la comprensión de los métodos de la inteligencia. Si la reflexión epistemológica permitió redefinir el tipo de conocimiento que produce la comunidad de inteligencia, era inevitable que esta transformación alcanzara sus modelos de funcionamiento, ya que la práctica no puede permanecer ajena al cambio teórico. Entonces, a medida que la inteligencia fue entendida como un proceso interpretativo y no como una ciencia exacta, el tradicional modelo lineal del ciclo de inteligencia comenzó a mostrar sus límites. La complejidad de los entornos informacionales y la multiplicidad de actores exigieron reemplazar la secuencia rígida

de fases por una visión más dinámica y relacional del proceso. De esa revisión surge la noción contemporánea de red de inteligencia, que se examina a continuación.

Del ciclo lineal a la red de inteligencia en contextos complejos

El *ciclo de inteligencia*, concebido como un proceso ordenado de cinco fases (planificación, recolección, procesamiento, análisis y difusión)¹⁸, ha sido durante varias décadas la metáfora dominante para representar el funcionamiento de los sistemas de inteligencia. Su simplicidad pedagógica permitió institucionalizar la práctica, organizar responsabilidades y justificar la asignación de recursos. Sin embargo, como advierte Hulnick (2006), ese modelo lineal nunca describió con precisión cómo opera la inteligencia en la realidad, ya que fue, ante todo, un constructo didáctico útil para enseñar la secuencia lógica de las tareas, pero insuficiente para comprender la naturaleza dinámica, interactiva y política del proceso.

La principal limitación del modelo clásico radica en su visión unidireccional de la información. En el ciclo tradicional, las necesidades del decisor fluyen hacia los recolectores, estos generan información, los analistas la transforman en productos, y finalmente los resultados se difunden hacia los usuarios. Pues bien, Arthur Hulnick (2006) demostró que la inteligencia en la realidad no fluye en un circuito cerrado, sino en múltiples direcciones y que la retroalimentación constante entre analistas, recolectores y usuarios es la norma, no la excepción. De hecho, las preguntas de los decisores suelen reformularse a la luz de hallazgos parciales, y los analistas influyen a su vez en lo que se decide recolectar. Este carácter interactivo invalida la metáfora del ciclo como secuencia cerrada.

Mark Phythian (2013) coincide en que la linealidad del modelo oculta la complejidad institucional y cognitiva de la inteligencia contemporánea, en la medida en que, en la práctica, los límites entre sus fases tienden a difuminarse. La recolección se entrelaza con el análisis, y la difusión es un proceso continuo de comunicación y ajuste, no un punto final. Por eso propone sustituir la idea de “ciclo” por la de “sistema adaptativo”, en el que cada componente responde y se reconfigura frente al entorno.

¹⁸ El “ciclo de inteligencia” es el modelo clásico que describe el proceso mediante el cual los organismos de inteligencia transforman la información en conocimiento útil para la toma de decisiones. Tradicionalmente comprende cinco fases interdependientes (Kent, 1965): 1) *planificación*, que define los requerimientos de información y orienta las prioridades según los objetivos estratégicos; 2) *recolección*, que obtiene datos por medios humanos, técnicos o abiertos; 3) *procesamiento*, que organiza, valida y clasifica la información recolectada; 4) *análisis*, que interpreta e integra los datos procesados para producir conocimiento relevante, y 5) *difusión*, que comunica los productos de inteligencia a los niveles de decisión correspondientes para su aplicación en políticas, operaciones o estrategias. Aunque representado de manera secuencial, en la práctica el ciclo de inteligencia funciona como un proceso continuo y retroalimentado.

Michael Warner (2013) coincide al señalar que la inteligencia no puede representarse como una serie de pasos mecánicos, sino como un ecosistema de conocimiento que evoluciona mediante aprendizaje institucional y retroalimentación constante.

Y esta reconceptualización responde a transformaciones profundas en el entorno informacional, ya que en la era digital, el volumen, la velocidad y la veracidad de los datos desbordan cualquier proceso lineal. La información ya no fluye desde una fuente controlada hacia un centro de análisis, sino que se dispersa en redes interconectadas de sensores, plataformas y actores humanos, por lo que el desafío consiste hoy en integrar fuentes heterogéneas (tecnológicas, humanas, abiertas o clasificadas), en una arquitectura coherente que mantenga la calidad epistémica del conocimiento. Por ende, en este nuevo entorno, la actividad de la inteligencia se comporta como un sistema complejo adaptativo, caracterizado por la no linealidad, la emergencia y la autoorganización¹⁹.

Gill y Phythian (2013) propusieron la noción de una *web de inteligencia* para describir esta evolución. En lugar de un ciclo cerrado, la inteligencia moderna opera como una red de nodos interdependientes donde fluyen información, interpretación y retroalimentación. Cada nodo (una agencia, una célula analítica, una unidad de campo, un aliado extranjero), actúa de manera autónoma pero conectada, contribuyendo al aprendizaje colectivo. En esa red, la autoridad del conocimiento se distribuye y la producción analítica se convierte en un proceso colaborativo. La calidad del resultado depende menos de la jerarquía y más de la capacidad de interacción entre los nodos.

Este concepto de *web de inteligencia* introduce una serie de implicaciones epistemológicas relevantes. En primer lugar, la inteligencia se vuelve intrínsecamente inacabada, ya que el conocimiento siempre está en revisión, sujeto a nuevas evidencias y reinterpretaciones. En segundo lugar, el análisis deja de ser un acto individual y pasa a ser una práctica social, donde la coordinación interagencia y la integración multinivel son esenciales. En tercer lugar, la confianza (tanto entre instituciones como entre analistas), se convierte en el nuevo capital cognitivo de la

¹⁹ En la teoría de sistemas complejos, un *sistema adaptativo complejo* es aquel compuesto por múltiples agentes interconectados cuyas interacciones locales generan comportamientos globales imposibles de predecir a partir de las partes individuales. La *no linealidad* implica que pequeñas variaciones en la información o en las condiciones iniciales pueden producir efectos desproporcionados, lo que hace que el proceso de inteligencia no siga una secuencia causa-efecto estable. La *emergencia* se refiere a la aparición espontánea de patrones, estructuras o conocimientos colectivos que no estaban explícitos en los componentes iniciales, producto de la interacción entre analistas, datos y contextos. Finalmente, la *autoorganización* describe la capacidad del sistema para reconfigurarse sin dirección centralizada, ajustando sus flujos de información, jerarquías y procedimientos en función de la retroalimentación que recibe del entorno operativo (Luhmann, 2013).

comunidad de inteligencia. En una red, la fiabilidad de la información no depende solo de su fuente, sino del tejido relacional que garantiza su validación colectiva.

Richards (2013) profundiza esta idea al afirmar que el modelo clásico de ciclo encubre una tensión persistente entre la teoría y la práctica. En teoría, el ciclo sugiere orden, control y previsibilidad; en la práctica, la inteligencia es turbulenta, fragmentaria y negociada. Los analistas pedalean “cuesta arriba” en medio de presiones políticas, escasez de tiempo y competencia de narrativas. La metáfora de “pedalear con fuerza” que utiliza Richards expresa la necesidad de mantener el movimiento (de seguir produciendo conocimiento), a pesar de la falta de claridad total. En una red, la dinámica es más parecida al equilibrio inestable de un ciclista que al engranaje perfecto de una máquina.

Hulnick (2013) retoma esta crítica años después para plantear que la búsqueda de “mejores modelos” de inteligencia no debe centrarse en diagramas, sino en prácticas adaptativas. Lo que hace eficaz a un sistema de inteligencia no es su estructura formal, sino su capacidad para aprender, improvisar y comunicarse. La inteligencia útil es aquella que logra conectar la información correcta con la pregunta correcta en el momento oportuno. Este criterio, más que la fidelidad al ciclo, define la eficiencia epistémica del proceso.

El paso del *ciclo de inteligencia* a la *web/red* refleja también un cambio en la lógica del poder informacional. En la estructura jerárquica clásica, la información ascendía de los niveles operativos a los estratégicos; en la red contemporánea, los flujos son horizontales y multidireccionales (Tabla 3). Los analistas interactúan con diplomáticos, fuerzas militares, expertos civiles y aliados extranjeros en un intercambio continuo de datos y de significados. Este modelo exige, por lo tanto, un tipo de liderazgo cognitivo distinto: menos controlador y más integrador. La gestión del conocimiento estratégico se convierte así en una tarea de orquestación más que de comando.

Tabla 3. Comparación entre el modelo clásico del ciclo de inteligencia y el modelo contemporáneo de red adaptativa

Elemento	Modelo clásico (ciclo)	Modelo contemporáneo (red/web)	Implicación epistemológica
Estructura	Lineal y secuencial	Interactiva y dinámica	Del proceso cerrado al sistema abierto
Flujo de información	Vertical: del recolector al decisor	Multidireccional y en tiempo real	Del control jerárquico a la co-creación cognitiva

Continúa tabla...

Elemento	Modelo clásico (ciclo)	Modelo contemporáneo (red/web)	Implicación epistemológica
Rol del analista	Receptor y sintetizador	Nexo de intercambio y aprendizaje	Del procesamiento a la adaptación reflexiva
Retroalimentación	Ocasional (al final del ciclo)	Permanente y distribuida	Del producto final al proceso continuo
Tecnología y entorno	Entorno estable, flujo limitado de datos	Entorno digital, sobrecarga informacional	Del método lineal al análisis adaptativo
Objetivo principal	Informe o producto terminado	Resiliencia cognitiva y aprendizaje institucional	Del resultado al proceso evolutivo

Fuente: Elaboración propia con base en Hulnick (2006; 2013), Phythian (2013), Gill & Phythian (2013), Richards (2013) y Warner (2013)

La Tabla 3 evidencia que la inteligencia ha transitado de una lógica mecanicista a una lógica ecológica. Mientras el modelo clásico del ciclo de inteligencia representaba un proceso burocrático de transformación de información, el modelo de red de inteligencia propone un sistema de aprendizaje distribuido donde el conocimiento emerge de la interacción. Esta transformación no solo es organizacional, sino epistemológica, en la que la inteligencia deja de ser un flujo de productos para convertirse en un ecosistema de comprensión compartida.

Desde una perspectiva teórica, el modelo de red de inteligencia tiene afinidad con la noción de los sistemas complejos enunciada en las ciencias contemporáneas. Como ya se mencionó, un sistema complejo adaptativo se define por su capacidad de autoorganización, aprendizaje y respuesta emergente a estímulos del entorno. La comunidad de inteligencia se comporta de manera análoga; cada evento, amenaza o innovación tecnológica reconfigura su estructura y la obliga a reorganizar sus flujos de información y sus prioridades analíticas. Este carácter evolutivo explica por qué los intentos de estandarizar la inteligencia a través de manuales o protocolos rígidos suelen fracasar.

En la práctica colombiana, esta evolución también es evidente. El marco normativo de la Ley 1621 de 2013 reconoce explícitamente que la inteligencia y la contrainteligencia son funciones estatales complejas que requieren coordinación entre múltiples organismos. La existencia de una comunidad de inteligencia nacional, compuesta por dependencias de las Fuerzas Militares, la Policía Nacional y otras agencias especializadas, materializa esa red institucional. El reto permanente consiste en mantener la coherencia estratégica y la interoperabilidad técnica dentro de un ecosistema que crece y se diversifica.

La transición del ciclo lineal a la red adaptativa introduce asimismo un cambio en los indicadores de éxito, debido a que ya no se trata solo de producir informes precisos, sino de construir resiliencia cognitiva, es decir, la capacidad de un sistema para absorber la sorpresa, adaptarse rápidamente y aprender de sus errores. Esta resiliencia depende de tres factores interconectados: 1) la calidad de la comunicación inter agencial, 2) la cultura de aprendizaje y 3) la integración de la contrainteligencia como función transversal. Cuando alguno de estos elementos se debilita, el sistema se fragmenta y la ventaja estratégica se erosiona.

El modelo de red, por tanto, no reemplaza al ciclo, sino que lo complejiza. El ciclo sigue siendo una herramienta útil para la gestión operativa; la red, en cambio, representa el marco epistémico desde el cual entender la inteligencia en el siglo XXI. La inteligencia contemporánea se define menos por la linealidad de sus procesos que por la adaptabilidad de sus interacciones. En una época de sobreinformación, la coherencia no se logra mediante el control, sino mediante la coordinación y la confianza.

En suma, la transición del ciclo de inteligencia a la red de inteligencia marca el paso de una inteligencia burocrática a una inteligencia ecológica, capaz de operar en entornos cambiantes y saturados de información. Como concluye Warner (2013), “la inteligencia no es una serie de pasos, sino un diálogo continuo entre quienes buscan comprender y quienes deben actuar” (p. 34). Comprender ese diálogo es comprender la esencia de la inteligencia estratégica en la era de la complejidad.

La comprensión de la inteligencia como red adaptativa no solo redefine su estructura funcional, sino también su naturaleza epistemológica. En un entorno donde la información circula de manera caótica y los actores compiten por imponer su interpretación del mundo, conocer se convierte en una forma de poder y, al mismo tiempo, en una vulnerabilidad. Allí donde existe observación, también surge el intento de engañar al observador. Así, la actividad de la inteligencia se enfrenta a su propio espejo cognitivo, caracterizado por el engaño, la desinformación y las operaciones reflexivas que buscan alterar su percepción de la realidad. El siguiente apartado explora esta tensión fundacional entre conocimiento y manipulación, eje central de la *guerra cognitiva* (GC) contemporánea²⁰.

²⁰ La GC constituye una forma emergente de conflicto en la que el dominio de la mente y de los procesos de percepción se convierte en el principal campo de batalla. Su objetivo no es destruir físicamente al adversario, sino alterar su capacidad de pensar, decidir y actuar, mediante la manipulación de la información, las emociones y los significados compartidos. En este tipo de guerra, los blancos ya no son solo infraestructuras o ejércitos,

Inteligencia, engaño y guerra cognitiva

Toda práctica de inteligencia encierra una tensión constitutiva entre el conocimiento y la manipulación. Si su propósito es obtener información veraz para orientar la decisión, su reverso lógico consiste en negar o distorsionar la información del adversario. En este doble movimiento (buscar saber y evitar ser conocido), la inteligencia comparte el mismo terreno que el engaño. En consecuencia, la línea que separa la inteligencia de la desinformación no es ontológica, sino ética y estratégica. Clark y Mitchell (2019) sostienen que el engaño es un componente estructural del ciclo de inteligencia, por cuanto es un sistema de conocimiento que solo puede comprenderse plenamente si se incluye el *contraengaño*²¹ como su espejo cognitivo. Ningún servicio de inteligencia puede considerarse completo si no domina ambas dimensiones, es decir, tanto la búsqueda de la verdad como la detección del error inducido.

El engaño, entendido como el arte de inducir percepciones falsas en el adversario, opera dentro del mismo ecosistema informacional en el cual la actividad de inteligencia produce conocimiento. Su eficacia depende de parecer verosímil, de imitar los signos de la información legítima. Clark y Mitchell (2019) explican que el engaño exitoso no consiste en fabricar mentiras burdas, sino en manipular la verdad contextual, al presentar hechos ciertos en un marco falso. El engaño es, por ende, una ingeniería inversa del análisis de inteligencia; mientras el analista busca reducir incertidumbre, el engañador la amplifica deliberadamente para inducir un razonamiento erróneo.

Según Álvarez et al. (2018b), el engaño se concibe como un fenómeno estratégico y comunicacional mucho más amplio que la simple mentira; en efecto, distinguen que mentir implica únicamente la acción de quien enuncia una falsedad, mientras que engañar abarca a ambas partes, tanto el emisor y el receptor. El engaño se configura solo cuando la falsedad es creída, es decir, cuando la víctima internaliza la narrativa falsa como verdadera. Asimismo, destacan que el propósito del engañador no es evitar que su estrategia sea descubierta, sino lograr que la

sino los sistemas cognitivos de individuos y comunidades: su atención, memoria, confianza y sentido de realidad. Desde una perspectiva epistemológica, representa la evolución del conflicto hacia una fase en la que la información no solo se emplea como medio de guerra, sino como medio para redefinir la realidad (Henschke, 2025).

²¹ El término *counterdeception*, traducido como "contraengaño", designa el conjunto de procedimientos analíticos y operativos mediante los cuales la inteligencia detecta, interpreta y neutraliza los intentos de engaño del adversario. No se limita a la verificación factual, sino que implica comprender las motivaciones, técnicas y sesgos que sustentan la manipulación informativa (Clark & Mitchell, 2019).

falsedad sea aceptada durante el tiempo suficiente para alcanzar tres objetivos: 1) condicionar las creencias del adversario, 2) influir en sus acciones, y 3) beneficiarse de sus decisiones erróneas.

Desde esta perspectiva, el engaño puede adoptar dos tipos de variantes. El Tipo A (aumento de la ambigüedad), que busca generar confusión e incertidumbre mediante información contradictoria o incompleta, dificultando la interpretación de las verdaderas intenciones del actor. El Tipo M (*misleading*), que procura reducir la ambigüedad reforzando una alternativa falsa pero plausible, de modo que el adversario concentre sus recursos en una dirección equivocada. Álvarez et al. (2018) concluyen que el engaño es una práctica de *poder astuto*²², sustentada en la comprensión profunda de la cultura estratégica del adversario y en la manipulación de sus marcos de referencia cognitivos. En este sentido, el engaño no opera fuera del campo del conocimiento, sino dentro del mismo ecosistema informacional donde la misma inteligencia busca la verdad, actuando como su contraparte estructural y estratégica.

Rid (2020) sitúa esta lógica dentro de la genealogía de las *medidas activas* soviéticas, mostrando cómo el aparato de inteligencia de la Unión Soviética (URSS) combinó espionaje, propaganda y operaciones psicológicas (OPSIC) en un sistema de manipulación cognitiva transnacional. Las medidas activas no eran simples instrumentos de desinformación, sino estrategias cognitivas destinadas a erosionar la confianza del adversario en sus propias instituciones. El engaño operaba así en el plano epistemológico, ya que desestabilizaba la frontera entre lo verdadero y lo falso, creando un estado de ambigüedad que paralizaba la acción.

El término *medidas activas* (*aktivnyye meropriyatiya*) proviene de la terminología soviética de inteligencia y designaba un conjunto de operaciones encubiertas destinadas a influir en la percepción, comportamiento y toma de decisiones de gobiernos, organizaciones o sociedades extranjeras. A diferencia de la simple recolección de información (*inteligencia pasiva*), las medidas activas buscaban

²² Álvarez et al. (2018) definen el *poder astuto* como la capacidad estratégica de combinar de manera flexible y adaptativa las tres formas de poder: el poder duro, el poder blando y el poder agudo. El *poder duro* corresponde al uso de la coerción y de los recursos materiales (fuerza militar, sanciones económicas o presión política), para imponer comportamientos. El *poder blando* se basa en la atracción, la legitimidad y la capacidad de persuasión mediante valores, cultura e instituciones que generan adhesión voluntaria. El *poder agudo*, por su parte, describe las acciones encubiertas de manipulación informativa, desinformación e injerencia política destinadas a erosionar la confianza en las democracias y alterar percepciones sin recurrir a la fuerza abierta. El *poder astuto* no es simplemente una suma de estos componentes, sino una estrategia integral que ajusta su uso según el contexto y los objetivos, buscando la máxima eficacia con el mínimo costo político y cognitivo (Álvarez et al., 2018).

modificar la realidad política o cognitiva de un rival. Entre sus métodos más comunes se incluían desinformación (*dezinformatsiya*), propaganda encubierta, manipulación de medios y fuentes periodísticas, infiltración de movimientos sociales o académicos, apoyo a partidos o grupos ideológicamente afines, y falsificación de documentos o pruebas comprometedoras (Rid, 2020).

El término “activas” se utilizaba para subrayar que estas operaciones no se limitaban a observar o analizar, sino que también actuaban directamente sobre el entorno informacional y psicológico del enemigo, con el propósito de generar divisiones internas, desacreditar líderes, influir en la opinión pública o debilitar la cohesión de los Estados objetivo. Durante la Guerra Fría, el Departamento A del Primer Directorio Principal del Comité para la Seguridad Estatal (KGB), coordinaba estas acciones en estrecha relación con los servicios de inteligencia del bloque soviético, configurando un antecedente histórico directo de las actuales estrategias de desinformación digital y GC (Bertelsen, 2021).

En este orden de ideas, la literatura reciente ha confirmado que las actuales prácticas rusas de GC son una adaptación sofisticada de esa tradición soviética. Gioe et al. (2020) señalan que las actuales operaciones de desinformación digital rusas conservan la estructura cognitiva del modelo soviético de medidas activas, pero se ejecutan con nuevas tecnologías. Según estos autores, las medidas activas modernas combinan el espionaje, el ciberataque y la manipulación mediática en una forma de *contrapoder cognitivo* que busca alterar no solo los hechos, sino las interpretaciones colectivas de la realidad. En este contexto, el *contrapoder cognitivo* designa la capacidad de un actor estatal o no estatal para desafiar la hegemonía informacional del rival mediante operaciones que manipulan percepciones, emociones y significados colectivos (Tabla 4).

Tabla 4. Poder cognitivo vs. Contrapoder cognitivo

Dimensión	Poder cognitivo	Contrapoder cognitivo
Definición	Capacidad de influir positivamente en percepciones, valores y creencias para fortalecer la cohesión social, la legitimidad institucional y la orientación estratégica de un Estado o actor.	Capacidad de desafiar, distorsionar o subvertir los marcos cognitivos del adversario mediante manipulación informacional, emocional o semántica.
Finalidad estratégica	Construir consenso, confianza y resiliencia informacional.	Erosionar la confianza, generar ambigüedad y desestructurar la coherencia narrativa del oponente.

Continúa tabla...

Dimensión	Poder cognitivo	Contrapoder cognitivo
Mecanismo central	Comunicación persuasiva basada en credibilidad, transparencia y legitimidad.	Manipulación cognitiva basada en desinformación, engaño y explotación de sesgos perceptivos.
Instrumentos principales	Educación, diplomacia pública, medios institucionales, cultura estratégica y gestión ética de la información.	Ciberataques, operaciones psicológicas, propaganda emocional, ingeniería social, <i>troll farms</i> y <i>bots</i> automatizados.
Relación con la verdad	Busca fortalecer la comprensión compartida de la realidad a partir de hechos verificables.	Pretende alterar el marco interpretativo mediante verdades parciales o falsedades plausibles.
Efecto sobre la sociedad	Incrementa la cohesión cognitiva y la confianza en las instituciones.	Fragmenta la opinión pública, fomenta la polarización y debilita la deliberación racional.
Ejemplos históricos	Campañas de resiliencia informacional, alfabetización mediática, estrategias de diplomacia cultural.	Medidas activas soviéticas, campañas de desinformación digital, manipulación electoral o guerra narrativa en redes sociales.

Fuente: Elaboración propia a partir de Floridi (2010; 2015); Álvarez et al. (2018); Rid (2020); Bertelsen (2021a; 2021b) y Henschke (2025)

A diferencia del *poder cognitivo* (que busca construir consenso y legitimidad), el contrapoder cognitivo actúa de manera subversiva sobre sistemas de creencias y narrativas dominantes, empleando medios como la desinformación, el ciberataque, la propaganda emocional y la ingeniería social. En las medidas activas modernas, esta forma de poder no pretende solo alterar hechos, sino redefinir los marcos interpretativos desde los cuales la sociedad comprende la realidad, generando una asimetría cognitiva que debilita la cohesión y la confianza institucional del oponente. La inteligencia, en este contexto, deja de ser exclusivamente un proceso de obtención de información para convertirse en un instrumento de ingeniería de percepciones.

Hosaka (2020) complementa esta visión al analizar la contrainformación ofensiva soviética como antecedente directo de la desinformación rusa en Ucrania y Occidente. Su investigación muestra cómo el KGB empleaba medidas activas no solo para defenderse de la inteligencia occidental, sino para manipularla desde dentro. Esta contrainteligencia ofensiva perseguía un objetivo doble, desorganizar la capacidad de análisis del enemigo y forzarlo a construir interpretaciones erróneas a partir de fuentes genuinas. En términos modernos, se trataba de una forma de *control reflexivo* que transformaba la epistemología del adversario en su propio punto débil.

Magee (2023) amplía esta idea al reinterpretar las operaciones del KGB como un fenómeno de cisne negro de la contrainteligencia, es decir, sucesos imprevisibles generados por la intersección entre vigilancia, simulacro y autoengaño. Para

Magee (2023), la grandeza del engaño soviético residía en su capacidad de infiltrarse en los marcos cognitivos del adversario, no solo en sus redes de información; el enemigo no era engañado por la falta de datos, sino por exceso de confianza en su interpretación. Esta observación resulta clave para entender la vulnerabilidad contemporánea de las democracias hiperinformadas, pues cuando la inteligencia se apoya ciegamente en la abundancia de información, pierde sensibilidad ante la manipulación sutil de su propio aparato cognitivo.

En este punto se hace inevitable introducir el concepto de *control reflexivo*, formulado por teóricos militares soviéticos en los años setenta y sistematizado por Vladimir Lefebvre (Lefebvre, 1977), y analizado con profundidad por Thomas (2004). El control reflexivo es el proceso mediante el cual un actor induce a otro a tomar una decisión predeterminada al alterar su percepción del entorno. Thomas (2004) lo define como “la transmisión de información especialmente preparada para inclinar al adversario a tomar voluntariamente la decisión deseada por quien la emite” (p. 237). Es decir, el objetivo no es forzar físicamente la conducta del oponente, sino guiar su pensamiento hasta que elija (libremente) lo que conviene al manipulador. El control reflexivo se apoya en una comprensión dialéctica de la cognición heredada del materialismo soviético. Como demuestra Merriam (2023), esta doctrina se basa en la idea de que la mente humana refleja la realidad material a través de filtros perceptivos previsibles. Si estos filtros se conocen, pueden manipularse. En la práctica, el operador ruso modela la forma en que su adversario percibe el entorno (*reflexión informacional*) y cómo interpreta esa información (*reflexión cognitiva*)²³. Una vez comprendido el mapa mental del oponente, puede introducir señales, narrativas o estímulos que produzcan decisiones predecibles. Así, el enemigo no es engañado; es programado.

Merriam (2023) actualiza este marco mostrando cómo Rusia ha utilizado el control reflexivo en el siglo XXI, desde la guerra de Georgia (2008) hasta la invasión de Ucrania (2022), para inducir a los gobiernos y las organizaciones occidentales a tomar decisiones desfavorables. En el caso georgiano, Moscú fabricó una situación de provocación controlada que llevó al presidente Saakashvili a iniciar

²³ En la teoría del control reflexivo desarrollada por la escuela soviética de psicología militar (Lefebvre, 1977), la *reflexión informacional* se refiere al proceso mediante el cual un actor modela o anticipa la información disponible para su adversario, es decir, cómo este percibe los datos y señales del entorno. Implica diseñar los flujos informativos (reales o falsificados), que condicionan la percepción inicial del oponente. Por su parte, la *reflexión cognitiva* alude al nivel superior del proceso, en el que se manipulan los esquemas mentales, valores, expectativas o marcos interpretativos a través de los cuales el adversario procesa esa información. En conjunto, ambas dimensiones permiten inducir decisiones “voluntarias” pero controladas, al influir tanto en los insumos perceptivos como en los mecanismos internos de interpretación del enemigo (Thomas, 2004).

el conflicto, legitimando la posterior invasión rusa. Lo mismo ocurrió en Ucrania con la acumulación de tropas rusas antes de febrero de 2022, en donde más que ocultar la invasión, la estrategia consistía en saturar el entorno informacional con señales ambiguas que paralizaran la respuesta occidental.

Según Merriam (2023), el control reflexivo combina dos formas de manipulación: la constructiva y la destructiva. La primera crea una imagen falsa de la realidad para inducir decisiones específicas; la segunda destruye la capacidad del adversario para percibir la realidad auténtica. En la práctica, ambas se complementan, ya que una edifica una narrativa atractiva mientras la otra sabotea los sistemas de información que podrían refutarla. Por consiguiente, la construcción de un "teatro cognitivo" implica no solo alterar los datos, sino diseñar emociones y sesgos que garanticen la adhesión del objetivo al marco manipulado. Thomas (2004) afirma que esta técnica se articula con la doctrina militar rusa de *maskirovka*, la ocultación y el engaño como principios tácticos y estratégicos. En la visión rusa, el engaño no es un acto marginal, sino un principio de guerra, debido a que la sorpresa no se logra solo con el movimiento de fuerzas, sino con la manipulación de la mente enemiga. Este principio, traducido al ámbito digital contemporáneo, convierte al ciberespacio en el nuevo escenario de *maskirovka* cognitiva²⁴.

Hosaka (2020) demuestra que el control reflexivo ya se practicaba en la Guerra Fría como componente de las operaciones de contrainteligencia ofensiva soviética, en donde las agencias occidentales eran alimentadas con información parcialmente veraz para inducir interpretaciones deseadas. En lugar de ocultar, se mostraba demasiado, configurando un espejo deformado donde el adversario se veía a sí mismo actuando racionalmente mientras servía al propósito del otro. No obstante, en el entorno digital contemporáneo, el control reflexivo ha adquirido una dimensión algorítmica, en la cual las operaciones rusas ya no se limitan a los servicios de inteligencia tradicionales, sino que se extienden a redes sociales, *bots* y plataformas mediáticas.

²⁴ El término *maskirovka* ("camuflaje" o "disimulo") designa la doctrina soviética, y posteriormente rusa, de engaño militar integral, concebida como la coordinación sistemática de medidas destinadas a ocultar las verdaderas intenciones y capacidades propias mientras se induce una interpretación errónea en el adversario. Más que simples operaciones de camuflaje, la *maskirovka* abarca un amplio espectro de acciones que combinan ocultamiento físico, engaño operacional, desinformación estratégica, simulación táctica y operaciones psicológicas. Sus raíces se remontan a las prácticas de engaño del Ejército Rojo en la Segunda Guerra Mundial, donde resultó decisiva en batallas como Kursk o la ofensiva de Berlín (Thomas, 2004). En su versión contemporánea, la *maskirovka* integra elementos de guerra electrónica, manipulación mediática, ciber operaciones y operaciones de influencia, funcionando como un mecanismo de control reflexivo destinado a alterar la percepción del adversario y su proceso de toma de decisiones. En la doctrina rusa moderna, el concepto conserva su carácter holístico, ya que es una "estrategia de ambigüedad" que combina ocultamiento, distracción y saturación informacional para lograr efectos cognitivos que preceden y condicionan la acción militar directa (Giles, 2016).

Merriam (2023) y Gioe et al. (2020) coinciden en que el objetivo de estas campañas no es tanto convencer como reflexionar la psicología del adversario; en otras palabras, observar cómo piensa y luego inducirlo a reproducir sus propias creencias de manera que beneficien a Rusia. El resultado sería, por lo tanto, un proceso de “automanipulación asistida” donde el individuo o la sociedad actúan contra sus intereses creyendo hacerlo libremente. Por su parte, Magee (2023) sostiene que esta forma de manipulación convierte la contrainteligencia en un ejercicio de metacognición, en donde la defensa ya no consiste en detectar mentiras, sino en comprender cómo se construyen las verdades. En un mundo donde los datos son infinitos y la atención es finita, el poder radica en controlar los filtros cognitivos. La GC, vista desde esta perspectiva, ya no busca destruir la información, sino modelar la mente que la interpreta.

Merriam (2023) propone una respuesta estratégica frente al control reflexivo, al sostener que su diagnóstico exige comprender la epistemología del adversario, es decir, los supuestos cognitivos, perceptivos y culturales desde los cuales construye y manipula la información. Solo al conocer cómo el oponente concibe el proceso de conocer y decidir es posible anticipar o neutralizar su capacidad de inducir decisiones a través de la manipulación cognitiva. En consecuencia, es necesario estudiar los marcos conceptuales rusos (su teoría de la decisión, su visión sistémica y su herencia dialéctica), para anticipar sus movimientos cognitivos; no se trata de “pensar como ellos”, sino de reconocer que el juego se libra en la mente.

De ahí la necesidad de desarrollar capacidades de *contra-reflexión*²⁵ o, dicho de otra manera, mecanismos de análisis que permitan detectar cuándo las propias decisiones han sido anticipadas por el adversario. Por lo tanto, este enfoque conecta directamente con la función contemporánea de la actividad de la inteligencia en la GC, relacionada con la *vigilancia epistémica*²⁶, en donde el analista ya no solo

²⁵ La *contra-reflexión* puede entenderse como la capacidad cognitiva y organizacional destinada a detectar, anticipar y neutralizar intentos de control reflexivo por parte del adversario. Consiste en un proceso metacognitivo mediante el cual la inteligencia analiza no solo la información entrante, sino también cómo sus propios procesos de análisis y decisión pueden estar siendo observados o inducidos. En términos operativos, implica la creación de bucles de retro análisis que comparan patrones de comportamiento propios con los posibles modelos predictivos del enemigo, buscando indicios de manipulación informacional o cognitiva. Su finalidad es restaurar la autonomía decisional frente a adversarios capaces de anticipar reacciones mediante operaciones de percepción estratégica (Thomas, 2004; Merriam, 2023).

²⁶ El concepto de *vigilancia epistémica* proviene de la psicología cognitiva (Sperber et al., 2010), y se refiere a la facultad de evaluar la confiabilidad de la información y de las fuentes desde las cuales se forma el conocimiento. En el ámbito de la inteligencia, se traduce en la capacidad institucional de supervisar la calidad del razonamiento analítico, los sesgos cognitivos y las dinámicas grupales que afectan la producción de conocimiento estratégico. Aplicada a la GC, la vigilancia epistémica implica que el analista no solo analiza el entorno

observa el entorno externo, sino que monitorea la integridad cognitiva de su propia comunidad decisional. En la práctica, esto significa integrar disciplinas como la psicología cognitiva, la semiótica, la inteligencia artificial y la sociología de la información en los procesos de producción analítica.

En resumen, el control reflexivo y las medidas activas revelan que el campo de batalla contemporáneo no es solo informacional, sino epistemológico. El objetivo ya no es destruir la infraestructura del enemigo, sino desorganizar su coherencia mental. En ese sentido, la GC es una prolongación natural de la inteligencia estratégica, pues ambas se fundan en la gestión del conocimiento. Por consiguiente, Clark y Mitchell (2019) afirman que el verdadero poder de la inteligencia reside en su capacidad de entender el pensamiento del adversario antes que él mismo. El control reflexivo lleva esa lógica al extremo: manipula el pensamiento antes de que se produzca (Tabla 5).

Tabla 5. *Tipos de engaño y mecanismos cognitivos en la inteligencia contemporánea*

Tipo de engaño o medida	Objetivo estratégico	Mecanismo cognitivo	Ejemplo histórico o contemporáneo	Autor / Fuente
Decepción clásico (engaño)	Desviar atención o disfrazar intención real	Ocultamiento/ disimulo	<i>Operation Fortitude</i> (1944) - Engaño aliado previo al Día D	Clark y Mitchell (2019)
Medidas activas soviéticas	Erosionar confianza en instituciones rivales	Saturación informacional/ manipulación mediática	Campañas KGB en Occidente (Guerra Fría)	Rid (2020); Hosaka (2020)
Contrainteligencia ofensiva	Manipular al enemigo desde dentro de su sistema analítico	Inyección controlada de información parcialmente veraz	<i>Operation Trust</i> (1921-1926)	Hosaka (2020); Magee (2023)
Control reflexivo	Inducir decisiones predeterminadas	Alteración de percepciones y marcos mentales	Guerra ruso-georgiana (2008); Ucrania (2014-2022)	Thomas (2004); Merriam (2023)
Desinformación digital	Construir realidades alternativas y polarización social	Explotación algorítmica de emociones y sesgos	Interferencias electorales globales	Gioe et al. (2020); Van Herpen (2021)
Contra-reflexión	Diagnosticar y resistir la manipulación cognitiva	Autoconciencia institucional y metainteligencia	Estrategias OTAN de resiliencia cognitiva	Magee (2023); Merriam (2023)

Fuente: Elaboración propia

externo, sino que también monitorea las vulnerabilidades cognitivas internas de su propia comunidad decisional. Esto convierte a la inteligencia en un sistema reflexivo que protege su coherencia interpretativa frente a la manipulación, la desinformación o la sobreexposición informacional.

En la era digital, esta dinámica se amplifica. Los algoritmos de recomendación y los ecosistemas de datos se han convertido en instrumentos de control reflexivo automatizado, capaces de ajustar las percepciones colectivas en tiempo real. Así, la *maskirovka* de la era soviética ha evolucionado en una *maskirovka* de datos, donde la falsedad ya no se impone desde afuera, sino que emerge de los propios hábitos informativos de las sociedades abiertas. La Tabla 5 permite visualizar la continuidad histórica y la innovación técnica del engaño en la práctica de inteligencia. Desde la *maskirovka* hasta el control reflexivo contemporáneo, el eje constante es la manipulación de los procesos cognitivos del adversario. En la era digital, el engaño ya no busca solo desinformar, sino moldear el pensamiento y la percepción, configurando así la esencia de la GC.

La evolución conceptual del engaño y de la manipulación cognitiva encuentra un eco directo en las reflexiones contemporáneas sobre el poder. En la obra de Álvarez et al. (2018), la noción de poder astuto amplía la comprensión tradicional del poder estratégico y ofrece un marco útil para entender la dimensión cognitiva de la inteligencia. Su enfoque describe un tipo de influencia que opera en el terreno de la percepción, donde la información se convierte en materia prima del control. El poder astuto no busca imponer la voluntad ni seducir al otro de manera explícita, sino modificar el entorno cognitivo en el que se toman las decisiones. En este sentido, la GC y el engaño comparten la misma lógica, pues ambos intervienen en la formación del juicio del adversario. La actividad de inteligencia, cuando actúa bajo esta lógica, deja de ser únicamente un instrumento de revelación para convertirse en una herramienta de modelación semántica capaz de alterar el marco mental desde el cual se interpreta la realidad.

Álvarez et al. (2018) entienden este poder como una forma de control estratégico propio de la era de información y la hiperconectividad²⁷. Su eficacia depende de la capacidad para gestionar la incertidumbre y combinar lo visible e invisible, lo verdadero y falso, dentro de un mismo relato. Desde esta perspectiva, el engaño no es una práctica marginal sino un componente esencial del poder astuto, una forma de inteligencia ofensiva que actúa sobre la mente y no sobre la materia. La GC representa así la manifestación más avanzada de este nuevo tipo de poder, ya que no busca destruir físicamente al enemigo sino condicionar su interpretación

²⁷ Álvarez et al. (2018) definen el poder como la capacidad de un actor para modificar el comportamiento, la percepción o la voluntad de otro mediante el control del flujo de información, de las narrativas y de los significados en el entorno estratégico. Desde esta perspectiva, el poder no se limita a la coerción o la persuasión, sino que actúa sobre la dimensión cognitiva de la realidad, configurando las condiciones bajo las cuales los sujetos interpretan el mundo.

del mundo. Allí donde la inteligencia tradicional perseguía la verdad, la inteligencia en la era del poder astuto busca también administrarla, comprendiendo que el conocimiento, cuando se gestiona estratégicamente, puede transformarse en un instrumento de dominio perceptual.

Esta concepción complementa los enfoques contemporáneos sobre la inteligencia y el control reflexivo, ya que integra el plano del conocimiento con el del poder simbólico. Si el control reflexivo intenta inducir decisiones específicas en el adversario, el poder astuto aspira a un dominio más profundo, el del sentido mismo que da coherencia a la realidad. En este punto, la inteligencia y la estrategia confluyen en un mismo espacio cognitivo donde conocer, influir y engañar son manifestaciones distintas de una misma lógica de poder.

La convergencia entre el poder simbólico y el conocimiento estratégico redefine la naturaleza misma de la inteligencia. En la GC, influir y conocer son operaciones simultáneas, por cuanto comprender al adversario implica también afectar su modo de comprender. Esta circularidad convierte la inteligencia en un sistema reflexivo donde cada observador es, a la vez, observado y modelado. Por ello, la evolución de la inteligencia en el siglo XXI exige un enfoque epistemológico capaz de examinar no solo cómo se obtiene la información, sino cómo se construye el sentido. En este tránsito, la inteligencia se transforma de una práctica instrumental a una disciplina interpretativa que opera en el corazón de la infosfera.

Hacia una epistemología de la inteligencia en la era cognitiva

Hablar de una *epistemología de la inteligencia* implica reconocer que esta no solo produce información sobre el mundo, sino también marcos de interpretación que configuran la manera en cómo ese mundo es finalmente comprendido. La inteligencia, en tanto forma institucionalizada de conocimiento estratégico, posee su propia lógica de la verdad, sus métodos de validación y sus sesgos inherentes. En la era cognitiva, esta reflexión se vuelve indispensable, debido a que la cuestión ya no es únicamente *qué se sabe*, sino *cómo se sabe* y *con qué propósito se organiza el saber*. De este modo, la epistemología de la inteligencia examina las condiciones de posibilidad, los límites y los riesgos del conocimiento producido en contextos donde la percepción y la decisión se han convertido en campos de batalla.

La inteligencia contemporánea ha dejado de ser una práctica confinada al espionaje o a la obtención de secretos. Es, ante todo, un sistema de conocimiento estratégico que opera dentro de la infosfera, donde la información, la percepción y el poder se entrelazan de manera inseparable. La evolución teórica revisada hasta

el momento muestra una transformación epistemológica, en la cual la inteligencia ha pasado de ser una técnica de observación a constituirse en una ciencia de la interpretación. En la era cognitiva, su función esencial es gestionar el significado en un entorno saturado de datos y vulnerado por la manipulación informacional.

Desde la teoría filosófica de la información de Floridi (2011; 2015), se comprende que la inteligencia se asienta sobre una ontología relacional. Los datos no existen de manera independiente, ya que adquieren sentido solo cuando un sujeto los interpreta dentro de un contexto. El valor epistémico de la información se mide, en consecuencia, por su capacidad de reducir la incertidumbre y aumentar la conciencia situacional. En ese proceso, la actividad de inteligencia funciona como un dispositivo de traducción semántica entre la realidad y la decisión. Su finalidad no es acumular conocimiento, sino transformar la información dispersa en comprensión orientada a la acción. Miller (2022) reafirma que la inteligencia persigue el ideal de la *creencia verdadera justificada*. Un analista solo puede afirmar que “sabe” algo cuando su juicio se apoya en evidencias verificables, métodos confiables y competencia técnica en su aplicación. Esta distinción entre la mera creencia y el conocimiento auténtico delimita la frontera entre información y comprensión estratégica. Así, la epistemología de la inteligencia se apoya en un principio normativo en el cual no todo lo verdadero es conocimiento, y solo el juicio fundamentado institucionalmente (esto es, aquel que puede ser defendido con razones), constituye un conocimiento legítimo.

Frente a esta visión relacional y constructivista, Mandrick y Smith (2022) proponen un *realismo ontológico* como fundamento filosófico de la actividad de inteligencia. Según estos autores, la coherencia y la utilidad del conocimiento estratégico dependen de que los sistemas informacionales se estructuren a partir de categorías que reflejen la realidad misma, y no solo interpretaciones subjetivas que se hacen de ella. Por ende, la epistemología de la inteligencia debe equilibrar la interpretación cognitiva con la correspondencia ontológica, ya que comprender el mundo también requiere poder representarlo de forma consistente²⁸.

La teoría del conocimiento estratégico, articulada por Kent (1965), Herman (1996), Heuer (1999) y Lowenthal (2022), complementa esta base ontológica al subrayar el carácter aplicado de la inteligencia. Su propósito es reducir la fricción y producir una ventaja de decisión. La inteligencia es, en esencia, conocimiento

²⁸ Así, el *realismo ontológico* actúa como un correctivo frente a la entropía informacional, garantizando interoperabilidad, trazabilidad y sentido en el conocimiento producido.

con propósito, saber que guía la acción bajo condiciones de incertidumbre. Pero, como señalan MacGaffin y Oleson (2015), esta ventaja solo se consolida cuando se acompaña de la confianza de decisión, es decir, la confianza racional en la validez del propio juicio. La epistemología de la inteligencia no se define solo por la búsqueda de la verdad, sino por la construcción de certeza operacional.

Gill (2010) y Wirtz (2010) aportan una dimensión metodológica a este proceso al situar la inteligencia dentro de un campo intermedio entre la ciencia y el arte. El conocimiento estratégico no puede verificarse en términos experimentales, aunque sí puede evaluarse por su coherencia y su eficacia decisoria. Como advierte Rønn (2022), esta evaluación no puede apoyarse en una noción de objetividad entendida como neutralidad absoluta. En la práctica de la inteligencia, la objetividad no es ausencia de interpretación, sino transparencia sobre las condiciones y límites de esa interpretación²⁹. En este sentido, al ser una ciencia práctica de la incertidumbre que combina evidencia empírica, inferencia analítica y juicio experto, la inteligencia se aproxima a la epistemología pragmática, en la que la verdad es aquello que resulta útil y permite actuar de manera eficaz. De ahí que la objetividad absoluta sea un ideal inalcanzable; lo que se busca es una intersubjetividad disciplinada, una convergencia de interpretaciones bien fundadas.

La crítica contemporánea al modelo lineal del ciclo de inteligencia (Hulnick, 2006; Phythian, 2013; Gill & Phythian, 2013), introduce la noción de complejidad como principio organizador. La inteligencia ya no puede concebirse como una secuencia cerrada de etapas, sino como una red adaptativa de producción de conocimiento. Esta red o web de inteligencia, se asemeja a un sistema complejo adaptativo donde cada componente interactúa, aprende y se retroalimenta. El conocimiento no fluye de manera vertical, sino horizontal, y se construye colectivamente mediante la integración de múltiples perspectivas. La epistemología de la inteligencia, por tanto, es también una epistemología de la red, en el que el saber emerge de la interacción.

Miller (2022) amplía esta noción al describir la inteligencia como una forma de acción epistémica colectiva. Según Miller, las agencias de inteligencia son instituciones epistémicas, cuya función consiste en coordinar conocimientos parciales,

²⁹ Rønn (2022) identifica cinco concepciones de objetividad en la comunidad de inteligencia (interpretación-libre, libre de valores, neutral, desapegada y justa), proponiendo una síntesis denominada "objetividad reflexiva", basada en la capacidad del analista para reconocer sus propios marcos de referencia y exponerlos críticamente. Desde esta perspectiva, la objetividad se convierte en una virtud epistémica situada, más cercana a la honestidad intelectual que al distanciamiento científico. Así, la práctica analítica gana en legitimidad precisamente cuando reconoce su carácter interpretativo.

validar inferencias y producir juicios compartidos que puedan orientar la acción política o militar. Este enfoque reconoce que el conocimiento estratégico no emerge de un individuo aislado, sino de un entramado cooperativo de analistas, mandos y sistemas técnicos. En tal estructura, la responsabilidad epistémica es compartida, pero también jerárquica, en el que cada nivel del sistema participa en la construcción y en la rendición de cuentas del saber institucional.

Este paso de la linealidad a la complejidad refleja la evolución de la inteligencia desde un paradigma mecanicista hacia uno ecológico. La inteligencia moderna se comporta como un ecosistema cognitivo que combina tanto tecnología como análisis humano y coordinación institucional. Su eficacia depende menos de la cantidad de información procesada que de la resiliencia del sistema para adaptarse a lo inesperado. En la era digital, el aprendizaje continuo y la capacidad de detectar retroalimentaciones adversas son indicadores de madurez epistémica. Un sistema de inteligencia eficaz es aquel que aprende más rápido que su adversario.

Por su parte, la relación entre la inteligencia, engaño y GC muestra la contracara de este proceso. La misma estructura informacional que permite conocer al mundo puede ser utilizada para manipularlo. Las teorías del engaño y del control reflexivo demuestran que el conocimiento estratégico es, a la vez, arma y blanco. La inteligencia, que en su sentido clásico buscaba la verdad, debe ahora defenderla. El adversario contemporáneo no solo oculta información, también fabrica realidades. La GC no busca destruir la infraestructura física del enemigo, sino colonizar su mente, perturbar su coherencia y erosionar su confianza.

El control reflexivo, formulado por Lefebvre (1977) y sistematizado por Thomas (2004) y Merriam (2023), revela la profundidad epistemológica del conflicto moderno. Quien domina la percepción del otro, domina su decisión. El objetivo ya no es vencer militarmente, sino inducir cognitivamente. En este contexto, la inteligencia se convierte en el órgano que protege la soberanía cognitiva del Estado, es decir, su capacidad de pensar por sí mismo. Por ende, defender la autonomía del juicio se vuelve un imperativo estratégico.

De ahí que la nueva frontera de la inteligencia sea la *metainteligencia*, es decir, la capacidad de observar y evaluar sus propios procesos cognitivos. Magee (2023) y Hosaka (2020) muestran cómo el contra engaño moderno implica un ejercicio de autoconciencia institucional, lo cual significa identificar cuándo los propios análisis han sido moldeados por el adversario, cuándo las certezas se han convertido en vulnerabilidades. Esta dimensión reflexiva convierte a la inteligencia en un sistema autorregulado de vigilancia epistémica.

Al integrar estos enfoques, se advierte que la inteligencia contemporánea se encuentra en un punto de convergencia entre tres paradigmas: el informacional, el estratégico y el cognitivo. El paradigma informacional (Floridi, 2010; Johnson, 2010) define la ontología del entorno, es decir, la infosfera como campo de interacción entre datos, agentes y significados. El paradigma estratégico (Kent, Herman, Lowenthal, Heuer) otorga finalidad y dirección, entendiendo la inteligencia como conocimiento aplicado a la toma de decisiones. y el paradigma cognitivo (Thomas, 2004; Rid, 2020; Bertelsen, 2021a; Merriam, 2023) introduce el nuevo dominio de la confrontación, la mente como espacio de poder (Tabla 6).

Tabla 6. Paradigmas epistemológicos de la inteligencia en la era cognitiva

Paradigma	Nivel de análisis	Objetivo de conocimiento	Tipo de racionalidad	Riesgo epistémico	Autores representativos
Informacional	Ontológico	Comprender los flujos de datos y su valor semántico dentro de la <i>infosfera</i>	Racional-técnica	Sobrecarga o falsificación de la información (entropía informacional)	Floridi (2010, 2015); Johnson (2010)
Estratégico	Político / institucional	Transformar información en ventaja de decisión y confianza racional	Pragmática	Sesgo de confirmación, politización o uso instrumental del análisis	Kent (1965); Herman (1996); Lowenthal (2022)
Cognitivo	Epistemológico / cultural	Proteger y modelar la percepción, el juicio y la narrativa nacional	Reflexiva y adaptativa	Manipulación mental, control reflexivo o desinformación sistémica	Thomas (2004); Rid (2020); Merriam (2023); Bertelsen (2021b)

Fuente: Elaboración propia

La articulación de estos tres niveles configura una epistemología de la inteligencia en la era cognitiva. En ella, el conocimiento estratégico se concibe como un proceso adaptativo, relacional y ético. Adaptativo, porque opera en entornos inciertos y cambiantes; relacional, porque depende de la interacción entre múltiples actores y niveles de análisis; ético, porque la manipulación informacional plantea dilemas sobre la legitimidad del poder cognitivo. La Tabla 6 sintetiza la evolución teórica revisada en el marco: de la información como sustancia, al conocimiento como acción y la cognición como dominio de conflicto. Cada paradigma aporta una forma distinta de racionalidad, pero todos confluyen en un mismo fin, el cual es preservar la coherencia epistémica del Estado frente a la entropía informacional y la manipulación cognitiva.

Desde esta perspectiva, la función de la inteligencia en el siglo XXI no se limita a informar decisiones; consiste en preservar la coherencia epistemológica del

Estado frente a la entropía informacional. Entonces, su misión es doble: conocer y proteger el conocimiento. En el plano externo, esto significa anticipar amenazas y comprender la lógica del adversario; en el plano interno, implica mantener la confianza del sistema político y social en la validez de la información que lo orienta. La inteligencia, en consecuencia, no solo actúa sobre la realidad, sino sobre la percepción de la realidad.

La GC lleva esta exigencia a su máxima expresión. Si el control del territorio definió las guerras industriales y el control de la información definió las guerras tecnológicas, el control de la percepción define las guerras cognitivas. En ellas, la superioridad no depende de la fuerza ni de los recursos, sino de la capacidad para construir sentido. La victoria ya no se mide por la destrucción del enemigo, sino por la imposición de una interpretación del mundo. La inteligencia, en este nuevo escenario, es el núcleo del poder semiótico del Estado. Por ello, la epistemología de la inteligencia en la era cognitiva debe orientarse hacia tres principios: 1) *integridad semántica*: garantizar la veracidad y coherencia de la información que sostiene la toma de decisiones; 2) *resiliencia cognitiva*: desarrollar mecanismos institucionales que permitan resistir y adaptarse a la manipulación informacional; y 3) *transparencia estratégica*: comunicar de manera veraz y oportuna, fortaleciendo la confianza social como antídoto frente a la desinformación.

En síntesis, el recorrido teórico desarrollado demuestra que la inteligencia es el puente entre información y poder, entre conocimiento y acción. Su evolución epistemológica la ha llevado del secreto a la comprensión, del espionaje a la cognición. En un mundo donde la información es abundante pero la verdad escasa, la inteligencia se convierte en el último guardián del juicio. Su campo de batalla no está en el espacio físico, sino en el dominio invisible del sentido. Allí, en la defensa de la coherencia cognitiva y la libertad de interpretación, se juega hoy la seguridad nacional del Estado.

Comprender la inteligencia en su dimensión epistemológica permite ahora rastrear sus raíces históricas. Antes de convertirse en un sistema formal de conocimiento estratégico, la inteligencia fue una práctica intuitiva del poder, un arte de conocer al enemigo y anticipar sus movimientos. A lo largo de los siglos, los imperios, ejércitos y Estados han desarrollado mecanismos para observar, interpretar y decidir bajo incertidumbre, sentando las bases de lo que hoy se entiende como ciclo de inteligencia. En esta trayectoria, la búsqueda de ventaja informacional precedió a toda institucionalización, revelando que la esencia de la inteligencia no reside en la tecnología ni en el secreto, sino en la capacidad humana de convertir la información en comprensión útil para la acción.

Los orígenes de la inteligencia: la información como conocimiento estratégico

La *inteligencia* ha sido definida de múltiples maneras, como conocimiento, como proceso, como producto, como organización y como actividad; sin embargo, en su sentido más primario, la inteligencia equivale a conocimiento. Según Lowenthal (2022), la información es todo lo que puede conocerse, sin importar cómo se obtenga, mientras que la inteligencia se refiere a aquella información que ha sido recopilada, procesada y analizada para satisfacer las necesidades de los responsables de la toma de decisiones. En este sentido, la información debe transformarse mediante el análisis antes de adquirir valor estratégico; de ahí que, en su fórmula más sencilla, pueda afirmarse que $\text{inteligencia} = \text{información} + \text{análisis}$.

McDowell (2009) añade que la inteligencia no consiste en una simple acumulación de datos, sino en un proceso sistemático de integración, evaluación y estimación cuyo propósito es anticipar escenarios futuros; por ende, su función esencial no es solo reducir la incertidumbre, sino también brindar confianza a los decisores. En esta línea, Kent (1965) señalaba que la inteligencia estratégica representa el conocimiento que los líderes necesitan para salvaguardar la seguridad nacional, articulando así la relación entre conocimiento y acción. Keegan (2003) observó que todos los servicios de inteligencia nacieron del esfuerzo por evitar que el enemigo obtuviera una ventaja militar; es decir, la inteligencia existe para proporcionar ventaja, pero también seguridad psicológica en la toma de decisiones.

Antes de institucionalizarse como práctica estatal, la inteligencia fue una extensión cognitiva de la supervivencia humana. Desde los grupos nómadas que aprendieron a observar los patrones del entorno hasta las primeras civilizaciones que registraron los movimientos de sus enemigos, la función esencial de la inteligencia fue siempre la de anticipar lo incierto. En su forma más elemental, la inteligencia constituye un mecanismo adaptativo mediante el cual las comunidades humanas aprendieron a identificar señales relevantes, descartar el ruido del entorno y proyectar escenarios probables. Este proceso (basado en observación, memoria colectiva e inferencia), puede entenderse como el primer sistema adaptativo de producción de conocimiento estratégico.

Según Andrew (2018), mucho antes de la aparición del Estado moderno, los reinos y otros tipos de gobiernos antiguos organizaron prácticas sistemáticas para ver más allá del horizonte inmediato. De los archivos asirios y los escribas egipcios a los mensajeros persas y los informantes hebreos, la inteligencia aparece como un

“saber de gobierno” embrionario cuyo objetivo constante fue reducir la incertidumbre política y militar. Para Andrew (2018), las civilizaciones que perduraron fueron precisamente aquellas capaces de convertir la observación en rutina institucional y la memoria en archivo, inaugurando un ciclo recurrente de obtención, evaluación y consejo al soberano que prefigura el análisis estratégico contemporáneo.

El primer analista de inteligencia pudo haber sido un cazador prehistórico que luego de una actividad de reconocimiento regresó a su cueva y entregó a los miembros de su clan familiar una evaluación de las capacidades de fuerza con las que contaban un clan vecino (por ejemplo, cuántos guerreros había, con qué armas contaban, cuál era la naturaleza del terreno intermedio entre su cueva y la del potencial adversario, etc.). Esa observación directa, basada en la experiencia y el contacto humano, constituye la forma más antigua de lo que hoy se conoce como HUMINT³⁰, es decir, la obtención de información mediante fuentes humanas. Probablemente se le pidió después que evaluara cual podría ser la probabilidad de éxito de un ataque de su clan o la probabilidad que pudiese presentarse un ataque del rival (McDowell, 2009). Por lo tanto, la observación, la inferencia y la anticipación constituyeron las primeras formas de análisis, en donde ver, escuchar y comunicar ya eran verbos esenciales del mando. La mente humana, dotada de la tendencia natural a establecer nexos causales, convirtió la información sensorial en conocimiento útil para la acción. La inteligencia nació así, como una extensión del instinto de supervivencia, un modo de eliminar la incertidumbre y controlar el entorno, base de toda estrategia posterior.

La primera evidencia escrita de una actividad organizada de inteligencia proviene de la antigua Mesopotamia. Unas tablillas descubiertas en el palacio de Mari, fechadas alrededor de 1800 a.C., documentan una red de mensajeros y observadores encargados de vigilar las fronteras, informar sobre movimientos de tribus nómadas e interceptar señales de fuego entre aldeas. Uno de esos mensajes, dirigido al rey por un oficial llamado *Bannum*, advertía de señales sospechosas entre los benjamitas y sugería reforzar la guardia y permanecer en el palacio (Sheldon, 2011). Este simple informe revela una estructura elemental de inteligencia, basada en la observación, la transmisión y la recomendación. El conocimiento dejó de ser

³⁰ HUMINT (*Human Intelligence*), designa la inteligencia obtenida a partir de fuentes humanas mediante la observación directa, el interrogatorio, la infiltración o la cooperación con informantes. Constituye la forma más antigua de recolección de información y sigue siendo esencial incluso en la era tecnológica, pues permite captar intenciones, percepciones y contextos que los sensores técnicos no registran. Según Lowenthal (2022), la HUMINT se basa en la interpretación de la conducta humana más que en la medición de señales, lo que la convierte en un instrumento insustituible para comprender la dimensión cognitiva de la seguridad y la guerra.

fortuito para volverse organizado, y el poder político comenzó a depender directamente de su circulación.

En Oriente, la inteligencia alcanzó pronto un grado de sofisticación filosófica. En el siglo V a.C., Sun Tzu (2008) formuló el principio eterno de la inteligencia: “Conócete a ti mismo y conoce a tu enemigo, y en cien batallas nunca estarás en peligro” (p. 84). En esta máxima se condensa una visión total de la estrategia: la guerra no se libra únicamente en el terreno físico, sino en el dominio del conocimiento. Para Sun Tzu, la victoria no depende de la fuerza material sino de la comprensión profunda de las condiciones (propias y ajenas) que configuran el conflicto. Conocer es anticipar, y anticipar equivale a controlar. En *El arte de la guerra*, la información aparece como la esencia misma de la victoria, el recurso que permite transformar la incertidumbre en previsión. Sun Tzu (2008) distinguía entre cinco tipos de agentes³¹, configurando uno de los sistemas más antiguos de clasificación de la inteligencia. Cada categoría cumplía una función dentro de un ciclo informativo que abarcaba obtención, validación, engaño y transmisión; un modelo que prefigura el moderno ciclo de inteligencia³².

No obstante, su comprensión del espionaje no se limitaba tan solo a la recopilación de datos, sino que implicaba gestionar percepciones, tanto del enemigo como de los propios gobernantes. Sun Tzu (2008) introduce, además, una dimensión moral y cognitiva de la inteligencia. La información, cuando se usa con sabiduría, es un instrumento de orden, no de destrucción. El conocimiento se convierte así en un poder moral, la capacidad de prever, persuadir y dominar sin recurrir a la violencia directa., ya que “subyugar al enemigo sin luchar es la forma suprema de excelencia” (Sun Tzu, 2008, p. 77). En este sentido, la inteligencia es una herramienta de control del entorno psicológico del adversario, una técnica de influencia sobre

³¹ En el capítulo XIII de *El arte de la guerra*, Sun Tzu (2008) distingue cinco tipos de agentes (*jian*): locales (*xiāngjiān*), reclutados entre la población del territorio enemigo; internos (*nèijiān*), pertenecientes al aparato político o militar del adversario; convertidos (*fānjiān*), agentes “dobles” o convertidos para servir a la propia causa; sacrificables (*sījiān*), enviados deliberadamente a entregar información falsa o incompleta al enemigo, aun a riesgo de ser descubiertos y ejecutados; y sobrevivientes (*shēngjiān*), quienes regresan con la inteligencia obtenida.

³² El ciclo de inteligencia describe el proceso mediante el cual la información se transforma en conocimiento útil para la decisión estratégica. Tradicionalmente se compone de cinco fases: 1) dirección, que define las necesidades de información del mando; 2) obtención, mediante fuentes humanas, técnicas o abiertas; 3) procesamiento, donde se filtra, traduce y clasifica la información; 4) análisis y producción, en la que se evalúan la veracidad y relevancia de los datos para generar inteligencia; y 5) diseminación, que comunica el producto final a los niveles de decisión. Aunque este modelo fue formalizado por las agencias occidentales en el siglo XX, su lógica ya se insinúa en la tipología de espías de Sun Tzu (2008), donde cada agente cumple una función dentro de un sistema de recolección, verificación, engaño y retorno (McDowell, 2009; Lowenthal, 2022).

su mente. Andrew (2018) subraya que, en China, más allá del ideario de Sun Tzu, la dinastía Han institucionalizó mecanismos de inteligencia con un alto grado de burocratización; por ejemplo, prefecturas fronterizas que remitían partes regulares, redes de informantes en rutas comerciales y uso de dobles agentes en contextos de rivalidad con los xiongnu y otros pueblos de la estepa. Aquella arquitectura administrativa convirtió la información en una función ordinaria del Estado (no un recurso episódico), y consolidó un ciclo que integraba vigilancia, verificación y consejo, es decir, una forma temprana de “conocimiento para decidir” que trasciende el espionaje *ad hoc*.

Como observa Rid (2020), esta concepción prelude la idea moderna de la GC, en la que el objetivo no es aniquilar al enemigo sino moldear su percepción de la realidad. Sun Tzu comprendió que el poder más efectivo es aquel que actúa en el plano invisible de la interpretación, orientada a inducir errores, sembrar duda, alterar la confianza. Henschke (2025) lo considera el antecedente remoto de la cognición estratégica, pues su arte del engaño parte de una ontología del conocimiento, donde quien controla la información controla el mundo. Así, el legado de Sun Tzu (2008) trasciende su contexto histórico y anticipa una comprensión proto-cognitiva de la estrategia. Su pensamiento no solo ordena la práctica del espionaje, sino que eleva la información a principio de gobierno y de guerra, mostrando que dominar la mente del adversario es más decisivo que derrotar sus ejércitos. En *El arte de la guerra*, la inteligencia inaugura una forma de poder que se ejerce a través del conocimiento, no de la fuerza.

Un siglo después, en la India, la reflexión sobre la información como instrumento de poder alcanzó un grado de sistematización excepcional con Kautilya, autor del *Arthashastra* (siglo IV a.C.). Este tratado, que combina economía política, diplomacia y arte militar, constituye una verdadera teoría de la inteligencia de Estado. En sus páginas, Kautilya (1992) concibe la información no solo como medio de gobierno, sino como su sustancia misma: “El rey que no conoce lo que ocurre en su reino perece en la oscuridad; el que ve todo con los ojos de sus agentes, mantiene su poder” (p. 78)³³.

³³ En el *Arthashastra*, Kautilya (1992) integra la inteligencia dentro de un marco geopolítico más amplio conocido como la doctrina de los seis métodos de política exterior (*śāddgunya*): paz (*sandi*), guerra (*vigraha*), neutralidad (*āsana*), preparación (*yāna*), alianza (*samsraya*) y doble política (*dvaidhibhava*). Cada una de estas posturas exige información precisa sobre las capacidades, intenciones y vulnerabilidades del enemigo. Así, el espionaje se convierte en el instrumento que permite calibrar cuál de los seis caminos conviene seguir según la correlación de fuerzas.

El sistema de espionaje propuesto por Kautilya (1992) es el más completo de la Antigüedad. Organizado jerárquicamente y sostenido por redes de espías disfrazados de ascetas, comerciantes o mendigos, funcionaba como un circuito de observación permanente de la vida política, militar y social. Toda información debía ser verificada por tres fuentes distintas, anticipando el principio moderno de corroboración. Kautilya recomendaba además el uso de contraespionaje y de agentes infiltrados en la corte propia para poner a prueba la lealtad de los ministros mediante tentaciones de riqueza o deseo, revelando una comprensión temprana de la naturaleza psicológica del poder.

Pero más que una colección de métodos, el *Arthashastra* propone una epistemología del gobierno. El conocimiento, en la filosofía política kautilyana, es una forma de soberanía, ya que el Estado existe en la medida en que puede conocer, anticipar y manipular. Kautilya (1992) afirma que “la inteligencia debe preceder a la acción, pues la acción sin conocimiento es la causa de la ruina” (p. 83). Aquí la información se transforma en *artha*, es decir, en fundamento material y moral del poder. Kautilya reconoce que la mente humana es el terreno donde se libra la verdadera batalla del dominio, por lo que controlar las percepciones, las emociones y las decisiones del adversario equivale a dominar su voluntad.

Como han señalado diversos estudios sobre historia comparada de la inteligencia (Sheldon, 2005; McDowell, 2009; Lowenthal, 2022), los principios operativos presentes en el *Arthashastra* (la profesionalización de los agentes, la validación cruzada de fuentes, la combinación de espionaje y propaganda, y la subordinación de la fuerza a la información), anticipan muchos de los rasgos de la inteligencia contemporánea. Ahora bien, desde una lectura contemporánea, Rid (2020) y Henschke (2025) verían en esta tradición un antecedente directo del pensamiento cognitivo moderno, donde el conocimiento ya no actúa solo como herramienta para describir el mundo, sino como mecanismo para transformarlo.

El *Arthashastra* no solo prescribe técnicas de espionaje, sino que construye una teoría cognitiva del poder político, en la que la inteligencia se entiende como la facultad de discernir entre la verdad y la apariencia, así como entre la percepción y la manipulación. Como señala Wallace (2020), toda forma de control estratégico presupone una arquitectura cognitiva capaz de procesar la complejidad del entorno; pues bien, al integrar moral, política e información, Kautilya (1992) inauguró precisamente esa arquitectura, un modo de gobernar a través del conocimiento. Así, mientras Sun Tzu (2008) había elevado la información a principio de la estrategia, Kautilya (1992) la convirtió en el núcleo mismo del Estado. Su legado revela que la

inteligencia no es solo una herramienta de la guerra, sino también una forma superior de prudencia política que les permite a los gobernantes actuar en un mundo de incertidumbre dominando, antes que las armas, las mentes y los deseos.

En otros confines del mundo antiguo, distintas civilizaciones llegaron a conclusiones similares por caminos propios. Por ejemplo, Egipto, Persia, los pueblos hebreos y las polis griegas comprendieron que el poder dependía tanto de la vigilancia como del conocimiento, y que ningún reino podía sostenerse sin información confiable sobre aliados, enemigos y súbditos. En efecto, los egipcios organizaron sistemas burocráticos de observación al servicio del faraón³⁴; los hebreos emplearon exploradores para reconocer la Tierra Prometida³⁵; y los persas crearon redes de mensajeros y vigías que cubrían vastos territorios, garantizando la comunicación del imperio³⁶. En todos los casos, la inteligencia aparece como la contracara del mito, es decir, un saber empírico y racional destinado a preservar el orden frente al caos.

En el Mediterráneo antiguo, la inteligencia adquirió por primera vez un carácter cívico y racional. En las polis griegas, la información se convirtió en una extensión del cálculo político. Tucídides (1972), en su *Historia de la guerra del Peloponeso*, concibió la narración bélica como un ejercicio analítico de causalidad, destinado

³⁴ En el Antiguo Egipto, la inteligencia formaba parte del aparato burocrático del Estado y estaba estrechamente vinculada al poder sagrado del faraón. Los visires y escribas del reino mantenían redes de informantes encargadas de reportar actividades económicas, movimientos de tribus y amenazas a la estabilidad interna. Según Wilkinson (2013), la administración egipcia desarrolló un sistema de observación casi permanente basado en la recolección de tributos, censos y comunicaciones oficiales, que servía tanto a fines políticos como militares. Las campañas del Imperio Nuevo (1550-1070 a.C.) muestran evidencias de exploradores (*rekhyt*) y emisarios diplomáticos utilizados para anticipar los movimientos de los hititas y de los pueblos del mar. En Egipto, conocer era una forma de mantener el orden cósmico (*maat*), por lo que la información era poder en su sentido literal y religioso.

³⁵ En la tradición hebrea, la inteligencia aparece vinculada al mandato divino y a la supervivencia del pueblo elegido. El *Pentateuco* recoge varios episodios de espionaje estratégico, entre ellos el envío de doce exploradores a Canaán por orden de Moisés (Deuteronomio 1:22-26) y la misión de reconocimiento de Josué antes de la conquista de Jericó (Josué 2:1-24). En ambos casos, la obtención de información antecede a la acción bélica, y el éxito depende tanto de la observación como del discernimiento moral. Como explica Keegan (2003), estos relatos expresan la idea de que el conocimiento del terreno, de los pueblos y de sus fortalezas constituye un deber religioso y político, en donde la inteligencia se presenta como una forma de obediencia estratégica a la voluntad divina.

³⁶ El Imperio Persa desarrolló uno de los sistemas de inteligencia más extensos de la Antigüedad. Dvornik (1974) describe cómo, bajo Darío I, se institucionalizó la red conocida como *Los Ojos y Oídos del Rey*, encargada de informar directamente al monarca sobre la conducta de gobernadores, generales y súbditos. Estos agentes, distribuidos por las satrapías y apoyados en el sistema de correos reales, constituían un mecanismo de control político y moral del imperio. La vigilancia no se limitaba a fines militares, ya que también era una herramienta de cohesión imperial basada en el flujo constante de información. Este modelo anticipa la noción moderna de inteligencia estratégica, en la que el conocimiento actúa como un instrumento de gobernabilidad y prevención, no solo de guerra.

a estudiar los motivos, pasiones y percepciones que mueven a las ciudades-Estado. Para él, el conocimiento era una forma de prudencia racional; solo quien entiende las causas profundas del conflicto puede prever sus desenlaces. Tucídides ofreció así la primera interpretación estructural del poder, donde la inteligencia no se limita a saber lo que el enemigo hace, sino a comprender por qué lo hace (Tucídides, 1972).

Dvornik (1974) observa que en Grecia coexistían dos formas complementarias de inteligencia: la militar, orientada al reconocimiento del terreno y al espionaje enemigo, y la política, vinculada a la diplomacia secreta y a la manipulación de alianzas. Autores como Aeneas Tacticus y Polibio documentan el uso de mensajes cifrados, señales de humo, códigos escritos en cera o textiles y sistemas de comunicación rápida entre comandantes. Los espartanos mantenían una estructura institucional de vigilancia interna (la *krypteia*) dedicada a controlar a los ilotas, mientras que Atenas combinaba el espionaje con el debate público, convirtiendo la información en instrumento de persuasión política. Grecia, como subraya Keegan (2003), fue el primer escenario donde la inteligencia dejó de ser una práctica del soberano para convertirse en función de la polis griega, caracterizado por un conocimiento compartido, debatido y, a menudo, manipulado.

El mundo romano heredó y perfeccionó de los griegos estas formas de saber. Sheldon (2005) y Dvornik (1974) coinciden en que Roma institucionalizó la inteligencia como un componente del mando. En efecto, durante la República, los *exploratores* y *speculatores* actuaban como observadores y mensajeros en campaña; en el Imperio, esta función evolucionó hacia una red estable de agentes imperiales conocida como los *frumentarii*, encargados no solo de la logística, sino del contraespionaje imperial. En tiempos de Augusto, la información se convirtió en fundamento del control social y del mantenimiento de la *pax romana*. La expansión territorial exigía saber antes de actuar; cada conquista requería mapas, censos y descripciones de pueblos, climas y recursos.

Sheldon (2005) señala que los romanos comprendieron algo decisivo: la información no tiene valor por su volumen, sino por su organización. La *cursus publicus*, o red de correos imperiales, no era solo un sistema logístico, sino una arquitectura informacional al servicio del poder. Los informes de los gobernadores, las crónicas militares y los censos formaban un entramado de datos que permitía al emperador conocer, y por tanto controlar, los espacios más distantes del imperio. En palabras de Keegan (2003), Roma inventó la inteligencia burocrática, un saber que no pertenece a un individuo, sino a una institución.

En este sentido, la inteligencia romana representó un punto de inflexión en la historia del conocimiento estratégico. Su finalidad ya no era únicamente anticipar al enemigo, sino preservar la estabilidad del sistema político. Como explica Rid (2020), esta evolución marca el paso de la inteligencia como observación táctica a la inteligencia como gestión de la percepción, en el cual la información se emplea para mantener la legitimidad del orden establecido. La propaganda imperial, los rituales de fidelidad y la censura del discurso público constituyen expresiones tempranas de lo que hoy denominaríamos operaciones de influencia. Por consiguiente, la convergencia entre espionaje, administración y comunicación en Roma anticipa la estructura cognitiva de los Estados modernos. Para Henschke (2025), las instituciones imperiales pueden entenderse como sistemas protocognitivos³⁷ capaces de procesar información, ajustar comportamientos y proyectar poder simbólico. La inteligencia, en este marco, no es solo una función técnica, sino una forma de cognición colectiva que permite al Estado adaptarse y sobrevivir.

Así, desde Atenas hasta Roma, la inteligencia dejó de ser una práctica artesanal para transformarse en un sistema racionalizado de conocimiento. El mundo clásico entendió que la información debía organizarse, verificarse y administrarse como recurso político. Grecia aportó la reflexión ética sobre la verdad y la persuasión; Roma aportó la estructura. Ambas legaron a la posteridad la idea de que la sabiduría del gobierno reside en conocer el mundo antes de transformarlo, prelu-diando la visión moderna en la que el poder se ejerce sobre mentes y significados tanto como sobre cuerpos y territorios.

Tras la caída de Roma, el Imperio Bizantino mantuvo viva la tradición de la información estratégica. El *Strategikon*, atribuido al emperador Mauricio (siglo VI), integra la inteligencia dentro de la doctrina militar y recomienda observar a los pueblos, sus costumbres, sus ejércitos y sus intenciones (Mauricio, 1984). El espionaje y la diplomacia se funden, ya que Bizancio prefería comprar la paz o manipular

³⁷ El concepto de *sistema protocognitivo* se utiliza en la teoría de la GC para describir organizaciones o estructuras colectivas que, sin poseer conciencia individual, cumplen funciones análogas a la cognición, ya que perciben el entorno, procesan información, aprenden de la experiencia y ajustan su conducta para alcanzar objetivos. En este sentido, los imperios antiguos, como el romano o el bizantino, pueden considerarse sistemas protocognitivos porque integraban mecanismos de percepción (espías, mensajeros, censos), memoria institucional (archivos, informes) y decisión (consejos, mando militar) que les permitían adaptarse al cambio y mantener la estabilidad del poder. Wallace (2020) aplica este marco a la dinámica de los sistemas sociales complejos, mostrando cómo las organizaciones políticas actúan como cerebros distribuidos, mientras que Henschke (2025) lo extiende al ámbito de la GC contemporánea, donde las instituciones y redes informacionales funcionan como mentes estratégicas capaces de moldear el comportamiento colectivo.

alianzas antes que recurrir a la fuerza. Su servicio de agentes y contraespías, descrito por Keegan (2003), fue probablemente el más eficiente de la Edad Media. La inteligencia se convierte aquí en sustituto de la violencia y en instrumento de disuasión y supervivencia imperial. En esta etapa surgió también una forma temprana de COMINT³⁸, basada en la interceptación y el cifrado de mensajes escritos o transmitidos por mensajeros (Tabla 7).

Tabla 7. Evolución cronológica de los tipos de inteligencia en el periodo clásico

Etapa	Técnica de recolección	Descripción y método	Ejemplo histórico	Tipo de inteligencia
Antigüedad (hasta el siglo V a.C.)	Observación directa y reconocimiento humano	Observadores, mensajeros o exploradores obtenían información por visión, oído o rumor.	Egipto y Mesopotamia: mensajeros del faraón; tablillas de Mari (1800 a.C.).	HUMINT (inteligencia humana)
China e India clásicas (siglos V-III a.C.)	Espionaje estructurado	Redes de agentes, infiltrados, dobles y contraespionaje. Clasificación de espías (Sun Tzu, Kautilya).	<i>El arte de la guerra</i> , <i>Arthashastra</i> .	HUMINT / CI (contra-inteligencia)
Mundo clásico grecorromano (siglos V a.C.-V d.C.)	Exploradores, diplomáticos y mensajeros cifrados	Recopilación de datos por exploración militar y diplomacia secreta.	<i>Speculatores y frumentarii</i> romanos.	HUMINT / SIGINT primitivo
Alta Edad Media (siglos VI-XIII)	Criptografía manual y mensajería codificada	Sustitución simple, cifrado monoalfabético, mensajeros con códigos verbales.	Código de César, cifrados árabes, <i>Bait al-Hikma</i> (Bagdad).	COMINT (inteligencia de comunicaciones)

Fuente: Elaboración propia

Durante la Alta Edad Media (siglos VI-XIII), se emplearon sistemas de sustitución simple y cifrados monoalfabéticos, técnicas que evolucionaron en el mundo islámico gracias al desarrollo de la criptografía científica en la *Bayt al-Hikma* de Bagdad. Estos métodos permitían proteger o interceptar comunicaciones diplomáticas, consolidando el principio según el cual el control de los mensajes equivalía al control de la información estratégica. En Asia oriental, la figura del *shinobi* o

³⁸ COMINT (*Communications Intelligence*) se refiere a la obtención de información mediante la interceptación, registro o análisis de comunicaciones verbales o escritas. En sus formas primitivas, surgió con la práctica del cifrado manual y la apertura de mensajes transportados por mensajeros. El desarrollo de la criptografía árabe durante la Alta Edad Media (en especial los trabajos de Al-Kindi sobre análisis de frecuencia), constituyó el punto de partida de la inteligencia de comunicaciones antes de la era electromagnética (Kahn, 1996; Andrew, 2018).

ninja en el Japón feudal representa otra forma de sistematización del conocimiento clandestino. Según las crónicas del período Heian, las escuelas de *ninjutsu* desarrollaron técnicas de infiltración, observación y engaño que trascendían la guerra, convirtiéndose en artes cognitivas para comprender y alterar el comportamiento del enemigo. Como señala Wallace (2020), estas tradiciones reflejan un principio universal según el cual la inteligencia no se limita a recolectar información, sino que busca modificar el campo perceptivo del adversario.

Y el espionaje en la América precolombina confirma la universalidad del fenómeno. Durante el Imperio Azteca, los *pochtecah* mexicas (mercaderes que también actuaban como informantes del *tlatoani*), ejemplifican la fusión entre comercio e inteligencia, ya que durante sus viajes, recababan información sobre las rutas, la riqueza, la disposición militar y las alianzas políticas de los pueblos vecinos, lo que permitía planificar futuras campañas o prevenir rebeliones (Townsend, 2021); asimismo, antes de cada campaña, los *quimichtin* eran enviados de noche para estudiar el terreno y las defensas enemigas³⁹. Su labor, según Keegan (2003), no difería esencialmente de la de los exploradores romanos o bizantinos, pues su función era observar, evaluar y comunicar.

Y más adelante, durante el periodo del Renacimiento, la inteligencia se integró de forma definitiva en la arquitectura del Estado moderno (Hughes, 2017). La República de Venecia creó un cuerpo diplomático permanente y profesionalizó la observación política con la elaboración de las *relazioni*, unos informes estratégicos que unían descripción, valoración y recomendación (Sheldon, 2005). En la Inglaterra isabelina, Francis Walsingham organizó la primera red europea de espionaje sistemático, anticipando la figura moderna del servicio de inteligencia; gracias a sus agentes infiltrados en el Imperio español y en las cortes católicas, descubrió los planes de la *Armada Invencible*, demostrando que el conocimiento podía ser tan decisivo como la artillería⁴⁰. Mientras que, en la Francia napoleónica, Fouché con-

³⁹ En el Imperio mexica, los *pochtecah* eran comerciantes de larga distancia que, además de su función económica, cumplían tareas de espionaje e inteligencia para el *tlatoani* (soberano). Los *quimichtin*, por su parte, constituían una red de espías profesionales que operaban de noche y bajo identidades encubiertas, infiltrándose en territorios enemigos para evaluar fortificaciones, recursos y ánimo de las tropas (Townsend, 2021).

⁴⁰ Un ejemplo temprano del uso sistemático de inteligencia estatal que influiría decisivamente en el curso de la historia fue el conflicto anglo-español de finales del siglo XVI. En esa época, la Inglaterra isabelina (una potencia emergente), se enfrentaba al imperio global de Felipe II de España. Sir Francis Walsingham, secretario de Estado de Isabel I, estableció una de las primeras redes de espionaje organizadas en Europa moderna, con agentes desplegados en Escocia, Francia, los Países Bajos, Italia, España e incluso dentro del propio territorio inglés. Gracias a esta red, Walsingham descubrió varias conspiraciones para asesinar a la reina y anticipó los planes de invasión de Felipe II. Su labor, apoyada por informantes como Giovanni Figliuzzi, embajador

solidó la “policía de la información” como herramienta de gobierno. En conjunto, los ejemplos anteriores muestran el tránsito de una inteligencia cortesana hacia una inteligencia de Estado, donde la continuidad institucional y la estandarización de productos informativos importan tanto como la audacia de los agentes (Hughes, 2017).

En todos estos casos, la inteligencia aparece como un arte de conocer bajo presión, el esfuerzo humano por iluminar la incertidumbre antes de actuar. Clausewitz (1984) lo expresó con claridad al afirmar que la guerra se desenvuelve en un “crepúsculo de probabilidades” donde el conocimiento nunca es completo, pero siempre necesario. La información, al reducir la fricción, se convierte en condición de la decisión. Lo que en Mesopotamia fue observación, en Roma transmisión y en Bizancio disuasión, en la modernidad se vuelve análisis, un sistema cognitivo al servicio del poder.

De esta manera, la historia de la inteligencia puede entenderse, como propone Henschke (2025), no solo como una serie de innovaciones técnicas, sino como la progresiva formalización de la cognición estratégica, es decir, la capacidad de transformar información dispersa en conocimiento orientado a la acción. Wallace (2020) amplía esta idea al sostener que la inteligencia representa la primera forma organizada de pensamiento adaptativo colectivo, el antecedente directo de la GC contemporánea. Para Rid (2020), la inteligencia es también un lenguaje, el medio por el cual las sociedades aprenden a traducir la incertidumbre en sentido operativo.

Así, desde las tablillas de arcilla de Mari hasta los centros digitales de análisis en la era de la información, la inteligencia ha acompañado a la humanidad como un espejo de su mente estratégica. Antes de que la información fuera un arma, fue conocimiento, y antes de servir para persuadir o controlar, sirvió para comprender. La historia de la inteligencia es, en última instancia, la historia del esfuerzo humano por pensar mejor que su adversario. En esa competencia cognitiva (antigua como la civilización misma), se encuentra el germen de la GC moderna, donde conocer ya no basta, porque ahora se disputa el derecho a definir qué significa conocer.

florentino en Londres, permitió frustrar las operaciones españolas. Aunque la red británica era modesta y carecía de recursos, su eficacia superó a la inteligencia española y demostró el poder de la información en la conducción de la política exterior. El desenlace final (la derrota de la Armada Invencible en 1588, agravada por una tormenta en el Canal de la Mancha) selló el ascenso de Inglaterra y subrayó el papel de la inteligencia en el equilibrio estratégico europeo.

Evolución de la inteligencia entre las guerras de primera y segunda generación

La evolución de la inteligencia entre las guerras de primera y segunda generación marca el tránsito definitivo de la observación empírica al conocimiento sistemático. A partir del siglo XVI, la centralización política de los Estados modernos y el avance de las ciencias de la observación (cartografía, criptografía, estadística), transformaron la información en un recurso estratégico institucionalizado. La inteligencia dejó de depender de la intuición de los soberanos para integrarse en estructuras permanentes al servicio del Estado, convirtiéndose en una función estable del poder. Este periodo, que abarca desde el Renacimiento hasta los albores de la Revolución Industrial, representa el momento fundacional de la inteligencia moderna: un saber técnico, político y militar orientado a garantizar la previsión y el control en la era de la guerra organizada.

La inteligencia en las guerras de primera generación

La primera generación de la guerra moderna⁴¹, surgida tras la Paz de Westfalia en 1648, se caracterizó por la organización lineal de los ejércitos y por el establecimiento del Estado soberano como actor central de la política internacional (Álvarez et al., 2017). En este contexto, la inteligencia emergió como una herramienta esencial de la razón de Estado, al servicio de la administración del poder y del equilibrio entre las monarquías absolutistas. A diferencia de la tradición medieval, donde el espionaje era una práctica ocasional y personal, durante la modernidad temprana se institucionalizó la recolección, el análisis y la circulación de la información, integrándolos en la maquinaria burocrática y militar de los Estados.

Wheeler (2011) señala que entre los siglos XVI y XVIII la inteligencia se transformó en un saber burocrático vinculado a la expansión imperial y administración del conocimiento sobre los territorios, las poblaciones y los enemigos. En este período, las cancillerías europeas consolidaron redes diplomáticas y sistemas de correo cifrado que convertían la información política en un instrumento de control

⁴¹ Su rasgo característico era el orden lineal, compuesto de largas filas de infantería armada con mosquetes de avancarga, sostenidas por una disciplina férrea que convertía la obediencia en el verdadero motor del combate. El mecanismo de derrota residía en la concentración de fuego y en la capacidad de mantener la cohesión frente al enemigo, lo que explica que las batallas campales tuvieran un papel decisivo. El énfasis estaba puesto en la forma, en la geometría militar y en la sincronización, más que en la maniobra creativa. En este marco, las guerras napoleónicas (1803-1815) y las de independencia hispanoamericanas (1809-1829) se inscriben en la primera generación de la guerra, dominada por el orden lineal y la batalla campal.

cognitivo y poder estatal. Como advierte Kahn (1996), la invención de códigos, cifras y mecanismos de comunicación segura reveló una nueva concepción de la información, en el sentido de que ya no era solo un medio para la acción, sino una forma de poder en sí misma, pues quien controlaba el flujo de los mensajes dominaba también la capacidad de decisión política. Esta nueva racionalidad informacional hizo de la inteligencia un componente estructural del Estado moderno.

Durante los siglos XVI y XVII, las redes de espionaje eran efímeras y dependían del favor de los monarcas, pero en esa misma época surgieron las prácticas fundacionales de la inteligencia moderna. Uno de los avances más significativos fue la creación de los llamados fondos secretos, presupuestos reservados empleados por Inglaterra, Francia, Austria y otras potencias para financiar el espionaje, el soborno y la propaganda. La existencia de estos fondos institucionalizó la inteligencia como una función permanente del Estado, más allá de los intereses personales del soberano. En el plano militar, la inteligencia acompañó la geometrización del campo de batalla. Los oficiales militares encargados de la observación enemiga registraban posiciones, trayectorias y formaciones con el rigor de un cartógrafo, transformando así percepción visual en conocimiento táctico. Este énfasis en la observación refleja el paradigma racionalista de la época, en el que la guerra se concebía como una ciencia del orden y la proporción. Sin embargo, también revela el límite cognitivo en los años tempranos de la primera generación de guerra, en la cual la inteligencia seguía siendo acumulativa, descriptiva y reactiva, más orientada a registrar que a interpretar.

Andrew (2018) destaca que el espionaje del periodo moderno temprano se convirtió en una extensión natural de la razón de Estado. En las monarquías absolutas, la información era concebida como un bien político, tan necesario como la hacienda o el ejército, por lo que figuras como Richelieu, Walsingham o Felipe II entendieron que la estabilidad de sus reinos dependía tanto del control de las armas como del control del saber. Hughes (2017) añade que el modelo francés del *Cabinet Noir* inspiró a otros Estados europeos a desarrollar sistemas equivalentes de control informacional⁴². En lugares como Viena, Berlín y San Petersburgo surgie-

⁴² El *Secret du Roi* y las *Cabinets Noires* constituyen los precedentes más notables de la inteligencia organizada en la Europa moderna. El primero fue una red secreta creada por Luis XV de Francia hacia 1745, dirigida personalmente por el monarca y fuera del control del Ministerio de Asuntos Exteriores. Su finalidad era recopilar información y ejecutar misiones diplomáticas paralelas, lo que le permitió intervenir en los asuntos de Polonia, Rusia e Inglaterra sin el conocimiento de su propio gabinete. Según Andrew (2010), el *Secret du Roi* representa el primer intento documentado de fusionar espionaje, diplomacia y manipulación de la información como instrumentos de política exterior. Por su parte, las *Cabinets Noires* surgieron en Francia desde el siglo XVI y fueron imitadas por Inglaterra, Austria y otros reinos. Se trataba de oficinas especializadas en interceptar,

ron oficinas permanentes encargadas de interceptar y analizar la correspondencia diplomática. En ellas trabajaban tanto criptógrafos como lingüistas y técnicos especializados en abrir y volver a sellar cartas sin dejar rastro, lo que convirtió a la interceptación postal en una práctica sistemática de vigilancia⁴³ (Kahn, 1996). Estas operaciones pueden considerarse una forma de proto-SIGINT⁴⁴, pues anticipaban el principio de la inteligencia de señales, orientado a obtener ventaja estratégica mediante el control de los flujos comunicativos del adversario (Tabla 8).

Tabla 8. *Etapas históricas del SIGINT primitivo*

Periodo	Medio o técnica	Descripción	Ejemplo histórico
Antigüedad	Señales de fuego, humo o espejos	Monitoreo de sistemas visuales de comunicación entre fortalezas o ciudades.	Grecia y Persia: vigilancia de torres de señales y antorchas (Heródoto).
Edad Media	Mensajeros interceptados y criptografía manual	Captura de cartas o uso de códigos por órdenes religiosas o cortes.	Imperio bizantino y papado: uso de sustitución monoalfabética.
Renacimiento (siglos XV-XVI)	Interceptación postal y lectura secreta	Surgimiento de oficinas dedicadas a abrir y copiar correspondencia diplomática (<i>Cabinets Noirs</i>).	Francia (Richelieu) y Venecia.
Siglo XVIII	Sistemas ópticos de señales (telégrafo óptico)	Transmisión por torres visuales; los Estados desarrollan vigilancia y descifrado de códigos ópticos.	Telégrafo de Chappe (Francia, 1794) vigilado por potencias vecinas.
Siglo XIX	Telégrafo eléctrico (SIGINT moderno inicial)	Interceptación de cables telegráficos y control de tráfico de mensajes durante guerras.	Guerra de Crimea (1854-1856); Guerra Civil estadounidense (1861-1865).

Fuente: Elaboración propia

abrir, leer y volver a sellar el correo diplomático y privado, tarea que requería criptógrafos, lingüistas y restauradores expertos. Kahn (1996) las considera las precursoras de la inteligencia de señales moderna, ya que su objetivo no era solo descubrir el contenido de los mensajes, sino también mapear las redes de comunicación del adversario. Ambas instituciones marcaron el tránsito desde el espionaje cortesano hacia un modelo de inteligencia institucional, centralizado y orientado a la gestión del flujo informacional como base del poder político.

⁴³ Hughes (2017) subraya que la creación de criptógrafos profesionales, archiveros y censores dio a la inteligencia un carácter casi científico, preludio de la burocracia informacional que dominaría la era industrial.

⁴⁴ Proto-SIGINT (o SIGINT primitivo) designa las formas tempranas de inteligencia de señales anteriores a la era electromagnética. Comprendía la interceptación, manipulación o análisis de mensajes físicos (cartas, mensajeros, señales ópticas o de humo), con el fin de obtener información sobre las comunicaciones del adversario. Según Andrew (2018) y Hughes (2017), prácticas como la apertura clandestina de correspondencia en los *Cabinets Noirs* franceses o la observación de los telégrafos ópticos en el siglo XVIII constituyen los primeros intentos sistemáticos de vigilancia de señales.

Estas instituciones, que unían ciencia, técnica y política, representaron un punto de inflexión en la historia del secreto de Estado, ya que la información pasó de ser un recurso al servicio del monarca a convertirse en una estructura impersonal de poder. En Inglaterra, el *Secret Office* del siglo XVII también empleaba criptógrafos y descifradores para interceptar y analizar comunicaciones extranjeras, marcando los inicios de la inteligencia de señales. Según Andrew (2010), este modelo británico anticipó el principio moderno de la *fusión de inteligencia*, es decir, la idea de que el conocimiento estratégico surge de la convergencia entre distintas fuentes y métodos, no de la observación aislada.

Desde finales del siglo XVI, Francia integró estas operaciones en el Ministerio de Relaciones Exteriores y el servicio postal, inaugurando un modelo de control informacional que combinaba espionaje político, censura y análisis de inteligencia. El cardenal Richelieu, primer ministro de Luis XIII, llevó estas prácticas a un nivel sin precedentes al utilizarlas tanto para espiar a potencias extranjeras como para vigilar a los opositores internos⁴⁵. Fue uno de los primeros estadistas en mantener archivos sistemáticos donde se almacenaban informes de embajadores, cartas interceptadas y documentos judiciales, lo que transformó la información en una forma de gobierno. Desde una perspectiva epistemológica, esta práctica representó un cambio cualitativo: la información dejó de ser un recurso ocasional para convertirse en un dispositivo de control cognitivo del Estado sobre la sociedad.

En este sentido, Richelieu anticipó la noción foucaultiana de vigilancia como forma de saber-poder y prefiguró la relación entre la inteligencia y la biopolítica que definiría la modernidad política. Durante el asedio de una fortaleza española en 1639, sus agentes interceptaron un mensaje enemigo y enviaron una falsificación que ordenaba la rendición, ejemplo paradigmático del uso del engaño informacional como instrumento de guerra. Con él, la información dejó de ser un medio pasivo de observación para convertirse en un arma de manipulación activa.

Hacia 1700, Francia había adquirido fama de maestra en el arte del espionaje, y no es casual que el vocabulario inglés de la inteligencia (*reconnaissance*,

⁴⁵ El cardenal Armand Jean du Plessis, duque de Richelieu (1585-1642), es considerado uno de los fundadores de la inteligencia moderna en su vertiente estatal. Como primer ministro de Luis XIII, comprendió que el poder del Estado no podía depender únicamente de la fuerza militar o de la diplomacia visible, sino también del conocimiento sistemático de las intenciones de amigos y enemigos. Richelieu organizó una red de informantes que operaba tanto en el exterior como en el interior del reino, estableciendo un sistema de vigilancia que combinaba espionaje, censura y recopilación de información sobre súbditos, clérigos y nobles potencialmente desleales (Wheeler, 2011).

surveillance, espionage), provenga del francés, reflejando su liderazgo técnico y cultural en el campo. Entre los agentes más singulares de este periodo destaca el caballero Charles d'Éon (1728-1810), diplomático y espía del *Secret du Roi* de Luis XV, una red clandestina que actuaba al margen de la diplomacia oficial. Sus misiones en Inglaterra y Rusia mostraron la sofisticación y el doble juego de la política secreta europea. D'Éon encarna la transición de la lealtad personal al profesionalismo informacional, ya que cuando fue despedido, intentó chantajear al rey con documentos secretos, revelando que la información había adquirido un valor independiente del poder político que la producía.

En el ámbito militar, Federico el Grande de Prusia sistematizó el empleo de espías con un enfoque casi científico. Clasificó a los agentes en comunes, dobles, de alta clase o coaccionados, según sus motivaciones y accesos, anticipando una tipología funcional del espionaje. Su insistencia en que ningún general puede vencer sin información simboliza el paso de la intuición táctica a la racionalidad estratégica basada en los datos. El espionaje se convirtió así en un saber de observación, registro y deducción, precursor de la inteligencia moderna. Warner (2002) sostiene que el nacimiento de esta última no radica en la figura del espía, sino en la capacidad de inferir y anticipar a partir de información incompleta, lo que convierte a la inteligencia en una práctica hermenéutica.

El proceso también adquirió una dimensión epistemológica. En las cancillerías se acumulaban cartas, informes y mapas que eran examinados por analistas que buscaban deducir intenciones o tendencias. Por lo tanto, la información se convirtió en un espacio de representación del mundo, un dispositivo para reconstruir cognitivamente la realidad. Floridi (2015) interpreta este cambio como la transición hacia una ontología informacional, en la que los Estados no solo actuaban sobre el mundo, sino que lo reconfiguraban mediante datos, informes y representaciones. En este sentido, la actividad de inteligencia fue el primer laboratorio de la cognición política moderna.

La expansión marítima y colonial amplió esta dimensión informacional. Wheeler (2011) describe cómo las potencias imperiales usaron la exploración geográfica como instrumento de inteligencia. Los mapas, bitácoras y registros climáticos eran mecanismos de conocimiento que permitían dominar el espacio y anticipar resistencias. La cartografía se transformó en una forma de espionaje del territorio, y la información geográfica se convirtió en poder imperial. De ahí que pueda afirmarse que la inteligencia de esta etapa fue, ante todo, un saber territorial, orientado a observar, clasificar y controlar el entorno físico y humano.

Durante el siglo XIX, este paradigma alcanzó su madurez institucional con la creación del Servicio Geográfico del Ejército Prusiano, encargado de elaborar mapas topográficos, realizar levantamientos triangulados y producir inteligencia geodésica al servicio de la planificación militar. Su labor demostró que el dominio del terreno era una forma superior de previsión estratégica y convirtió la geografía en un instrumento del Estado Mayor. Esta práctica constituye el antecedente directo de lo que en la actualidad se denomina GEOINT⁴⁶, la inteligencia derivada de la integración entre datos espaciales, imágenes, coordenadas y análisis topográfico que permite vincular el conocimiento geográfico con la acción estratégica (Tabla 9).

Tabla 9. Evolución cronológica de los tipos de inteligencia en las guerras de primera generación

Etapa	Técnica de recolección	Descripción y método	Ejemplo histórico	Tipo de inteligencia
Renacimiento y Modernidad temprana (siglos XV-XVII)	Diplomacia secreta, interceptación postal y criptografía compleja	Cancillerías establecen gabinetes de interceptación (<i>Cabinets Noirs</i>).	Walsingham (Inglaterra), Richelieu (Francia).	SIGINT primitiva / HUMINT institucional
Siglo XVIII (Ilustración y razón de Estado)	Censura y vigilancia sistemática de la correspondencia	Se crea infraestructura estatal para el control de flujos informativos.	<i>Cabinet Noir</i> francés, oficinas de Viena.	SIGINT / OSINT temprana
Siglo XIX (Revolución Industrial)	Reconocimiento topográfico y cartográfico	Recolección de información por exploradores, geógrafos y agregados militares.	Servicio Geográfico del Ejército prusiano.	GEOINT (inteligencia geoespacial)
	Intercepción telegráfica	Primeros escuchas de cable y control de tráfico de mensajes.	Guerra de Crimea (1854-1856); Guerra de Secesión (1861-1865).	SIGINT
	Fotografía terrestre y aérea primitiva	Aplicación de la fotografía al reconocimiento militar.	Globos de observación, 1860-1870.	IMINT (inteligencia de imágenes)

Fuente: Elaboración propia

⁴⁶ GEOINT (*Geospatial Intelligence*) hace referencia a la obtención, análisis y visualización de información geoespacial proveniente de mapas, sensores, imágenes y datos de posicionamiento para apoyar la toma de decisiones estratégicas, militares o de seguridad. Su genealogía remota incluye el trabajo de los servicios cartográficos de las potencias coloniales y, de forma más sistemática, del Servicio Geográfico del Ejército Prusiano, fundado en 1816, cuya precisión topográfica y uso de triangulación geodésica sentaron las bases de la inteligencia geoespacial moderna, la cual integra tecnologías de observación satelital, sistemas de información geográfica (SIG) y análisis espacial automatizado (Andrew, 2018; NGA, 2017; Wheeler, 2011).

En consecuencia, a finales del siglo XVIII y principios del siglo XIX, el espionaje se había consolidado como una práctica transnacional. Los sistemas de señales, las escrituras secretas y las redes diplomáticas coexistían con formas más modernas de intercambio informativo. Empresas privadas como Lloyd's of London o los bancos Rothschild crearon redes de mensajería capaces de transmitir noticias de batallas antes que los propios gobiernos, convirtiendo la información en capital estratégico. En el caso de Lloyd's of London, las oficinas establecidas en los principales puertos del Atlántico y el Mediterráneo recopilaban datos sobre movimientos navales, rutas comerciales, condiciones meteorológicas y pérdidas marítimas, lo que les permitió anticipar riesgos y fijar primas de seguro antes que cualquier autoridad estatal. Su sistema de correspondencia y avisos marítimos funcionaba como una verdadera red de inteligencia naval privada⁴⁷.

En América, George Washington organizó durante la Revolución estadounidense una red de agentes financiada por fondos secretos del Congreso, anticipando la estructura de la inteligencia estadounidense⁴⁸ (Wheeler, 2012). En Europa, la Revolución francesa llevó esta institucionalización a un nuevo extremo. El Ministerio de Relaciones Exteriores del gobierno revolucionario creó un aparato de espionaje y contraespionaje encargado de censurar prensa y correo, sabotear operaciones extranjeras y difundir propaganda, prácticas que presagiaban los métodos de los servicios totalitarios del siglo XX.

En Hispanoamérica, generales como Simón Bolívar y Francisco de Paula Santander también comprendieron la importancia de la inteligencia como herramienta de supervivencia política y militar. Bolívar organizó redes informativas en

⁴⁷ Por su parte, la familia Rothschild desarrolló en el siglo XIX una red de mensajeros y agentes financieros que enlazaba las principales capitales europeas (Londres, París, Viena, Nápoles y Fráncfort), adelantándose incluso a los servicios diplomáticos. Durante las guerras napoleónicas, sus correos privados transmitían información política y militar que les permitió especular con bonos del Estado según el resultado de las campañas. Como relata Andrew (2018), Nathan Rothschild conoció la derrota de Napoleón en Waterloo veinticuatro horas antes que el gobierno británico gracias a sus informantes en el continente. Este tipo de inteligencia financiera mostró que la información podía convertirse en una forma de poder económico y político, preludio del espionaje corporativo y de la inteligencia económica contemporánea.

⁴⁸ Durante la Guerra de Independencia de los Estados Unidos (1775-1783), George Washington organizó una red de espionaje que combinaba la recopilación de inteligencia humana (HUMINT) con el uso sistemático de códigos, tinta invisible y mensajeros cifrados. Conocida como la *Culper Spy Ring*, esta red operó principalmente en Nueva York y Long Island, y fue financiada mediante fondos secretos aprobados por el Congreso Continental. Wheeler (2012) destaca que Washington fue, de facto, el primer jefe de inteligencia de una república moderna, al concebir la información no como un recurso personal del gobernante, sino como un bien público destinado a la seguridad nacional. Esta innovación implicó una ruptura epistemológica respecto al espionaje monárquico, ya que la inteligencia dejó de servir a la razón del príncipe para servir a la razón del Estado. En términos contemporáneos, puede afirmarse que la *Culper Spy Ring* inauguró la tradición institucional y cognitiva que más tarde daría origen a la inteligencia estadounidense como un sistema permanente de conocimiento estratégico.

el Caribe para monitorear los movimientos españoles y planificar la emancipación de Cuba y Puerto Rico, en coordinación con México. Sin embargo, la operación conjunta fue frustrada por el espionaje diplomático de los Estados Unidos, lo que revela que América Latina entró en la modernidad política en un entorno de vigilancia y competencia informacional.

La inteligencia de la primera generación de la guerra combinó observación, archivo y engaño como mecanismos de control cognitivo. Fue un sistema jerárquico y centralizado que buscaba reducir la incertidumbre mediante la organización racional del conocimiento. Andrew (2018) y Hughes (2017) coinciden en que entre los siglos XVI y XVIII la inteligencia dejó de ser una práctica periférica para integrarse en la estructura misma del Estado. Los gobiernos modernos comenzaron a organizar la observación, clasificar la información y normalizar su interpretación, creando las primeras redes burocráticas de conocimiento. Este proceso marcó el tránsito de una inteligencia empírica, basada en la experiencia directa, hacia una inteligencia informacional, sustentada en la sistematización y el análisis. Wheeler (2011) y Warner (2002) señalan que hacia fines del siglo XVIII la actividad de inteligencia ya no era solo un instrumento de recopilación de secretos, sino una forma de conocimiento aplicada a la acción. Así, la inteligencia se erigió en el primer dispositivo cognitivo de la modernidad, antecedente directo de la guerra informacional y de las OPSIC que dominarían los siglos posteriores.

La inteligencia en las guerras de segunda generación

Aunque el espionaje es tan antiguo como la guerra, su empleo sistemático como instrumento permanente de los Estados solo comenzó a consolidarse a partir de 1800. Antes de las revoluciones tecnológicas y políticas del siglo XIX, los dirigentes políticos y militares obtenían inteligencia mediante los métodos tradicionales. En tiempos de paz, banqueros, comerciantes y aseguradoras recopilaban información sobre rutas, mercados y riesgos para proteger o ampliar sus inversiones. En tiempos de guerra, los exploradores de caballería y los espías recolectaban datos sobre las posiciones enemigas, interceptaban correspondencia, interrogaban prisioneros y confiscaban documentos. Los diplomáticos, por su parte, se comportaban como jugadores de ajedrez atentos a los movimientos de sus adversarios, buscando anticipar su próxima jugada en el tablero político.

Sin embargo, estos métodos tradicionales de recolección y observación comenzaron a mostrar sus límites frente a la aceleración de los cambios técnicos y políticos que inauguraron la modernidad industrial. La expansión del comercio, el

desarrollo de la prensa y el surgimiento de la telegrafía transformaron radicalmente la velocidad y el alcance del conocimiento estratégico. La información dejó de ser un recurso local y artesanal para convertirse en un flujo transnacional, lo que exigió nuevas formas de organización y análisis. Así, la inteligencia entró en una etapa de transición, es decir, de una práctica empírica basada en la experiencia individual pasó a convertirse en un sistema institucional de gestión del conocimiento, anticipando el modelo que dominaría la segunda generación de la guerra.

La segunda generación de la guerra se asoció con la Revolución Industrial y alcanzó su clímax en la Primera Guerra Mundial (1914-1918). La innovación tecnológica de la artillería y la producción en masa transformó el campo de batalla en una maquinaria de desgaste. Según Álvarez et al. (2017), el mecanismo de derrota ya no se basaba en romper la línea enemiga con maniobras de infantería o caballería, sino en infligir pérdidas hasta agotar la capacidad de resistencia del adversario. La guerra de trincheras simboliza este modelo, donde el poder de fuego y la capacidad industrial resultaban más decisivos que el genio táctico. Hammes (2006) recuerda la Gran Guerra fue, en esencia, una lucha de producción sostenida, en la que la victoria dependía de quién lograra resistir más tiempo bajo el peso del desgaste de los recursos humanos y materiales.

Pues bien, con la irrupción de la Revolución Industrial, la inteligencia entró en una nueva fase de desarrollo, ya que el siglo XIX fue un laboratorio de innovación en el que las transformaciones tecnológicas, comunicacionales y logísticas ampliaron de manera radical las capacidades de recopilación y difusión de información. Wheeler (2012) observa que, en este periodo, la inteligencia militar y diplomática evolucionó paralelamente a los grandes conflictos que marcaron la transición de las guerras de primera a segunda generación, como la Guerra Civil estadounidense, las campañas austro-prusiana y franco-prusiana, las guerras coloniales, la hispano-americana, la anglo-bóer y la ruso-japonesa. Cada una de estas guerras amplió los límites de la observación, la codificación y la comunicación, estableciendo la base de la inteligencia contemporánea.

Los avances técnicos fueron decisivos. La invención del telégrafo, la máquina de escribir, la fotografía, la óptica mejorada para telescopios y binoculares, los globos de observación, el ferrocarril y el barco a vapor transformaron la relación entre tiempo, espacio y conocimiento. Por primera vez, la información podía transmitirse a una velocidad que modificaba la percepción misma del campo de batalla. El siglo XIX también vio surgir instituciones dedicadas de manera permanente a la actividad de inteligencia. Las potencias europeas establecieron escuelas de formación

de agentes en Alemania, Austria, Francia y Gran Bretaña, y adoptaron el sistema de agregados militares en embajadas extranjeras, una práctica que los Estados Unidos copiarían en la década de 1880. Aunque formalmente estos oficiales cumplían funciones de enlace diplomático, en la práctica también actuaban como recolectores de información estratégica⁴⁹.

La inteligencia militar prusiana se convirtió en modelo de eficacia durante las guerras de 1866 y 1870-1871. Su éxito se basó en el empleo de técnicas de espionaje de saturación y en la disposición de sus líderes a actuar con base en los informes de sus agentes. De acuerdo con Samuels (2019), Japón aplicó un método similar durante la Guerra Ruso-Japonesa (1904-1905), demostrando que la capacidad cognitiva para procesar información estratégica podía compensar la inferioridad material. En contraste, Austria y Francia fueron sorprendidas por la falta de previsión, lo que puso de manifiesto que la modernización de la inteligencia no dependía solo de la tecnología, sino de la cultura organizacional y la atención al conocimiento producido por los servicios de información.

La expansión de la economía industrial también dio lugar al espionaje económico y tecnológico. El caso del empresario estadounidense Francis Cabot Lowell, quien memorizó los planos de los telares británicos y fundó en 1814 la primera fábrica de algodón mecanizada en Massachusetts, ilustra la transferencia clandestina de conocimiento como herramienta de poder económico. En una era de creciente interdependencia entre industria y defensa, el espionaje comercial se convirtió en un componente esencial de la competencia interestatal. Kahn (1996) sostiene que esta forma de espionaje técnico fue el precursor directo de la inteligencia científica y tecnológica del siglo XX.

La industrialización, la urbanización y el aumento de la alfabetización impulsaron el desarrollo de la prensa moderna, que comenzó a difundir información militar con una inmediatez sin precedentes. Durante la Guerra de Crimea (1854-1856), *The Times* de Londres publicó detalles tan precisos sobre el orden de batalla británico que los oficiales rusos podían conocerlos simplemente leyendo el periódico. El zar llegó a declarar que ya no necesitaba espías, ya que bastaba con leer *The Times*. Este episodio anticipó la tensión entre la libertad de prensa y la seguridad nacional, un dilema que marcaría toda la historia posterior de la inteligencia en las sociedades democráticas.

⁴⁹ En consecuencia, surgieron las primeras leyes de protección del secreto militar; por ejemplo, la *Official Secrets Act* británica de 1889 tipificó como delito la posesión o divulgación de información gubernamental sin autorización, consagrando la noción moderna de seguridad de la información.

Hacia finales del siglo XIX, el espionaje se institucionalizó como práctica global, al punto que Estados Unidos, Rusia y Japón establecieron servicios de inteligencia permanentes y burocratizados, por lo que la inteligencia dejó de depender de la intuición individual del comandante y se integró al proceso de planificación estratégica. El espionaje ya no era solo una herramienta táctica, sino una forma de conocimiento estructural destinada a reducir la incertidumbre, evaluar escenarios y anticipar contingencias. Esta dimensión cognitiva se relaciona con lo que Floridi (2010) denominaría siglos después "la lógica de la información": la capacidad de transformar datos dispersos en conocimiento orientado a la acción.

El periodo también estuvo marcado por escándalos que revelaron tanto los riesgos morales como las implicaciones políticas del espionaje. El caso Dreyfus en Francia (1894-1906) simbolizó la paranoia del espionaje en una Europa dominada por el nacionalismo y las carreras armamentistas. El capitán Alfred Dreyfus, acusado falsamente de traición, fue víctima de un sistema de contrainteligencia politizado y antisemita, lo que dividió a la sociedad francesa durante décadas. En Austria, el general Alfred Redl, jefe de la inteligencia militar, vendió a Rusia los planes de guerra y las identidades de los agentes austrohúngaros. Descubierta en 1913, se suicidó antes de ser juzgado, y su traición alimentó el clima de sospecha que precedió a la Primera Guerra Mundial. Estos casos ilustran cómo la información, al convertirse en un recurso estratégico, también se volvió un campo de batalla moral y político.

Al concluir el siglo XIX, la inteligencia había alcanzado una madurez institucional sin precedentes. Los servicios permanentes, los códigos cifrados, las leyes de secreto y los agregados militares constituyeron el esqueleto de una nueva arquitectura informacional del poder. En términos epistemológicos, la inteligencia se consolidó como un sistema de gestión del conocimiento bajo condiciones de incertidumbre, preludeo directo de las guerras de información del siglo XX. Como señala Warner (2002), la inteligencia moderna no consiste simplemente en conocer al enemigo, sino en comprender el entorno como un campo informacional que puede ser cartografiado, manipulado y utilizado como fuente de ventaja estratégica.

La irrupción de la Primera Guerra Mundial representó una ruptura radical en la historia de la inteligencia moderna. Todas las grandes potencias europeas ingresaron en el conflicto con estructuras de información insuficientes para comprender la magnitud de lo que se avecinaba. Wheeler (2012) describe este momento como un fracaso generalizado de previsión estratégica, en el que las redes de espionaje y los servicios diplomáticos fueron incapaces de anticipar las consecuencias en

cadena de los tratados de alianza ni el impacto de la nueva potencia de fuego industrial. Las instituciones militares, acostumbradas a guerras breves y decisivas, no lograron prever el estancamiento prolongado de las trincheras ni la transformación del conflicto en una *guerra total* que involucraría a ejércitos, economías y poblaciones enteras⁵⁰.

La inteligencia, que durante el siglo XIX había sido esencialmente un servicio auxiliar, se vio súbitamente arrastrada al centro del esfuerzo bélico. La guerra total exigió la creación de una infraestructura informacional capaz de sostener tanto la conducción estratégica como la resistencia moral de las sociedades. Stout (2014) observa que entre 1914 y 1918 se produjo una expansión sin precedentes de los aparatos de inteligencia en todos los frentes, acompañada por la incorporación de nuevas tecnologías de recolección y transmisión de información. En efecto, la fotografía aérea, el telégrafo, la radio y los sistemas de cifrado transformaron el modo en cómo los actores estatales percibían el entorno y procesaban la incertidumbre. La información dejó de ser un apoyo táctico para convertirse en un recurso estructural de la guerra industrial.

Pero el estallido de la guerra en agosto de 1914 evidenció las limitaciones de los métodos tradicionales. Los cuerpos de inteligencia existentes, reducidos y mal coordinados, seguían pensando en términos propios de la guerra franco-prusiana. Las doctrinas de reconocimiento basadas en caballería y observadores terrestres resultaban obsoletas frente a un campo de batalla dominado ahora por las ametralladoras, la artillería de largo alcance y las comunicaciones instantáneas. Es más, Wheeler (2012) señala que incluso en el ejército estadounidense la visión predominante de la inteligencia era casi romántica, centrada en el espía individual y no en la estructura organizacional del conocimiento. La publicación en 1914 de una traducción del manual francés "El servicio de información: un estudio práctico" en el *Infantry Journal* norteamericano refleja esta mentalidad. El texto describía al espía como un individuo sigiloso y observador, pero no mencionaba el avión, el teléfono o la radio, símbolos de un nuevo paradigma informacional que estaba a punto de transformar la guerra.

⁵⁰ El concepto de *guerra total* alude a la movilización integral de los recursos humanos, industriales y comunicativos del Estado. Desde un punto de vista cognitivo, implica que la información y la percepción se transforman en recursos bélicos. La guerra deja de ser un fenómeno exclusivamente militar para convertirse en una dinámica sistémica donde economía, cultura y comunicación participan en la producción del esfuerzo bélico (Chickering, 2006).

La Primera Guerra Mundial extendió el campo de la inteligencia desde el frente hasta la retaguardia. El conflicto se convirtió en una guerra de economías, de moral y de percepción, donde el espionaje, la propaganda y la censura se entrelazaban en un mismo sistema de control cognitivo. Los gobiernos comprendieron que la información era tanto un recurso de combate como un medio de cohesión social. En este sentido, la inteligencia no solo recolectaba datos sobre el enemigo, sino que producía realidades narrativas que moldeaban la voluntad de lucha. Las operaciones de sabotaje, la desinformación y las campañas de influencia fueron tan decisivas como las maniobras militares. Alemania, por ejemplo, promovió la revolución bolchevique en Rusia con el objetivo de debilitar el frente oriental, demostrando que la manipulación política podía ser un arma estratégica de igual o mayor eficacia que el fuego artillero.

La guerra total amplió además la vigilancia sobre la sociedad civil. Stout (2014) explica que la frontera entre espionaje interno y externo se desdibujó. Los Estados Unidos, tras su entrada en la guerra en 1917, establecieron mecanismos de control sobre toda persona sospechosa de simpatías germanas o de actividades subversivas. La vigilancia abarcó desde comunidades luteranas hasta intelectuales y periodistas, y en algunos casos alcanzó niveles absurdos, como la investigación de un oficial naval por tener una ama de llaves de aspecto alemán. Este clima de sospecha generalizada convirtió la inteligencia en un dispositivo de biopolítica, orientado no solo a proteger el Estado, sino a modelar la conducta y la lealtad de los ciudadanos.

El espionaje clásico no desapareció, pero se vio transformado por la escala y la tecnología del conflicto. Las redes de agentes belgas y franceses, apoyadas por la inteligencia británica, operaron en los territorios ocupados vigilando el movimiento de trenes y tropas alemanas. La legendaria "Dama Blanca", figura central de una red de resistencia belga, logró anticipar ofensivas enemigas mediante observación sistemática y comunicación cifrada. Este tipo de operaciones demostraba que la inteligencia ya no dependía del heroísmo individual, sino de la capacidad de coordinar información dispersa en sistemas de observación colectiva. La Primera Guerra Mundial introdujo así la noción de la *inteligencia como red*, preludio del modelo contemporáneo de análisis distribuido.

La aparición del reconocimiento aéreo marcó otro salto epistemológico. Por primera vez, el conocimiento estratégico se derivaba de la visión vertical del territorio. Los globos de observación y las primeras aeronaves equipados con cámaras

convirtieron el cielo en una extensión sensorial de la mente militar⁵¹. Wheeler (2012) subraya que este desarrollo dio origen a la interpretación fotográfica, una disciplina que transformó la observación en análisis visual codificado. La fotografía aérea exigía decodificar signos, medir distancias, detectar patrones, convertir la percepción en lenguaje. Este proceso dio nacimiento a lo que más tarde se denominaría IMINT⁵², la inteligencia derivada del análisis de imágenes capturadas desde plataformas aéreas o espaciales (Tabla 10). El campo de batalla se volvió, entonces, una superficie de lectura, un texto que debía ser interpretado más que experimentado, y el camuflaje, como respuesta a esta nueva forma de observación, fue la primera manifestación de la GC en el dominio visual.

Tabla 10. Evolución cronológica de los tipos de inteligencia en las guerras de segunda generación

Etapa	Técnica de recolección	Descripción y método	Ejemplo histórico	Tipo de inteligencia
Primera Guerra Mundial (1914-1918)	Intercepción radiofónica (wireless interception)	Monitoreo de mensajes de radio y telégrafo.	Y-Service británico, Abhorchdienst alemán.	SIGINT
	Análisis de tráfico y radiolocalización (DF)	Identificación de redes y localización de emisores por triangulación.	Frentes occidental y oriental (1915-1918).	SIGINT / ELINT
	Fotografía aérea sistemática	Captura y análisis de imágenes verticales para cartografía y artillería.	Servicio Aéreo británico y francés.	IMINT
	Reconocimiento acústico y detección de flashes	Medición de sonido y luz para localizar artillería.	Frentes de Verdún y Somme.	MASINT primitiva

Fuente: Elaboración propia

A la dimensión visual se añadió la auditiva. La interceptación de comunicaciones telegráficas y radiofónicas permitió a las potencias desarrollar sistemas de inteligencia de señales. En Tannenberg, en agosto de 1914, la victoria alemana se

⁵¹ En el nivel táctico, la inteligencia de artillería combinó fotografía aérea, *ranging* acústico, *flash-spotting* y tráfico inalámbrico para localizar baterías y ajustar fuegos. Matthews (2013) y Andrew (2018) coinciden en que esta fusión proto-algorítmica transformó el frente en una superficie de medición, donde datos heterogéneos se convertían en soluciones de tiro. Es el antecedente directo de la noción moderna de *sensor-to-shooter*, mucho antes de la era digital.

⁵² IMINT (*Imagery Intelligence*) hace referencia a la obtención y análisis de información a partir de imágenes fotográficas, aéreas o satelitales. Su origen se remonta al reconocimiento aéreo de la Primera Guerra Mundial, cuando la observación visual se transformó en un proceso analítico capaz de inferir intenciones y capacidades enemigas. En el siglo XX, con la fotografía infrarroja, los satélites espía y la teledetección digital, la IMINT evolucionó hasta convertirse en un componente esencial de la inteligencia multifuente moderna (Wheeler, 2012; Andrew, 2018).

debió en gran parte a la explotación de mensajes rusos transmitidos sin cifrado. La combinación de análisis de tráfico y descifrado de contenido reveló movimientos de tropas y permitió a los alemanes anticipar las maniobras enemigas⁵³. Stout (2014) considera este episodio como la primera gran victoria de la SIGINT⁵⁴ moderna, donde la inteligencia técnica sustituyó la intuición por la inferencia estadística. El dato, más que el espía, se convirtió en el núcleo de la ventaja estratégica⁵⁵.

Como documenta Matthews (2013), a partir de 1915 el Reino Unido desplegó una red escalonada de interceptación (el llamado *Y-Service*), compuesta por estaciones fijas, puestos avanzados y equipos móviles de escucha que cubrían desde niveles de cuerpo de ejército hasta la retaguardia estratégica. Además del contenido, el análisis de tráfico⁵⁶ se convirtió en una disciplina propia capaz de anticipar concentraciones artilleras y preparativos de ofensiva incluso cuando el cifrado impedía leer los mensajes. Por ende, la novedad no fue solo técnica, ya que el dato inalámbrico empezó a “pesar” en la estimación, desplazando el protagonismo del espía individual hacia equipos analíticos especializados. El radiogoniómetro (DF) añadió una dimensión geométrica a la inteligencia operativa. Matthews (2013) detalla cómo la triangulación de emisores permitió cartografiar redes enemigas, fijar puestos de mando, y seguir movimientos ferroviarios asociados a refuerzos, todo ello sin descifrar el contenido. Esta “SIGINT sin lectura” probó su utilidad para sincronizar barreras artilleras y para la contra-batería, al ubicar centros de control de fuego. En definitiva, la SIGINT dejó de ser un apéndice criptográfico para convertirse en sensor de maniobra.

Simultáneamente, los servicios de inteligencia navales británicos perfeccionaron el arte del bloqueo económico gracias al uso sistemático de la información.

⁵³ El análisis de tráfico es una técnica de inteligencia que extrae información no del contenido de los mensajes, sino de sus patrones de emisión, frecuencia y rutas. Permite deducir jerarquías de mando, niveles de actividad y posibles operaciones sin necesidad de romper el cifrado. Nació en la Primera Guerra Mundial y se convirtió en herramienta clave durante la Segunda Guerra y la Guerra Fría (Kahn, 1996).

⁵⁴ SIGINT (*Signals Intelligence*) se refiere a la obtención de información a través de la interceptación y análisis de señales electromagnéticas, ya sean comunicaciones entre personas (COMINT) o emisiones electrónicas de equipos y radares (ELINT). Matthews (2013) explica que la SIGINT surgió durante la Primera Guerra Mundial con la interceptación de mensajes telegráficos y radiofónicos, y evolucionó hacia sistemas globales de vigilancia electrónica. Su objetivo no es solamente escuchar, sino inferir patrones, frecuencias y estructuras de red, convirtiéndose en una forma de inteligencia inferencial basada en el dato técnico.

⁵⁵ La Batalla de Tannenberg en agosto de 1914 entre Alemania y Rusia, es considerada la primera gran victoria de la SIGINT, ya que el ejército ruso transmitía sin cifrar sus órdenes por radio, lo que permitió a los alemanes descifrar movimientos y concentrar fuerzas para destruir al Segundo Ejército ruso. Según Stout (2014), este episodio mostró que la información técnica podía reemplazar al reconocimiento visual como la principal fuente de conocimiento estratégico.

⁵⁶ Frecuencia de emisiones, volumen, cambios de indicativos y “silencios” operativos.

Las redes de observadores en los Países Bajos neutrales detectaban puntos débiles por los que Alemania intentaba romper el bloqueo, y la Royal Navy actuaba en consecuencia mediante la presión diplomática o la interdicción marítima. La combinación de inteligencia económica, política y logística mostró que el conocimiento podía emplearse como arma estructural para debilitar la moral y la capacidad productiva del enemigo. En este contexto, el control del flujo de información equivalía al control del flujo de recursos.

Hacia 1918, la actividad de inteligencia se había convertido en un sistema complejo de observación, interpretación y acción. La cantidad de datos generados por la Gran Guerra superaba cualquier experiencia previa, por lo cual se constituyeron oficinas especializadas en análisis y síntesis de información para asistir tanto al mando operativo como a los estrategas nacionales⁵⁷. Wheeler (2012) interpreta esta expansión como el nacimiento de una nueva racionalidad militar basada en la gestión del conocimiento. La guerra había dejado de ser solo una confrontación de cuerpos y materiales para convertirse en una lucha por la supremacía cognitiva. La información, entendida como materia prima del poder, reorganizó la relación entre percepción, decisión y acción, inaugurando la era de la inteligencia moderna.

Por lo tanto, el cierre de la Primera Guerra Mundial consolidó la inteligencia como una disciplina científica del poder. La magnitud del conflicto había obligado a los Estados a desarrollar aparatos informativos permanentes, capaces de procesar volúmenes de datos cada vez mayores. La guerra ya no podía entenderse sin su dimensión informacional, y los mandos comprendieron que el conocimiento del enemigo debía abarcar tanto su infraestructura material como su psicología colectiva. Stout (2014) señala que en este período la inteligencia dejó de ser una función de apoyo para convertirse en un componente esencial de la estrategia, anticipando la centralidad que adquiriría en la segunda mitad del siglo XX.

Entre los episodios más reveladores de esta nueva lógica se encuentra la historia del telegrama Zimmermann, interceptado y descifrado por la inteligencia naval británica en 1917. El mensaje, enviado por el ministro de Asuntos Exteriores alemán Arthur Zimmermann al embajador en México, proponía una alianza militar entre ambos países en caso de que Estados Unidos entrara en guerra contra Alemania,

⁵⁷ La Primera Guerra Mundial también inauguró la cooperación SIGINT. Matthews (2013) muestra que británicos y franceses compartieron indicativos, claves rotas parciales y catálogos de redes, mientras que Alemania desarrolló un *Abhorchdienst* eficaz en el frente oriental. Hughes (2017) añade que este intercambio aceleró un aprendizaje organizacional, con la aparición de manuales, procedimientos y mesas de situación con capas superpuestas (tráfico, DF, observación aérea) que estandarizaron productos y acortaron el ciclo entre interceptar, inferir y decidir.

ofreciendo a cambio el apoyo para recuperar Texas, Nuevo México y Arizona. La operación de descifrado realizada en la célebre Sala 40 del Almirantazgo británico demostró que la información podía alterar el rumbo de la guerra tanto como una batalla decisiva⁵⁸.

Wheeler (2012) afirma que el éxito británico no fue solo técnico, sino epistemológico, porque mostró cómo la manipulación del flujo informacional podía generar efectos políticos de alcance global. Al hacerse público el contenido del telegrama, la opinión estadounidense se volvió decisivamente contra Alemania, lo que precipitó la entrada de Estados Unidos en el conflicto. La inteligencia había logrado lo que las armas aún no podían: transformar la voluntad de una nación. Por lo tanto, este episodio evidenció una dimensión inédita de la guerra moderna; la información dejó de ser un reflejo de la realidad para convertirse en un instrumento que la configuraba. Las operaciones secretas, el cifrado y la propaganda se entrelazaron en un mismo circuito de producción simbólica, en el que la verdad y la percepción eran inseparables. Floridi (2015) interpretaría este fenómeno como el paso de la información descriptiva a la información constitutiva, donde conocer y actuar se confunden. Así, la inteligencia se convirtió en epistemología aplicada, en una práctica de construcción del mundo a través del control de los datos y las interpretaciones.

A medida que la guerra avanzaba, el espionaje se diversificó en escalas y objetivos. Además de la vigilancia militar, los servicios de inteligencia ampliaron su radio de acción hacia la economía, la industria y la moral pública. Alemania intentó sabotear el suministro de municiones a los aliados mediante redes clandestinas en Estados Unidos, mientras los imperios británico y francés promovían campañas para desmoralizar a las poblaciones civiles enemigas. En todos los casos, la información se convirtió en una forma de energía estratégica, capaz de desplazar el poder sin necesidad de contacto físico. Stout (2014) destaca que esta multiplicación de frentes cognitivos transformó el trabajo de los agentes en un proceso

⁵⁸ La Sala 40 (*Room 40*) fue la unidad de criptoanálisis del Almirantazgo británico creada en 1914 bajo la dirección del almirante William Reginald Hall. Su misión consistía en interceptar y descifrar las comunicaciones alemanas obtenidas de los cables submarinos cortados por la Royal Navy. Se considera el antecedente directo del *Government Code and Cypher School* y del posterior *Bletchley Park*, responsables de romper el código *Enigma* durante la Segunda Guerra Mundial. Más allá del telegrama Zimmermann, Room 40 explotó sistemáticamente el tráfico alemán para anticipar salidas de *U-boats*, rutas de superficie y puntos de reabastecimiento, información que fue decisiva para consolidar el sistema de convoyes en 1917 (Matthews, 2013). Andrew (2018) subraya que el valor estratégico residió tanto en las lecturas parciales como en la combinación de tráfico, DF y informes mercantes: una fusión multisensor que permitió pasar del bloqueo "ciego" a la interdicción informada, reduciendo pérdidas críticas en el Atlántico.

interdisciplinario, en el que la psicología, la ingeniería y la sociología se volvieron tan importantes como la táctica o la logística.

El conflicto también generó una revolución en el modo de procesar la información. Los servicios aliados comenzaron a desarrollar departamentos de análisis integrados, donde los informes de campo, las interceptaciones y las observaciones aéreas eran consolidados y evaluados colectivamente. Esta práctica dio origen a la inteligencia analítica moderna, cuyo objetivo no era solo acumular datos, sino generar inferencias. Warner (2002) sostiene que la esencia de la inteligencia no radica en la recolección, sino en la capacidad de construir sentido a partir de fragmentos incompletos. Este principio se materializó durante la guerra en la transición del "espía individual" al "sistema interpretativo", donde la decisión dependía de la calidad cognitiva de las inferencias más que del volumen de información.

La experiencia de la guerra total introdujo además una comprensión política más profunda del espionaje. Las operaciones de contrainteligencia, la censura y el control del discurso público mostraron que la percepción era una zona estratégica del conflicto. La llamada "manía de los espías"⁵⁹ en Europa y Estados Unidos no fue solo una expresión de paranoia colectiva, sino una manifestación de la nueva conciencia informacional del poder. La vigilancia masiva, los archivos de ciudadanos y las listas negras eran síntomas de un cambio de paradigma, en el cual la seguridad del Estado se medía por la transparencia de su entorno cognitivo. En este sentido, la Primera Guerra Mundial inauguró el régimen moderno de visibilidad y control, en el que la información no solo describe al enemigo, sino que lo produce simbólicamente.

El final del conflicto en 1918 no trajo la desaparición de los servicios secretos, sino su institucionalización definitiva. Aunque muchos organismos fueron desmovilizados, la estructura de la inteligencia había quedado establecida como componente esencial del Estado moderno. Wheeler (2012) identifica en este proceso la semilla de las futuras agencias de inteligencia centralizadas, como el MI6 británico o la OSS estadounidense. La guerra había demostrado que la supervivencia

⁵⁹ La "manía de los espías" hace referencia al clima de histeria colectiva que se extendió en Europa y Estados Unidos durante la Primera Guerra Mundial, caracterizado por la sospecha generalizada hacia extranjeros, periodistas, intelectuales o ciudadanos de ascendencia alemana, acusados sin pruebas de espionaje o deslealtad. En el Reino Unido, la *Defence of the Realm Act* (1914) autorizó arrestos y censura preventiva; en Estados Unidos, el *Espionage Act* (1917) y el *Sedition Act* (1918) legitimaron la vigilancia masiva y el control del discurso público. Este fenómeno evidenció la emergencia de un nuevo paradigma de seguridad basado en la gestión cognitiva de la sospecha (Stout, 2014; Andrew, 2018).

nacional dependía tanto del conocimiento como de la fuerza. A partir de entonces, la preparación para el conflicto implicó también la gestión del saber.

El caso de la recién creada Unión Soviética resulta ilustrativo. En 1917, el régimen bolchevique estableció la *Cheka* bajo el liderazgo de Félix Dzerzhinsky⁶⁰. Este organismo no solo asumió funciones de espionaje y contrainteligencia, sino que introdujo el concepto de control informacional como mecanismo de gobierno. Stout (2014) observa que la *Cheka* anticipó las prácticas de vigilancia política y censura sistemática que caracterizarían a los servicios de seguridad del siglo XX, desde la NKVD hasta el KGB. La inteligencia dejó de limitarse al ámbito militar para convertirse en una herramienta ideológica, destinada a modelar la conciencia colectiva. Con la *Cheka*, el espionaje adquirió una dimensión total, integrando la violencia física con la manipulación simbólica.

Por ende, la herencia de la Primera Guerra Mundial fue doble. Por un lado, consolidó la inteligencia técnica (descifrado, interceptación, fotografía aérea), como un campo científico y profesional. Por otro, reveló que la información era una forma de poder tan decisiva como la artillería o la industria. Stout (2014) concluye que el siglo XX comenzó cuando los Estados comprendieron que la victoria dependía de la capacidad para dominar la percepción. En esa comprensión se encuentra el germen de la inteligencia contemporánea, donde la gestión de la información sustituye a la conquista territorial como forma primaria de dominación.

Epistemológicamente, esta guerra también marcó el paso de la observación empírica al control cognitivo del entorno. La inteligencia se transformó en una práctica hermenéutica que buscaba interpretar, no solo registrar, la realidad⁶¹. Floridi (2015) sostiene que en la era de la información todo conflicto es una lucha por la semántica, y la Gran Guerra fue el primer laboratorio de esa lucha. La información, ahora procesada por analistas, interceptores y propagandistas, se convirtió en un nuevo tipo de arma: una que operaba en el terreno invisible de las mentes.

⁶⁰ La VChK o *Cheka* (Comisión Extraordinaria Panrusa para Combatir la Contrarrevolución y el Sabotaje), fue fundada por el Consejo de Comisarios del Pueblo en diciembre de 1917. Su estructura combinó funciones policiales, de inteligencia y represión política. De ella derivaron la OGPU, NKVD, MGB y KGB, consolidando el modelo soviético de seguridad del Estado basado en la fusión entre control informacional, vigilancia ideológica y coerción (Andrew & Mitrokhin, 1999).

⁶¹ El paso de una inteligencia empírica a una inteligencia hermenéutica puede entenderse en términos de la epistemología de la información de Floridi (2010). Esta sostiene que el conocimiento no reside únicamente en la acumulación de datos, sino en la capacidad de asignarles significado y contexto. La Primera Guerra Mundial hizo evidente que la interpretación del dato era tan estratégica como su obtención, anticipando la centralidad del análisis cognitivo en la guerra moderna.

En la posguerra, figuras emblemáticas como Allen Dulles, Dilly Knox y William Friedman, formados en los laboratorios de inteligencia de Gran Guerra, encarnaron la continuidad entre la guerra total y la era del espionaje global. Dulles dirigiría la CIA en los años de la Guerra Fría; Knox perfeccionaría en Bletchley Park las técnicas de criptoanálisis que descifraron la máquina *Enigma*; y Friedman diseñaría la estructura de la Agencia de Seguridad Nacional (NSA) de Estados Unidos. Todos ellos fueron herederos directos de aquella transformación epistemológica que convirtió la información en el eje del poder. La Primera Guerra Mundial no solo cambió la manera de combatir, sino también la manera de conocer. Desde entonces, la victoria ha pertenecido a quien logra comprender antes, interpretar mejor y decidir más rápido (Boyd, 1987).

Evolución de la inteligencia entre las guerras de tercera y cuarta generación

El tránsito entre las guerras de tercera y cuarta generación marcó un punto de inflexión en la función estratégica de la inteligencia. Dejó de concebirse únicamente como instrumento de apoyo al mando y la maniobra para convertirse en un sistema de conocimiento integral, orientado tanto a anticipar como a modelar el comportamiento del adversario. Este cambio respondió a transformaciones más amplias en el carácter y la conducta de la guerra, ocasionado por la masificación tecnológica, la expansión de los medios de comunicación, la irrupción de la informática y la creciente importancia de la información como recurso de poder. En este contexto, la inteligencia pasó de operar sobre un campo de batalla físico a intervenir sobre el dominio cognitivo, donde la percepción, la narrativa y la decisión se volvieron tan decisivas como las armas y los ejércitos.

La inteligencia en las guerras de tercera generación

El fin de la Primera Guerra Mundial no trajo consigo una era de estabilidad, sino un breve interludio en el que los servicios de inteligencia se debatieron entre la desmovilización y la necesidad de adaptación a un orden internacional incierto. Wheeler (2013) sostiene que, aunque el espionaje había alcanzado una madurez técnica sin precedentes en 1918, las instituciones responsables de la inteligencia todavía carecían de autonomía política y de una estructura analítica permanente. La desmovilización general durante la posguerra redujo los presupuestos en defensa y el

pie de fuerza, lo que condujo a una contracción temporal del aparato informacional estatal. En 1924, por ejemplo, la Oficina de Inteligencia Naval de Estados Unidos pasó de trescientos funcionarios a apenas cuarenta, reflejo del desinterés político por la inteligencia en tiempos de paz. Sin embargo, esa aparente decadencia fue solo un repliegue antes de una transformación profunda.

La crisis económica mundial y la inestabilidad política de los años veinte prepararon el terreno para la emergencia de regímenes totalitarios que comprendieron, mejor que las democracias liberales, el valor cognitivo del control informacional. En Alemania, Italia, la Unión Soviética, España y Japón, los servicios de inteligencia se convirtieron en pilares del poder estatal y en instrumentos de vigilancia y coerción social. El concepto de *Estado policial* alcanzó una nueva dimensión: no se trataba solo de reprimir, sino de moldear la percepción colectiva⁶². Las policías secretas como la OGPU y la *Kempeitai* funcionaron como redes de conocimiento sobre el enemigo tanto interno como externo, en una suerte de epistemología autoritaria del control⁶³. Andrew (2010) observa que el totalitarismo introdujo la noción de que la inteligencia ya no servía únicamente para conocer al adversario, sino también para producir una visión ideológicamente controlada del mundo.

El periodo de entreguerras fue, además, un laboratorio para la competencia entre criptografía y criptoanálisis. Los avances de la radio, el teléfono y la telegrafía transformaron el flujo de información en un nuevo dominio de conflicto. A pesar de que la comunicación inalámbrica redujo las distancias, amplificó los riesgos de la interceptación, y los servicios europeos reanudaron la carrera por el dominio de las señales. En la Alemania de Weimar, la introducción de la máquina *Enigma* en la década de 1920 marcó el inicio de la criptografía electromecánica⁶⁴, mientras que

⁶² El término de *Estado policial* fue usado por primera vez en el siglo XIX en la teoría política alemana (*Polizeistaat*), pero alcanzó su sentido moderno durante el auge de los regímenes totalitarios del siglo XX, donde el aparato de seguridad se integró al sistema de gobierno como un mecanismo de conocimiento y control social.

⁶³ La OGPU (*Ob'edinennoe Gosudarstvennoe Politicheskoe Upravlenie*), sucesora de la Cheka soviética y precursora del NKVD, institucionalizó el espionaje interno y la purga de "enemigos del pueblo" como mecanismos de ingeniería social al servicio del Estado estalinista. La *Kempeitai*, policía militar japonesa establecida en 1881, ejerció funciones de inteligencia, contrainsurgencia y represión en los territorios ocupados, extendiendo el modelo imperial de control social mediante el miedo y la vigilancia. Estas organizaciones representaron lo que puede denominarse una epistemología autoritaria del poder, basada en la acumulación sistemática de información para producir obediencia, modelar la conducta y definir la verdad oficial (Haslam, 2015; Samuels, 2019).

⁶⁴ La máquina *Enigma*, patentada por Arthur Scherbius en 1918, fue adoptada por el ejército alemán en 1926. Su sistema de rotores móviles generaba combinaciones casi imposibles de descifrar sin el conocimiento de la clave del día, lo que convirtió su ruptura en Bletchley Park en una hazaña de la criptología moderna.

en Gran Bretaña la Government Code and Cypher School (GC&CS)⁶⁵, heredera de la Room 40, perfeccionaba técnicas de interceptación y descifrado que anticipaban la futura SIGINT. Jeffery (2010) destaca que esta institución, aunque aún modesta, encarnó una mutación epistemológica, en la que la inteligencia se volvía científica, cuantificable y susceptible de la automatización, alejándose cada vez más del espionaje artesanal y acercándose a un modelo algorítmico del conocimiento.

En el continente europeo, el espionaje siguió siendo una práctica de alto riesgo y doble filo. El caso del mayor polaco Jerzy Sosnowski, quien entre 1926 y 1934 logró infiltrar el Ministerio de Guerra alemán bajo la fachada de aristócrata y empresario, ilustra el grado de sofisticación que alcanzaron las operaciones humanas⁶⁶. Su red de agentes, que incluía a mujeres de la nobleza berlinesa, demostró la eficacia del engaño personal y del uso de la seducción como herramienta cognitiva. Pero el desenlace trágico de Sosnowski (liberado en un intercambio y luego encarcelado en Polonia por sospechas de traición), muestra también cómo el espionaje se había convertido en una guerra de percepciones y contrapercepciones. Este caso, que Wheeler (2013) describe de manera implícita como una dinámica de engaño y contra engaño, puede interpretarse aquí (siguiendo una lectura epistemológica propia), como una *epistemología del doble espejo*⁶⁷, en donde la inteligencia moderna no solo busca información, sino que produce incertidumbre en el adversario mediante el juego de reflejos del engaño.

En este contexto, la Unión Soviética consolidó una de las arquitecturas de inteligencia más amplias de la historia moderna. Como advierte Haslam (2015), su estructura combinó elementos heredados de la policía zarista con una nueva misión ideológica, el control de la información como medio para modelar la conciencia revolucionaria. De la Cheka inicial surgieron la OGPU y luego la NKVD, acompañadas por el GRU y la red clandestina del *Comintern*⁶⁸. Estos organismos combinaban

⁶⁵ La Government Code and Cypher School (GC&CS), creada en 1919 como sucesora de la Room 40, se transformaría en 1946 en el Government Communications Headquarters (GCHQ), epicentro de la inteligencia de señales británica y piedra angular del futuro acuerdo *Five Eyes*.

⁶⁶ El caso del mayor polaco Jerzy Sosnowski fue emblemático por el uso simultáneo de espionaje humano, manipulación afectiva y desinformación. Ilustra la convergencia entre inteligencia y psicología, que caracterizó a las operaciones de entreguerras.

⁶⁷ Propongo el término de *epistemología del doble espejo* que remite al principio hermenéutico del espionaje moderno, en el cual cada observador es, a su vez, observado, y cada dato puede ser verdadero o inducido para desinformar.

⁶⁸ El *Comintern* (Internacional Comunista) funcionó desde 1919 como brazo ideológico de la política exterior soviética. A través de sus redes, Moscú combinó diplomacia, subversión y espionaje bajo la lógica de la "revolución permanente".

espionaje, propaganda y eliminación física de opositores, en una lógica donde el conocimiento y la represión se confundían. La coexistencia competitiva entre la NKVD y el GRU, lejos de debilitar el sistema, fortaleció su capacidad de control, al generar un modelo de vigilancia cruzada dentro del propio aparato estatal (Haslam, 2015).

Stalin comprendió que la información era un arma de doble filo, ya que servía tanto para anticipar amenazas externas como para modelar la lealtad interna. Wheeler (2013) subraya que el aparato soviético desarrolló la práctica sistemática del “espía ilegal”, sin cobertura diplomática, cuyo valor radicaba en su invisibilidad política. La red de agentes soviéticos se extendió por toda Europa, América y Asia, con un énfasis especial en los puertos, las zonas industriales y las comunidades de exiliados. Como observa Haslam (2015), esta expansión perseguía un objetivo más ambicioso que la simple obtención de datos: la difusión de una visión del mundo afín al comunismo internacional. Así, la inteligencia soviética no solo observaba el sistema internacional, sino que intentaba transformarlo mediante la penetración ideológica. En esta etapa, adoptó un enfoque protocibernético del poder, es decir, una red capaz de absorber información, procesarla y retroalimentar las decisiones del Estado bajo una lógica de control total del entorno.

Las democracias liberales, en cambio, se movían con mayor cautela. El Reino Unido y Francia emplearon sus servicios para vigilar el cumplimiento de los términos del Tratado de Versalles y detectar el rearme clandestino de Alemania. Las limitaciones presupuestales y la subestimación del espionaje enemigo condujeron a numerosos fallos de apreciación. Jeffery (2010) señala que el MI6 (todavía conocido como el *Secret Intelligence Service* —SIS—) dependía más de la intuición personal de sus jefes que de un proceso institucionalizado de análisis. La ausencia de coordinación entre los servicios británicos y la diplomacia oficial generó una brecha cognitiva que permitió a Alemania y a la Unión Soviética reorganizar sus arsenales sin ser detectados a tiempo. Sin embargo, esta etapa también marcó el nacimiento de la cultura analítica que distinguiría al SIS durante la Segunda Guerra Mundial, definida por una inteligencia orientada no solamente a recolectar datos, sino a construir sentido a partir de ellos.

El espionaje económico se convirtió en una dimensión esencial de la rivalidad en el sistema internacional. Japón y la URSS destacaron en esta forma de inteligencia aplicada al desarrollo industrial. Las misiones soviéticas buscaban secretos tecnológicos para acelerar la industrialización, mientras que los japoneses desarrollaban redes comerciales y culturales que servían de fachada a sus

operaciones. Según Samuels (2019), desde la Restauración Meiji Japón entendió la inteligencia como una herramienta de modernización nacional, es decir, un sistema de aprendizaje estratégico destinado a absorber el conocimiento extranjero y luego convertirlo en ventaja industrial. Durante el periodo de entreguerras, sus agencias militares y comerciales coordinaron operaciones de espionaje tecnológico en Europa y los Estados Unidos, sentando las bases de una comunidad de inteligencia integrada que combinaba economía, diplomacia y seguridad⁶⁹. Wheeler (2013) sostiene que el periodo 1919-1939 fue el punto de inflexión en que la información económica adquirió valor estratégico comparable al militar. La inteligencia dejó de ser una mera práctica de espionaje político para convertirse en un sistema de gestión del conocimiento, vinculado a la planificación estatal y al control de los flujos de innovación.

Japón también destacó por su temprana incorporación de la tecnología en el arte de la inteligencia. Como señala Samuels (2019), fue uno de los primeros Estados en integrar de forma sistemática SIGINT e IMINT en sus estructuras militares antes de la Segunda Guerra Mundial. Desde la década de 1930, la Armada Imperial japonesa desarrolló capacidades de interceptación radioeléctrica y de reconocimiento aéreo que le permitieron obtener ventajas tácticas frente a sus adversarios en el Pacífico. Con la creación de unidades especializadas en descifrado, fotografía aérea y cartografía avanzada, la inteligencia japonesa trascendió la recolección tradicional de datos para convertirse en un sistema de procesamiento técnico del entorno, prefigurando la convergencia posterior entre tecnología, información y estrategia que caracterizaría a la guerra en la era digital.

Los servicios de inteligencia norteamericanos mantuvieron durante los años veinte un enfoque esencialmente interno. Las amenazas anarquistas y comunistas en Estados Unidos, exacerbadas por el miedo al "peligro rojo", impulsaron la vigilancia doméstica más que la recopilación externa. A nivel regional, la atención estadounidense se concentró en el Caribe, donde sus agregados militares monitoreaban los intereses de Washington en países como Nicaragua, Honduras, República Dominicana y Haití. No obstante, en el terreno tecnológico, Estados Unidos avanzó en la inteligencia de señales, estableciendo las bases de la futura red de cooperación angloamericana que dominaría el siglo XX; Andrew (2010) subraya que, aunque marginal al principio, este desarrollo anticipó la lógica de la

⁶⁹ Según Samuels (2019), durante el periodo de entreguerras, esta lógica derivó en una red global de recopilación económica y tecnológica, y durante la Guerra Fría se institucionalizó en organismos como el MITI y JETRO, que convirtieron la inteligencia comercial japonesa en política de Estado.

comunidad "Five Eyes", cimentada en la Segunda Guerra Mundial y consolidada durante la Guerra Fría.

Por su parte, los Estados totalitarios perfeccionaron la fusión entre la inteligencia, la propaganda y la coerción. En efecto, el fascismo italiano y el nazismo alemán comprendieron que controlar la información equivalía a controlar la realidad, por lo que la inteligencia se convirtió en el laboratorio de una epistemología autoritaria donde el conocimiento se subordinó a la ideología. En Alemania, la Gestapo y el Sicherheitsdienst (SD) desarrollaron una red de vigilancia interna y externa que anticipaba la lógica de la panóptica digital moderna⁷⁰. Jeffery (2010) advierte que esta expansión de la inteligencia como instrumento ideológico no solo sirvió para la represión, sino para la movilización emocional de las masas mediante la propaganda; en consecuencia, las OPSIC y la manipulación de percepciones se convirtieron en un complemento natural del espionaje técnico.

La Guerra Civil Española (1936-1939), funcionó como campo experimental de las tecnologías y tácticas militares que marcarían la transición de guerras de segunda a tercera generación; y también sirvió como laboratorio de prueba para que la URSS, Alemania e Italia probaran sus sistemas de inteligencia, propaganda y OPSIC. Por ejemplo, los soviéticos reclutaron agentes, saboteadores y asesinos españoles que posteriormente operarían en varias misiones clandestinas en América Latina y Europa, incluyendo el asesinato de Trotsky en México. El SD alemán utilizó la guerra como laboratorio de contrainteligencia, mientras que los italianos practicaron la coordinación entre información y operaciones militares (Andrew, 2018).

En paralelo, el desarrollo tecnológico para la inteligencia continuó redefiniendo los límites del conocimiento estratégico. Las cámaras ocultas, las grabadoras portátiles y los equipos de interceptación telefónica transformaron la forma de recolectar información, y los servicios de inteligencia que podían permitírselo (como los de Alemania, Francia y el Reino Unido), comenzaron a utilizar equipos de escucha y micrófonos ocultos, aunque todavía su disponibilidad seguía siendo limitada. La

⁷⁰ La Gestapo (*Geheime Staatspolizei*) fue la policía secreta del Tercer Reich, creada en 1933 y subordinada a la SS bajo Heinrich Himmler. Su función era identificar, vigilar y eliminar toda forma de oposición política o social al régimen nazi mediante un sistema de delación ciudadana y control ideológico. El Sicherheitsdienst (SD), dirigido por Reinhard Heydrich, constituía el servicio de inteligencia de las SS y actuaba como órgano de planificación del terror, recopilando información sobre enemigos reales o imaginarios dentro y fuera de Alemania. Ambas instituciones funcionaron como una maquinaria de vigilancia total, articulando espionaje interno, control de la información y análisis social para sostener la obediencia colectiva (Andrew, 2018). Su estructura anticipó lo que Foucault (1995) denominaría la lógica panóptica del poder, es decir, un sistema en el que la visibilidad constante produce autocensura y disciplina; una prefiguración del modelo de control informacional y conductual propio de las sociedades digitales contemporáneas (Haslam, 2015).

inteligencia se hacía más técnica, pero también más dependiente de la interpretación. La saturación de información requería nuevos métodos analíticos para distinguir lo esencial de lo accesorio. Como subraya Stout (2014), esta etapa preparó la transición desde la inteligencia como observación empírica hacia la inteligencia como ciencia del análisis probabilístico.

Hacia 1939, el panorama internacional se había transformado en un entramado de espionaje global. Los servicios europeos eran más amplios, sofisticados y burocratizados que en 1914, pero aún adolecían de fallos estructurales. Las democracias liberales carecían de mecanismos integrados de coordinación, mientras que los regímenes totalitarios habían subordinado la inteligencia a sus dogmas ideológicos. El resultado fue un desequilibrio cognitivo que favoreció a quienes comprendieron la guerra como un fenómeno informacional antes que material. Wheeler (2013) resume esta paradoja al señalar que, en la víspera de la Segunda Guerra Mundial (1939-1945), las potencias estaban mejor equipadas para registrar los movimientos del enemigo que para interpretar sus intenciones.

En términos epistemológicos, el periodo de entreguerras fue el laboratorio donde la inteligencia adquirió su forma moderna. Dejó de ser una práctica auxiliar del poder para convertirse en un dispositivo de observación del mundo, un sistema cognitivo capaz de estructurar la realidad mediante datos, códigos y narrativas. Los Estados comenzaron a pensarse a sí mismos como entidades informacionales, conscientes de que la supervivencia dependía tanto de la capacidad de conocer como de la de ocultar. Así, la inteligencia de las guerras de tercera generación encarnó la transición desde el espionaje artesanal a la gestión científica del secreto, preludio de la revolución cognitiva que caracterizaría al siglo XX.

La tercera generación de la guerra moderna surgió como respuesta a la rigidez de la segunda. Inspirada en el pensamiento militar alemán de entreguerras, su esencia radicaba en la maniobra, la sorpresa y la velocidad. El ejemplo paradigmático fue la *blitzkrieg* de 1939, que combinó tanques, aviación y comunicaciones modernas para lograr penetraciones profundas en la retaguardia enemiga, desorganizando tanto su logística como su moral (Singh, 2005). En este modelo, el mecanismo de derrota consistía en la dislocación física y psicológica del adversario, obligándolo a colapsar antes de poder reorganizar sus fuerzas (Álvarez et al., 2017). La tercera generación no solo supuso un cambio en la tecnología militar, sino también en la cultura militar, ya que otorgaba mayor iniciativa a los mandos inferiores y concebía la guerra como un proceso dinámico en lugar de una secuencia rígida.

La Segunda Guerra Mundial transformó la inteligencia en un componente estructural del poder militar y político. Lo que en 1914 había sido un conjunto disperso de prácticas empíricas se convirtió, tres décadas después, en una red global de conocimiento aplicada al mando y control. Stout (2014) afirma que, aunque la mayoría de las potencias llegó al conflicto mejor preparadas que en la Primera Guerra Mundial, sus sistemas de información seguían condicionados por inercias organizativas, errores de apreciación y sesgos cognitivos. El estallido de la guerra reveló tanto la expansión tecnológica de la inteligencia como sus limitaciones epistemológicas: abundaban los datos, pero escaseaba la capacidad de interpretarlos de manera estratégica.

El período inicial fue un laboratorio de fracasos. Polonia, Francia y el Reino Unido subestimaron las capacidades de la *Wehrmacht* y la velocidad de su “guerra relámpago”. Los británicos sobrestimaron la fuerza de la *Luftwaffe* y los franceses confiaron en la solidez de la línea Maginot, ignorando advertencias precisas de agentes y diplomáticos. La invasión alemana de Noruega en abril de 1940 sorprendió tanto a Londres como a Oslo. Las señales interceptadas por la GC&CS habían sugerido una inminente operación naval, pero fueron desestimadas por el Almirantazgo británico. La falta de coordinación entre la inteligencia técnica y el mando operativo impidió traducir la información en conocimiento útil; el fracaso noruego, seguido por la caída de Francia en junio, demostró que la inteligencia no solo debía recolectar, sino también persuadir y sincronizar.

Empero, la guerra aceleró la profesionalización del ciclo de inteligencia. En Bletchley Park, la GC&CS se convirtió en un laboratorio de ciencia aplicada. Bajo la dirección de Alastair Denniston y Alan Turing, los equipos británicos lograron descifrar el código *Enigma* de la *Luftwaffe* en mayo de 1940 y, posteriormente, las versiones navales de la *Kriegsmarine* en 1941. La operación *Ultra*⁷¹ generó una revolución epistemológica, debido a que, por primera vez, los estrategas podían acceder a la mente del enemigo casi en tiempo real. Jeffery (2010) observa que este salto no radicó solo en criptografía, sino en la integración interdisciplinaria entre matemáticos, lingüistas, ingenieros y analistas militares. La inteligencia se convirtió en un proceso cognitivo colectivo donde la cooperación humana era tan decisiva como la máquina.

⁷¹ *Ultra* fue el nombre en clave de la inteligencia derivada de la ruptura de *Enigma* y otros sistemas cifrados alemanes y japoneses. Representa el paso del espionaje artesanal al procesamiento masivo de datos, preludio de la inteligencia algorítmica moderna.

Por lo tanto, el control del conocimiento se tradujo en una ventaja operacional. En el Atlántico, el descifrado de los mensajes de la *Kriegsmarine* permitió neutralizar el modelo táctico de manada de los *U-Boats*, reduciendo las pérdidas de los convoyes aliados. En África del Norte, las interceptaciones de radio y los análisis de tráfico revelaron los movimientos de las fuerzas de Rommel, aunque en las primeras etapas el propio mariscal del Eje disfrutó de una superioridad de señales gracias a la lectura de los informes cifrados del agregado militar estadounidense en El Cairo. La captura posterior de la unidad SIGINT de Rommel revirtió esa asimetría. En el Mediterráneo, el *Combined Bureau Middle East* (CBME) descifraba el 90 % de los mensajes italianos, facilitando las victorias británicas en Libia y Etiopía. Stout (2014) resalta que esta capacidad de explotación de señales convirtió a la inteligencia en una nueva forma de artillería invisible: en lugar de proyectiles, lanzaba información que alteraba la percepción y la decisión del adversario.

Pero la dimensión técnica no eclipsó a la humana, ya que el espionaje de campo y la contrainteligencia vivieron una expansión sin precedentes. La Operación *Double Cross*, coordinada por el MI5 bajo el Comité XX, logró capturar y convertir a casi todos los agentes del Eje en el Reino Unido⁷². El caso más célebre fue el del agente español Juan Pujol García, alias "Garbo", cuya red ficticia de veintisiete supuestos informantes engañó al alto mando alemán y jugó un papel decisivo en la Operación *Fortitude*. Durante los meses previos al Día D, Pujol transmitió más de quinientos mensajes que convencieron a Berlín de que la invasión aliada ocurriría en Calais y no en Normandía. Andrew (2010) subraya que *Fortitude* fue el experimento más avanzado de ingeniería cognitiva de la guerra moderna, ya que fue un diseño de creencias que utilizó la información como arquitectura del engaño⁷³.

En paralelo, la inteligencia norteamericana vivió un proceso de institucionalización acelerado. Antes de 1941, sus funciones estaban fragmentadas entre el Departamento de Guerra, la Marina y el Buró Federal de Investigaciones (FBI), pero la entrada de Estados Unidos en la Segunda Guerra Mundial tras el ataque a Pearl Harbor reveló la necesidad de un mando unificado. La creación del *Office of Strategic Services* (OSS) bajo el liderazgo de William Donovan respondió a esa urgencia; inspirada en el modelo británico, la OSS se concibió como una "universidad

⁷² La Operación *Double Cross* o "Comité XX" (1940-1945) fue una de las empresas más sofisticadas de contrainteligencia de la historia. Convirtió agentes enemigos en informantes británicos y estableció un modelo de gestión cognitiva de la percepción del adversario.

⁷³ La operación *Fortitude*, parte del plan *Bodyguard* para el desembarco aliado en Normandía, demuestra cómo la desinformación puede estructurar la realidad estratégica del enemigo. Constituye un antecedente directo de las doctrinas contemporáneas de *control reflexivo*.

del espionaje”, donde se fusionaron ciencia, tecnología y humanidades en función de la recolección humana, el sabotaje, el análisis psicológico y la propaganda. Sus analistas procedían de las universidades, las corporaciones y los estudios de Hollywood, combinando conocimiento académico y creatividad comunicacional para la producción de inteligencia estratégica y operaciones de influencia (Harris, 2021). Jeffery (2010) considera que esta simbiosis entre inteligencia y operaciones encubiertas fue el germen de la CIA y del principio de “acción y conocimiento” que dominaría la Guerra Fría. La OSS no solo recolectaba información, la generaba activamente mediante la manipulación del entorno, anticipando lo que hoy se conoce como GC.

Asimismo, la cooperación entre Londres y Washington dio origen a una comunidad epistemológica transatlántica. En 1942, ambos países firmaron acuerdos para el intercambio completo de inteligencia militar. La división del trabajo asignó a Gran Bretaña el liderazgo frente a Alemania e Italia, y a Estados Unidos la responsabilidad en el Pacífico. Canadá, Australia y Nueva Zelanda se incorporaron a esta red, que sería conocida posteriormente como la alianza *Five Eyes*. Andrew (2010) explica que su éxito residió en compartir no solo información, sino metodologías de interpretación. En este sentido, la guerra de inteligencia angloamericana fue la primera empresa cognitiva global: una alianza basada en el flujo y la validación del conocimiento.

Mientras tanto, la inteligencia soviética mantenía un doble papel. Por un lado, el GRU y la NKVD desarrollaban redes de espionaje en Europa y Asia; por otro, sufrían las purgas internas de Stalin, que diezmaron su eficacia inicial. No obstante, sus agentes lograron advertir con precisión la inminencia de la invasión alemana en 1941, aunque las advertencias fueron ignoradas. El caso de Richard Sorge en Tokio fue emblemático, ya que su informe sobre la decisión japonesa de no atacar Siberia permitió a Stalin trasladar divisiones clave al frente occidental, decisivas en la defensa de Moscú⁷⁴. La inteligencia soviética demostró así la potencia del conocimiento estratégico en la guerra total, aunque su aparato seguía marcado por el terror y la desconfianza interna.

En el teatro del Pacífico, la criptografía alcanzó una dimensión decisiva. El descifrado estadounidense del código naval japonés JN-25 permitió prever los movimientos de la flota imperial y preparar la emboscada de Midway en junio de 1942.

⁷⁴ Richard Sorge (1895-1944), agente del GRU, proporcionó a Moscú la información decisiva de que Japón no planeaba atacar la Unión Soviética. Su ejecución en Tokio simboliza el carácter sacrificial del espionaje en la guerra total.

La victoria no solo alteró el curso de la guerra, sino que confirmó la supremacía de la información sobre la fuerza bruta. Wheeler (2013) subraya que, desde ese momento, el paradigma militar incorporó la noción de inteligencia anticipatoria, en donde conocer el futuro probable se volvió tan importante como dominar el presente. La guerra de señales, más que los cañones o los portaaviones, se convirtió en el verdadero corazón de la estrategia.

El frente europeo de la guerra también fue escenario de una sofisticada interacción entre conocimiento técnico y engaño psicológico. Durante la Batalla de Inglaterra, el radar y la SIGINT táctica de la *Y-Service* permitieron anticipar los ataques de la *Luftwaffe* y organizar una defensa aérea flexible. En este contexto también surgió la ELINT⁷⁵, centrada en la detección y el análisis de las emisiones electromagnéticas de radares y sistemas de comunicación enemigos; gracias a esta capacidad, los aliados pudieron rastrear la frecuencia y alcance de los radares alemanes, diseñar contramedidas electrónicas y perfeccionar las operaciones de engaño. En el Atlántico, el rastreo de transmisiones permitió hundir al acorazado *Bismarck* en mayo de 1941; en los Balcanes y el norte de África, la lectura de códigos italianos y alemanes alteró la correlación de fuerzas a favor de los aliados. Cada éxito reforzaba la convicción de que la inteligencia no era un apoyo logístico, sino una dimensión constitutiva de la guerra (Stout, 2014).

El desarrollo de la inteligencia visual amplió aún más ese dominio cognitivo (Tabla 11). El fotoreconocimiento aéreo, nacido en la Gran Guerra, se perfeccionó como disciplina autónoma (IMINT). Las imágenes obtenidas por aviones de reconocimiento, y más tarde por cámaras automáticas en bombarderos, ofrecían información sobre movimientos, fábricas y objetivos estratégicos. Esta revolución visual introdujo la noción de una guerra observada desde la distancia, en la que ver equivalía a prever. Epistemológicamente, la guerra se desplazaba del campo de batalla al campo de la información: el enemigo se conocía antes de ser enfrentado.

⁷⁵ ELINT (*Electronic Intelligence*) se refiere a la obtención y el análisis de información a partir de señales electromagnéticas no comunicativas (como radares, sistemas de defensa aérea o misiles), con el fin de identificar las capacidades técnicas del adversario. Su origen se remonta a la Segunda Guerra Mundial, cuando las potencias aliadas desarrollaron unidades especializadas en interceptar y estudiar las emisiones de radar enemigas para crear contramedidas electrónicas y estrategias de engaño. En este sentido, la ELINT marcó el nacimiento de la guerra electrónica moderna y amplió el dominio informacional del combate (Matthews, 2013; Andrew, 2018).

Tabla 11. Evolución cronológica de los tipos de inteligencia en las guerras de tercera generación

Etapa	Técnica de recolección	Descripción y método	Ejemplo histórico	Tipo de inteligencia
Periodo de entreguerras (1919-1939)	Fusión interagencial y decodificación avanzada	Creación de centros como GC&CS (Reino Unido).	Predecesor de Bletchley Park.	SIGINT / ANALISIS
	Fotointerpretación y cartografía aérea	Uso de estereoscopia y fotomosaicos.	Guerra civil española, 1936.	IMINT / GEOINT
Segunda Guerra Mundial (1939-1945)	Criptanálisis mecanizado	Máquinas de descifrado (Bombes, Colossus).	Bletchley Park, Enigma, Lorenz.	SIGINT / CYBINT primitiva
	Radar y detección electrónica	Empleo de señales de radar para inteligencia.	Batalla de Inglaterra.	ELINT (inteligencia electrónica)
	Reconocimiento aéreo estratégico	Fotografía de gran altitud y análisis sistemático de objetivos industriales.	RAF PRU, U-2.	IMINT

Fuente: Elaboración propia

En el terreno de la contrainteligencia, los británicos desarrollaron una maestría sin precedentes. El MI5 neutralizó más de doscientos agentes del Eje y convirtió la mayoría en dobles agentes; en América Latina, el FBI desmanteló redes nazis en Brasil y vigiló los movimientos del Eje en Argentina. La coordinación entre servicios permitió un control sin precedentes del espacio informacional global. Jeffery (2010) argumenta que esta capacidad de gestión integral de la información fue el primer paso hacia la inteligencia total, entendida como un sistema de observación planetaria que combinaba espionaje, análisis y acción.

A medida que el conflicto se acercaba a su fin, la inteligencia se consolidó como infraestructura del orden mundial. Las operaciones conjuntas de SIGINT y HUMINT, el manejo del engaño y la manipulación de la percepción se convirtieron en funciones naturales de los Estados mayores. La sorpresa estratégica de Pearl Harbor y los éxitos de Midway, las campañas en África y Europa, así como el desembarco de Normandía demostraron que el conocimiento, más que la violencia, decide los desenlaces históricos. El engaño de *Fortitude*, al mantener al alto mando alemán convencido de que la invasión principal aún estaba por ocurrir, prolongó la confusión enemiga y aseguró el éxito aliado. Andrew (2010) interpreta este episodio como la culminación de un proceso que había comenzado siglos atrás, de la transición de la inteligencia como arte de la observación a la inteligencia como ciencia de la creación de realidades.

En términos organizativos, el final de la guerra marcó el nacimiento del ecosistema moderno de inteligencia. En Estados Unidos, la OSS dio paso en 1947 a la CIA, mientras que en el Reino Unido el MI6 consolidó su posición como eje de la cooperación occidental. La comunidad *Five Eyes* institucionalizó el principio de intercambio integral de señales y análisis, creando una epistemología compartida del poder⁷⁶. Jeffery (2010) destaca que este modelo sentó las bases de la Guerra Fría de un sistema de observación global donde la seguridad dependía de la capacidad de procesar información más rápido que el adversario.

Desde una perspectiva epistemológica, la inteligencia de la Segunda Guerra Mundial fue el punto de inflexión donde la información adquirió valor ontológico, debido a que los Estados comprendieron que dominar los flujos informacionales significaba dominar la realidad política y militar. El conocimiento se volvió performativo, ya que no solo describía el mundo, también lo producía. La guerra de tercera generación, centrada en la maniobra y la velocidad, alcanzó en la inteligencia su correlato cognitivo, en el que el poder dejó de medirse solo por la capacidad de fuego y comenzó a definirse por la capacidad de saber.

En síntesis, la inteligencia entre 1939 y 1945 no solamente acompañó la evolución tecnológica de la guerra, sino que redefinió su naturaleza⁷⁷, ya que dejó de ser un instrumento táctico para convertirse en un dispositivo epistemológico del mando militar. La información, estructurada, interpretada y manipulada, se convirtió en el nuevo campo de batalla. Como anticipaba Warner (2002), el conocimiento ya no era una ventaja auxiliar, sino el terreno mismo donde se libraba la lucha por la supervivencia. Al término de la guerra, el mundo entró en la era de la inteligencia global, donde la capacidad de procesar señales y narrativas sustituyó a la mera fuerza como fundamento del poder.

La inteligencia en las guerras de cuarta generación

El fin de la Segunda Guerra Mundial inauguró una nueva etapa en la historia del conocimiento estratégico. Si las dos guerras mundiales habían demostrado que la victoria dependía tanto del poder material como del manejo de la información, la era nuclear consagró a la inteligencia como el pilar epistemológico de la seguridad global. En el contexto bipolar emergente, el saber dejó de ser un instrumento

⁷⁶ El sistema *Five Eyes*, formalizado tras la Segunda Guerra Mundial, institucionalizó la cooperación entre las agencias de SIGINT de Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda. Es la arquitectura informacional más longeva de la historia contemporánea.

⁷⁷ Desde un punto de vista epistemológico, la guerra de inteligencia de 1939-1945 inaugura lo que Floridi (2011) llamaría la "era de la infosfera", donde la información se convierte en el tejido ontológico de la realidad política y militar.

subordinado a la fuerza para convertirse en su propio sustituto; el conocimiento se transformó en poder disuasivo. En este orden de ideas, la Guerra Fría (1945-1991) no fue solamente un conflicto ideológico o geopolítico, sino un experimento de cognición institucionalizada, donde las superpotencias libraron una guerra por la percepción, la interpretación y el control de la incertidumbre.

A diferencia de los periodos anteriores, la inteligencia se convirtió en una función estructural del Estado. Estados Unidos, que antes de 1941 carecía de una tradición sólida en espionaje, reorganizó su aparato informativo tras la experiencia de la OSS. La creación de la CIA en 1947, junto con el Consejo de Seguridad Nacional⁷⁸, marcó el nacimiento de una arquitectura de conocimiento permanente que integraba el análisis, la acción encubierta y la tecnología. Jeffery (2010) y Andrew (2010) destacan que este proceso de institucionalización no solo profesionalizó la inteligencia, sino que le otorgó una nueva función epistémica, al convertir la información en previsión, y la previsión en disuasión. La CIA y el MI6 británico no eran ya simples recolectores de secretos, sino fábricas de sentido que producían mapas cognitivos del enemigo para anticipar su comportamiento.

En paralelo, el caso israelí mostró cómo una comunidad de inteligencia joven podía convertirse en un nodo de intercambio con servicios consolidados. Desde comienzos de los cincuenta, la cooperación CIA-Israel se profundizó, tanto que James Angleton sostuvo un canal privilegiado con Jerusalén y valoró la *debriefing* sistemática de inmigrantes del bloque soviético, cuya información "era oro puro" para perfilar capacidades e intenciones detrás del Telón de Acero⁷⁹. Según Black y Morris (1991), esta alianza no solo elevó el prestigio del *Mossad* y del *Shin Bet*⁸⁰,

⁷⁸ La *National Security Act* de 1947 creó oficialmente la CIA, consolidando la idea de una "inteligencia centralizada" propuesta por el general William Donovan tras la disolución de la OSS en 1945. Véase Jeffery (2010) para la evolución institucional del MI6 y Andrew (2010) para el proceso paralelo en Estados Unidos.

⁷⁹ La relación entre la CIA y los servicios israelíes se consolidó rápidamente después de 1948. Durante los primeros años de la Guerra Fría, Israel desarrolló una capacidad única: la *debriefing* sistemática de inmigrantes judíos procedentes de países del bloque soviético, quienes aportaban información fresca sobre dinámicas internas, clima político, infraestructura militar y percepciones sociales dentro de la URSS y Europa del Este. Para Washington, que enfrentaba enormes dificultades de penetración en territorios soviéticos, estos insumos resultaban excepcionalmente valiosos. James Jesus Angleton, jefe de Contrainteligencia de la CIA y enlace principal con Israel, consideraba este flujo informativo como "oro puro", y lo convirtió en la base de un canal privilegiado de cooperación que reforzó la posición del Estado de Israel como un actor clave en la arquitectura de inteligencia occidental.

⁸⁰ El *Mossad* (*Ha-Mossad le-Modi'in ule-Tafkidim Meyuhadim*, Instituto para la Inteligencia y Operaciones Especiales), creado en 1949, constituye el servicio de inteligencia exterior de Israel, encargado de operaciones encubiertas, espionaje internacional y cooperación con agencias aliadas. Por su parte, el *Shin Bet* (*Sherut ha-Bitachon ha-Klali*, también conocido como *Shabak*), actúa como servicio de seguridad interior, centrado en la contrainteligencia, la prevención del terrorismo y la protección de altas autoridades.

sino que conectó HUMINT, contrainteligencia y análisis en un flujo constante que reforzó la arquitectura occidental de conocimiento.

Del otro lado del Telón de Acero, la Unión Soviética heredó una tradición mucho más antigua, en la cual el KGB y la inteligencia militar (GRU) no solo operaban como servicios de seguridad del Estado, sino como instrumentos de ingeniería social. La vigilancia interior, la penetración de instituciones extranjeras y el reclutamiento ideológico eran expresiones de un mismo principio: conocer es dominar. Sulick (2015) observa que esta asimetría inicial definió la primera década de la Guerra Fría, en la que mientras Washington intentaba construir una comunidad de inteligencia unificada, Moscú ya desplegaba una red mundial de espionaje y desinformación⁸¹. La herencia leninista del control informacional se combinó con el ideal estalinista de la omnisciencia estatal, generando una cultura del secreto donde la realidad misma se volvía una construcción política.

La década de 1950 se convirtió en un verdadero laboratorio de innovación tecnológica y epistemológica. Los casos de espionaje alcanzaron entonces una intensidad sin precedentes. El descubrimiento de la red de los “Cinco de Cambridge” reveló que la inteligencia soviética había logrado infiltrarse en el núcleo mismo de la seguridad británica⁸². Aquella traición no solo representó una pérdida operativa, sino también un trauma cognitivo al demostrar que el conocimiento podía volverse contra quien lo produce. Como subraya Andrew (2010), la Guerra Fría transformó la información en una sustancia ambivalente, capaz de conferir poder o de corroer la confianza que lo sustenta.

La respuesta occidental incorporó operaciones técnicas sin precedentes antes de la era satelital. Entre ellas, el Túnel de Berlín (1952-1956)⁸³ destacó como el mayor esfuerzo de exfiltración de datos desde un único punto en la fase precibernética.

⁸¹ La OGPU y posteriormente el KGB heredaron la estructura de la Cheka de Dzerzhinsky, pero ampliaron sus funciones a la propaganda internacional y la infiltración de partidos comunistas extranjeros, práctica sistematizada desde el Comintern (Sulick, 2015).

⁸² El escándalo de los *Cambridge Five* (Philby, Burgess, Maclean, Blunt y Cairncross) fue uno de los mayores fracasos de contrainteligencia occidental. Andrew (2010) lo considera un punto de inflexión en la cultura del secreto británica.

⁸³ La Operación *Gold* (también conocida como Operación *Stopwatch* para el SIS británico) fue una misión conjunta de la CIA y el MI6 llevada a cabo entre 1952 y 1956, destinada a interceptar las comunicaciones por cable entre los cuarteles generales soviéticos en Berlín Este y Moscú. Consistió en la construcción de un túnel subterráneo de más de 450 metros que permitía acceder al tendido telefónico y telegráfico soviético, logrando la captación de más de medio millón de conversaciones y mensajes militares. Sin embargo, el operativo fue comprometido desde su inicio por la traición del doble agente George Blake, quien informó al KGB. Aun así, los soviéticos permitieron que continuara durante meses para proteger la identidad de su informante y obtener inteligencia inversa sobre los métodos occidentales.

Conducida por la CIA en coordinación con el SIS británico, la operación interceptó tráfico telegráfico y telefónico del cableado soviético para obtener indicadores y alerta temprana sobre intenciones militares. Más que una hazaña de ingeniería, simbolizó un giro metodológico: del ataque a los cifrados (tras el ocaso de *Venona*)⁸⁴, a la interceptación directa de comunicaciones por cable (Dylan et al., 2020).

A la par de los episodios humanos, la revolución tecnológica transformó el horizonte del espionaje. El desarrollo de las telecomunicaciones, los radares y la criptografía elevó el valor del SIGINT, mientras que la IMINT, nacida en la Primera Guerra Mundial con la fotografía aérea, alcanzó una nueva dimensión con los vuelos de reconocimiento a gran altitud y los sistemas ópticos de largo alcance. El programa U-2, iniciado en 1956 bajo la administración Eisenhower, simbolizó esta nueva mirada desde el cielo, ya que los vuelos del U-2 de la CIA sobre territorio soviético proporcionaron una visión sin precedentes de las instalaciones nucleares y de los movimientos militares, desmontando el mito del “*gap*” estratégico que la propaganda soviética pretendía mantener. Sin embargo, el derribo del piloto Francis Gary Powers en 1960 mostró los límites políticos del espionaje técnico⁸⁵; la imagen del U-2 ardiendo sobre Sverdlovsk se convirtió en una metáfora de la vulnerabilidad cognitiva, ya que ver al enemigo implicaba exponerse a su mirada (Sulick, 2015).

Pese al escándalo, la información obtenida por el U-2 permitió redefinir la estrategia nuclear estadounidense. Las imágenes mostraron que el arsenal soviético era mucho menor de lo que se creía, evitando un gasto masivo en armamento y corrigiendo la narrativa del “*missile gap*” que dominaba el discurso político. Este episodio ilustra lo que Floridi (2010) llamaría, en otro contexto, una “política de la información”; es decir, el conocimiento como base de decisiones racionales frente al miedo inducido por la incertidumbre. De esta manera, la inteligencia técnica se convirtió en la herramienta más eficaz para gestionar el riesgo existencial de la era nuclear.

La información dejó de depender del HUMINT y se apoyó cada vez más en la observación remota y en el análisis automatizado de datos. Graham y Hansen

⁸⁴ El *Proyecto Venona* fue un programa ultrasecreto de criptoanálisis iniciado por la Army Security Agency (ASA) de Estados Unidos en 1943 y posteriormente asumido por la NSA, cuyo objetivo era descifrar los mensajes cifrados de la inteligencia soviética transmitidos entre Moscú y sus embajadas y redes de espionaje en el extranjero. A lo largo de más de tres décadas, los analistas estadounidenses lograron romper parcialmente los códigos del sistema soviético de “libreta de un solo uso”, revelando cientos de agentes y operaciones clandestinas en Occidente, incluidos casos emblemáticos como los de Klaus Fuchs, Julius y Ethel Rosenberg y Donald Maclean. El programa permaneció clasificado hasta 1995, cuando fue desclasificado parcialmente, y demostró el alcance de la penetración soviética en los círculos científicos y gubernamentales aliados durante y después de la Segunda Guerra Mundial.

⁸⁵ El incidente del U-2 deterioró la cumbre Eisenhower-Khrushchev en París y forzó la transición de vuelos tripulados a programas satelitales como *Corona* (Sulick, 2015).

(2007) afirman que este tránsito marcó una mutación cognitiva y metodológica en la que la inteligencia dejó de ser una práctica interpretativa para convertirse en un sistema técnico de percepción extendida, en el que los sensores sustituyeron los ojos humanos y las máquinas comenzaron a producir conocimiento sobre territorios enteros. En este contexto emergió el TECHINT⁸⁶, inicialmente concebido como una práctica de explotación técnica de materiales capturados (armas, radares o aeronaves enemigas), que pronto evolucionó hacia el análisis sistemático de capacidades industriales y tecnológicas (Tabla 12).

Tabla 12. Evolución cronológica de los tipos de inteligencia en las guerras de cuarta generación

Etapa	Técnica de recolección	Descripción y método	Ejemplo histórico	Tipo de inteligencia
Guerra Fría (1945-1991)	Satélites de observación (Corona, Keyhole)	Captura de imágenes orbitales del territorio enemigo para identificar instalaciones militares y movimientos estratégicos.	Programa Corona (EE. UU., 1960).	IMINT / GEOINT
	Intercepción global de comunicaciones	Red de estaciones de escucha planetarias para interceptar señales de radio, microondas y telecomunicaciones.	Sistema Echelon (NSA / GCHQ).	SIGINT global
	Sensores electrónicos y detección de radiaciones nucleares	Medición espectral, radar, sonar, infrarrojo y detección de pruebas atómicas o emisiones electromagnéticas.	Redes Masint (U.S. Air Force, 1960s).	MASINT
	Análisis científico y tecnológico de capacidades estratégicas	Evaluación de programas nucleares, espaciales y biotecnológicos mediante infiltración científica y fuentes técnicas.	Espionaje nuclear soviético; caso Klaus Fuchs.	SCIINT
	Explotación técnica de materiales y sistemas capturados	Estudio de armas, radares y equipos enemigos para inferir capacidades, vulnerabilidades y líneas de innovación.	Análisis del MiG-15 (Guerra de Corea); cohetes V-2.	TECHINT
	Procesamiento computacional y análisis automatizado de datos	Uso inicial de ordenadores para integrar información SIGINT, logística y estratégica.	Arpanet / NSA.	CYBINT (incipiente)

Fuente: Elaboración propia

⁸⁶ TECHINT (*Technical Intelligence*) designa la inteligencia derivada del análisis técnico y científico de equipos, materiales, armas, vehículos, radares o tecnologías capturadas al enemigo. Su origen práctico se remonta a la Segunda Guerra Mundial, cuando los aliados estudiaron misiles, submarinos y aeronaves alemanas para evaluar sus capacidades y replicar sus avances. Durante la Guerra Fría, esta práctica se institucionalizó dentro de las agencias de defensa y se amplió al estudio de sistemas industriales, electrónicos y nucleares, integrándose progresivamente con la inteligencia científica (SCIINT) y con la medición y firma de señales (MASINT).

El avance del TECHINT, basado en la explotación de materiales enemigos y el análisis técnico de sus sistemas, abrió paso a una comprensión más amplia del conocimiento como poder estratégico. La Guerra Fría transformó la recolección de datos en una empresa tecnocientífica, en la que el dominio de la física, la electrónica y la química se volvió tan decisivo como la maniobra militar. Por ello, y a medida que las armas y sistemas de defensa se volvían más complejos, los Estados comprendieron que la superioridad técnica dependía no solo de poseer tecnología, sino de comprender su lógica interna. En consecuencia, emergió una nueva rama de la inteligencia orientada a estudiar los fundamentos tecnológicos del adversario y a anticipar los límites y posibilidades de su innovación, conocido como el SCIINT⁸⁷. Su objetivo no era solo obtener información sobre proyectos militares enemigos, sino comprender los principios científicos que los sustentaban.

Por consiguiente, la SCIINT se consolidó como el principal instrumento para evaluar el avance nuclear, aeroespacial y biotecnológico de las potencias rivales, institucionalizando el conocimiento científico dentro del ciclo estratégico⁸⁸. Físicos, ingenieros y químicos comenzaron a desempeñar un papel central como analistas de inteligencia, transformando la investigación científica en un lenguaje de previsión geopolítica. Como señala Andrew (2018), esta integración marcó el momento en que la ciencia dejó de ser un ámbito neutral del saber para convertirse en un vector directo del poder estatal.

Poco después, la expansión de los sensores electrónicos y la vigilancia espectral dio origen al MASINT⁸⁹, concebida para detectar fenómenos físicos y patrones

⁸⁷ La SCIINT (*Scientific Intelligence*) se refiere a la obtención, análisis y aplicación de información relacionada con avances científicos y tecnológicos de relevancia militar o estratégica. Surgió durante la Segunda Guerra Mundial y se consolidó en la Guerra Fría, cuando el conocimiento sobre física nuclear, coherencia, química, biología o materiales avanzados se volvió crítico para la seguridad nacional de los Estados. A diferencia de la TECHINT, centrada en el estudio de equipos y armas capturadas, la SCIINT se enfoca en comprender los principios científicos que sustentan la innovación tecnológica del adversario y prever su potencial desarrollo. Durante la Guerra Fría, los informes sobre el programa atómico soviético, las pruebas termonucleares y las capacidades balísticas intercontinentales derivaban tanto de la observación técnica como del análisis científico de materiales, emisiones y residuos (Haslam, 2015).

⁸⁸ La arquitectura tecnológica anglo-estadounidense generó una ventaja comparativa para estimar despliegues y capacidades soviéticas, impulsando incluso ventanas de distensión y control de armamentos; sin embargo, el liderazgo estadounidense no siempre fue sinónimo de "más inteligente": plataformas costosas y burocracias extensas podían rendir de forma desigual fuera del eje soviético. El objetivo clave (evitar el fin del mundo) convivió con la disputa por qué mundo emergería después (Warner, 2014).

⁸⁹ MASINT (*Measurement and Signature Intelligence*) se refiere a la recolección y análisis de datos científicos obtenidos mediante sensores que detectan radiaciones, emisiones, vibraciones, sonidos o rastros químicos asociados a actividades militares o tecnológicas. Surgió formalmente en la década de 1960 dentro de la Fuerza Aérea de los Estados Unidos, como una disciplina destinada a complementar la SIGINT y la IMINT mediante la detección de "firmas" físicas o energéticas que permiten identificar armas, pruebas nucleares o movimientos

invisibles a la observación convencional. A diferencia de la IMINT o la SIGINT, el MASINT no se centra en imágenes ni mensajes, sino en las “huellas” materiales de la actividad tecnológica, como la radiación, vibraciones, emisiones térmicas, acústicas o electromagnéticas. Su desarrollo durante la década de 1960 permitió identificar pruebas nucleares encubiertas, rastrear lanzamientos de misiles y monitorear la firma infrarroja de instalaciones militares. Wheeler (2012) considera que el MASINT transformó la inteligencia en una ciencia de la detección, capaz de inferir la existencia de un evento a partir de sus rastros energéticos. Con ello, la guerra del conocimiento entró en una dimensión posvisual, donde la información ya no dependía de lo visible, sino de la interpretación de señales y firmas invisibles.

Pero el avance tecnológico no se detuvo en la Tierra, ya que, tras el lanzamiento del Sputnik 1 en 1957, la competencia bipolar se trasladó al espacio. Estados Unidos respondió con el programa *Corona*, el primer sistema de satélites de reconocimiento fotográfico. Según Graham y Hansen (2007), este programa inauguró la era del “ojo orbital”⁹⁰, una etapa en la que la Tierra se transformó en un campo de observación total. Las imágenes satelitales, recuperadas por intermedio de cápsulas fotográficas, ofrecían una representación cartográfica del poder, en la que arsenales, bases, silos y rutas de transporte se convertían en datos visuales que sostenían la lógica de la disuasión estratégica. De este modo, la Guerra Fría se configuró como una guerra de imágenes, donde el equilibrio nuclear dependía tanto de la capacidad de destrucción como de la transparencia del conocimiento recíproco.

Mientras tanto, el espionaje humano continuaba siendo decisivo. Uno de los casos más emblemáticos fue el del Coronel Oleg Penkovskiy, agente del GRU que proporcionó a la CIA y al MI6 manuales técnicos sobre los sistemas de misiles soviéticos. Sus documentos, cruzados con las fotografías aéreas del U-2 y los informes de la NSA, permitieron confirmar en 1962 la instalación de misiles balísticos en Cuba. La crisis de los misiles representó el punto culminante de la inteligencia como disciplina cognitiva, ya que la combinación de HUMINT, SIGINT e IMINT

ocultos. La MASINT se consolidó como la rama más técnica de la inteligencia, al traducir fenómenos físicos en indicadores estratégicos y convertir la medición en una forma de conocimiento sobre el entorno operacional (Matthews, 2013).

⁹⁰ El Programa *Corona* (1959-1972) fue el primer sistema operativo de reconocimiento satelital de los Estados Unidos, desarrollado conjuntamente por la CIA y la US Air Force bajo el nombre en clave *Discoverer*. Utilizaba satélites equipados con cámaras panorámicas capaces de fotografiar el territorio soviético desde órbitas bajas, recuperando los rollos de película mediante cápsulas que reentraban en la atmósfera y eran capturadas en el aire por aviones C-119 o C-130. *Corona* permitió identificar bases de misiles, instalaciones nucleares y movimientos estratégicos, revolucionando la IMINT y estableciendo el modelo de vigilancia orbital que definiría la inteligencia espacial moderna.

generó un conocimiento integrado que le permitió a John F. Kennedy calibrar su respuesta sin precipitar una guerra nuclear (Sulick, 2015). Wheeler (2013) sostiene que este episodio redefinió el sentido del saber estratégico, porque la inteligencia dejó de ser una herramienta para vencer y se transformó en una práctica para evitar la catástrofe.

En ese contexto, la disuasión se convirtió en una epistemología política. Conocer al adversario ya no significaba tan solo anticipar su ataque, sino comprender su lógica, su percepción del riesgo y su umbral de acción. El control del conocimiento equivalía al control del tiempo, razón por la cual cada informe, fotografía o interceptación era una manera de aplazar la guerra mediante la gestión de la incertidumbre. La Guerra Fría transformó así el espionaje en una forma de pensamiento sistémico. Como subraya Kent (1965), el propósito del análisis de inteligencia no es predecir lo inevitable, sino reducir la ignorancia estratégica que conduce al error. Entonces, el analista, más que un observador, se convierte en un modelador de escenarios posibles.

La consolidación del análisis profesional dentro de la CIA materializó esta visión. La creación de la *Office of National Estimates* (ONE), dirigida por Kent desde 1950, introdujo un modelo racional de producción de conocimiento basado en hipótesis verificables y niveles de confianza expresados cuantitativamente⁹¹. La inteligencia dejó de ser un arte oscuro para transformarse en una ciencia de la inferencia. Este giro epistemológico, como señala Sulick (2015), definió la identidad de la inteligencia occidental frente al secretismo ideológico soviético, ya que mientras el KGB cultivaba el mito de la infalibilidad, la CIA construía una cultura del error controlado, donde dudar era parte del método.

En paralelo, la inteligencia se convirtió en un instrumento para la influencia global. Las acciones encubiertas de la CIA en Irán (1953) y Guatemala (1954) mostraron cómo el conocimiento podía traducirse en manipulación política. De acuerdo con Jeffery (2010), estas operaciones no fueron simplemente intervenciones militares, sino los primeros ensayos de ingeniería informacional, en donde la propaganda, la infiltración y el apoyo a grupos locales configuraron un modelo de subversión política propio de las guerras de cuarta generación. En este contexto, las potencias occidentales también comprendieron que la información debía ser

⁹¹ Sherman Kent consideraba que el valor de una estimación dependía de su capacidad para delimitar la incertidumbre, no de su exactitud predictiva, un principio central del análisis moderno; Kent (1965) formalizó el uso de escalas de probabilidad ("probable", "posible", "remoto") para estandarizar el lenguaje analítico, práctica adoptada luego por la comunidad de inteligencia estadounidense.

gestionada como un frente estratégico. Según Riso (2015), la OTAN institucionalizó esta comprensión al crear en 1950 el *NATO Information Service* (NATIS)⁹², organismo encargado de coordinar la comunicación pública, la diplomacia informativa y las OPSIC en una estrategia de persuasión orientada a reforzar la cohesión ideológica del bloque atlántico y contrarrestar la propaganda soviética.

A diferencia de las generaciones anteriores, la cuarta generación de la guerra ya no estaría dominada exclusivamente por los Estados, sino también por actores no estatales como movimientos revolucionarios, insurgencias y redes terroristas (Álvarez et al., 2017). En este tipo de conflictos, el campo de batalla se desplazó hacia la población civil y los medios de comunicación convencionales, difuminando las fronteras entre lo militar, lo político y lo informativo. Hammes (2006) identifica la Segunda Guerra de Indochina (1955-1975) como el paradigma de esta transformación, pues a pesar de la abrumadora superioridad militar estadounidense, el conflicto se resolvió en favor de los insurgentes norvietnamitas gracias a su capacidad para desgastar la voluntad política de Washington y socavar su legitimidad ante la opinión pública nacional e internacional.

Asimismo, el escenario de Oriente Medio mostró durante la década de 1960 cómo la inteligencia podía redefinir el equilibrio en conflictos asimétricos, donde la supervivencia dependía más de la anticipación que de la masa militar. Israel se convirtió en un laboratorio táctico y cognitivo, demostrando que el conocimiento estratégico podía compensar la desventaja numérica y geopolítica. Durante la Guerra de los Seis Días (1967), la coordinación entre el Aman⁹³, el Mossad y el Shin Bet permitió anticipar los movimientos de los ejércitos árabes y ejecutar ataques preventivos que neutralizaron su poder aéreo en cuestión de horas. En cambio, la Guerra de Yom Kippur (1973) evidenció los riesgos de esa aparente superioridad cognitiva, ya que los servicios israelíes ignoraron múltiples señales de advertencia por sesgos analíticos y exceso de confianza, permitiendo la sorpresa inicial de Egipto y Siria. Como sostienen Black y Morris (1991), estos episodios consolidaron

⁹² El NATIS fue creado como el primer organismo permanente de comunicación y diplomacia pública de la OTAN. A través de campañas mediáticas, conferencias, materiales educativos y cooperación con embajadas aliadas, el NATIS integró la comunicación estratégica, las OPSIC y la diplomacia informativa, convirtiéndose en un antecedente directo de las actuales divisiones de *Strategic Communications* (STRATCOM) de la OTAN (Riso, 2015).

⁹³ El Aman (*Agaf Ha-Modi'in*) es la Dirección de Inteligencia Militar de las Fuerzas de Defensa de Israel (FDI), responsable del análisis estratégico, la recolección de inteligencia táctica y la planificación operativa. En conjunto con el Mossad y el Shin Bet, estas tres agencias conforman el núcleo del sistema israelí de inteligencia, caracterizado por una estrecha integración entre recolección, análisis y acción operativa, especialmente en contextos de conflicto asimétrico.

a la comunidad de inteligencia israelí como un actor estructural del sistema de defensa nacional y confirmaron que, en los conflictos asimétricos modernos, la inteligencia constituye el principal multiplicador de poder, capaz de convertir la información en disuasión y la previsión en supervivencia.

En ese sentido, la experiencia israelí fue un microcosmos de la transformación global que estaba gestándose, donde la inteligencia dejaba de ser un instrumento reactivo para convertirse en una forma de dominio cognitivo sobre la incertidumbre. Lo que en Oriente Medio se expresaba como anticipación táctica, en la Guerra Fría adquiría dimensión estructural, al integrar ciencia, tecnología y percepción dentro de un mismo sistema de control estratégico. De esta manera, los conflictos locales sirvieron como laboratorios de experimentación epistemológica que anticiparon la fusión entre información, seguridad y poder característica del orden bipolar.

En consecuencia, la Guerra Fría no fue todavía una GC en pleno sentido, pero sí el laboratorio donde comenzó a gestarse la centralidad del conocimiento como arma estratégica. La inteligencia funcionó como el sistema nervioso del nuevo orden mundial, regulando el flujo de información entre política, tecnología y percepción. Cada crisis (Berlín, Corea, Cuba), confirmó que dominar la información equivalía a dominar el conflicto. En ese proceso, la inteligencia no solo preparó el terreno para las guerras de cuarta generación, sino que las configuró intelectualmente, debido a que, al convertir el saber en poder, transformó la mente humana en el nuevo espacio de disputa.

Tras la crisis de los misiles en 1962, el equilibrio entre Estados Unidos y la URSS se transformó en un régimen permanente de observación mutua, por cuenta de los avances tecnológicos de los sesenta y setenta que expandieron de manera exponencial las capacidades de vigilancia. En efecto, los satélites KH-7 Gambit y KH-9 Hexagon, sucesores del programa *Corona*⁹⁴, llevaron la resolución óptica a nuevos niveles, mientras los sensores infrarrojos y los radares de apertura sintética permitieron observar incluso en condiciones de nubosidad o de noche. Graham y

⁹⁴ El programa *Keyhole* (KH) fue la serie sucesora del proyecto CORONA, concebida para perfeccionar la inteligencia satelital de los Estados Unidos a partir de la década de 1960. Bajo esta designación se agruparon distintos sistemas de reconocimiento orbital (KH-1 a KH-11) que incorporaron mejoras progresivas en resolución, alcance y transmisión. Los primeros modelos (KH-1 a KH-4) continuaban utilizando cápsulas de recuperación fotográfica, mientras que el KH-11, lanzado en 1976, introdujo por primera vez la transmisión digital en tiempo real de imágenes hacia estaciones terrestres, marcando la transición de la fotografía analógica al reconocimiento electro-óptico. Gracias a esta innovación, la IMINT se fusionó con la SIGINT y la GEOINT, dando origen a una vigilancia continua del planeta que redefinió la estrategia de disuasión y el control del equilibrio nuclear durante la Guerra Fría (Graham & Hansen, 2007).

Hansen (2007) subrayan que la observación orbital se convirtió en la forma más pura de conocimiento estratégico: una mirada que trascendía las fronteras políticas y la geografía, produciendo un tipo de saber omnisciente que convertía al planeta en un objeto de lectura permanente⁹⁵. Las imágenes ya no eran solo documentos visuales, sino insumos epistemológicos para la disuasión; saber dónde estaban los misiles, las bases o las pruebas nucleares era, en sí mismo, una forma de control político del miedo.

La NSA se consolidó como el corazón de esta nueva epistemología de la vigilancia. Su expansión tras 1952, y especialmente durante la Guerra de Vietnam, permitió convertir la interceptación de señales en una ciencia autónoma. El SIGINT global⁹⁶ no solo complementaba al espionaje humano, sino que lo reemplazaba como fuente principal de información estratégica. Satélites como los *Canyon* y *Rhyolite* interceptaban comunicaciones militares y diplomáticas desde órbitas geo sincrónicas, traduciendo conversaciones en conocimiento político. Como observa Sulick (2015), la Guerra Fría fue el primer conflicto donde el silencio (la ausencia de emisiones), podía interpretarse como un dato. En este nuevo paradigma, la inteligencia dejó de buscar únicamente hechos para concentrarse en patrones, correlaciones y probabilidades: era la era de la inferencia algorítmica antes del algoritmo digital.

En paralelo, la HUMINT continuaba desempeñando un papel crucial. A medida que las tecnologías hacían visible el espacio y el territorio, los seres humanos seguían siendo las únicas fuentes capaces de descifrar intenciones. El espionaje de campo, especialmente en Europa Oriental, se convirtió en un arte de la ambigüedad. El caso de Oleg Gordievsky, agente doble del KGB reclutado por el MI6 en la década de 1970, reveló la profundidad de la penetración occidental en las estructuras soviéticas. Gordievsky advirtió a los británicos sobre la paranoia del Kremlin durante la operación *Able Archer*⁹³, cuando Moscú interpretó un ejercicio de la OTAN como preparación para un ataque nuclear. Según Andrew (2010), su testimonio permitió calibrar la respuesta occidental y evitar una escalada accidental.

Ese giro cognitivo definió la esencia de la estrategia de disuasión. Las superpotencias ya no buscaban el secreto absoluto, sino la transparencia controlada, es decir, mostrar lo suficiente para intimidar y ocultar lo necesario para sobrevivir. En

⁹⁵ Los satélites KH-7, KH-9 y KH-11 proporcionaron imágenes de hasta 10 cm de resolución. El KH-11 (1976) introdujo la transmisión digital directa a estaciones terrestres (Graham & Hansen, 2007).

⁹⁶ La NSA desarrolló el sistema *Echelon* para interceptar comunicaciones globales. Su red de estaciones de escucha (Menwith Hill, Pine Gap, Waihopai) fue la base del posterior acuerdo *Five Eyes* (Sulick, 2015).

esta economía simbólica del saber, la información era al mismo tiempo un arma y parte del lenguaje diplomático. La inteligencia se convirtió en mediadora entre el conocimiento y la política, una gramática de la guerra que producía sentido antes que destrucción. Wheeler (2013) interpreta este fenómeno como el paso de la "inteligencia operativa" a la "inteligencia reflexiva", basado en la capacidad de pensar al enemigo pensando en cómo él pensaría en uno mismo, una doble hermenéutica del poder.

En la URSS, la inteligencia adoptó una forma diferente. Las *medidas activas* se transformaron en un instrumento esencial del KGB⁹⁷, las cuales, más que obtener secretos, buscaban moldear la percepción de las sociedades adversarias. Risso (2015) muestra cómo estas operaciones iban desde la creación de rumores hasta la infiltración de movimientos pacifistas y la manipulación mediática en Europa y América Latina. La inteligencia, en este sentido, se desplazó del dominio del conocimiento al dominio de la creencia, ya que no bastaba con saber, había que hacer creer. La propaganda soviética difundió narrativas sobre conspiraciones occidentales, racismo estadounidense y agresiones imperialistas, mientras promovía imágenes del modelo socialista como un orden moral superior. Era una guerra de significados, una confrontación semántica donde la verdad se volvía relativa al sistema político que la enunciaba.

En este clima de manipulación simbólica y desinformación estructural, la frontera entre realidad y ficción se volvió cada vez más difusa. Tanto en Oriente como en Occidente, los servicios de inteligencia comenzaron a operar dentro de un ecosistema de sospecha permanente, donde la verdad ya no se medía por los hechos, sino por la capacidad de controlarlos o negarlos. El espionaje dejó de ser un juego de suma cero para convertirse en una guerra psicológica de reflejos, donde la desconfianza era la única certeza posible. Las filtraciones del caso Penkovskiy en la URSS, el espionaje de Aldrich Ames y Robert Hanssen en la CIA y el FBI, o las desertiones de agentes dobles occidentales, evidenciaron que el conocimiento absoluto es una ilusión peligrosa. Cada servicio de inteligencia se convirtió en su propio adversario potencial, atrapado en la lógica del espejo infinito: observar y ser observado, engañar y ser engañado. Andrew (2010) lo resume afirmando que la Guerra

⁹⁷ El KGB definía las *aktivnye meropriyatiya* como "acciones políticas encubiertas" que incluían falsificación de documentos, manipulación de prensa, infiltración cultural y financiamiento de grupos de influencia (Risso, 2015).

Fría fue “una guerra de confianza en la que nadie confiaba en nadie” (p. 638)⁹⁸. El conocimiento se volvió autorreferencial, un círculo donde la certeza era imposible, y la duda, la única forma de seguridad.

Hacia finales de los años setenta, la inteligencia comenzó a transitar con mayor determinación hacia la ingeniería informacional. Uno de sus antecedentes más significativos fue el *Proyecto Mockingbird*, una operación secreta de la CIA iniciada a finales de los años cuarenta y desarrollada durante las décadas de 1950 y 1960, cuyo propósito era influir en los medios de comunicación nacionales e internacionales con fines políticos y estratégicos. Su misión consistió en moldear la opinión pública y contrarrestar la propaganda soviética mediante la infiltración de periodistas, la financiación encubierta de agencias de noticias y la cooperación con directores de medios en Europa, América Latina y Estados Unidos. De acuerdo con Bernstein (1977), al menos 400 periodistas colaboraron directa o indirectamente con la CIA durante este tiempo, y si bien el programa fue desmantelado a mediados de los setenta tras las investigaciones del *Comité Church*⁹⁹, dejó en clara evidencia la dimensión mediática de la Guerra Fría y el papel de la información como instrumento de poder cultural y cognitivo.

Con el avance de la computación y el surgimiento de Arpanet a finales de los sesenta, la inteligencia comenzó a migrar progresivamente hacia el dominio digital. Lo que en la Guerra Fría había sido una lucha por controlar narrativas en la prensa convencional, empezó a transformarse en una competencia por dominar los flujos de información interconectados. Los primeros nodos de Arpanet (concebidos por la DARPA como una red militar y académica descentralizada), abrieron el camino a nuevas formas de recolección, transmisión y análisis de datos en tiempo real. En este contexto emergió una ciberinteligencia incipiente (CIBINT), orientada a explorar las vulnerabilidades de las redes, interceptar comunicaciones electrónicas y anticipar amenazas en el entorno informático naciente. Así, la guerra por el sentido y la información comenzó a expandirse más allá de los medios tradicionales hacia los espacios digitales que preludiaban el ciberespacio.

⁹⁸ Andrew (2010) utiliza esta expresión para describir la paradoja de la seguridad en la comunidad de inteligencia, en donde cuanto mayor es el conocimiento, mayor la sospecha recíproca.

⁹⁹ El Comité Church fue una comisión especial del Senado de los Estados Unidos, creada en 1975 y presidida por el senador Frank Church, con el objetivo de investigar los abusos cometidos por las agencias de inteligencia estadounidenses (principalmente la CIA, el FBI y la NSA), desde el final de la Segunda Guerra Mundial. Sus audiencias públicas revelaron prácticas ilegales de espionaje interno, experimentos de control mental (MK-Ultra), operaciones de asesinato político y manipulación mediática, lo que llevó a una profunda reforma del sistema de inteligencia y a la creación de los actuales mecanismos de supervisión legislativa.

El legado de la inteligencia durante la Guerra Fría dejó una infraestructura técnica sin precedentes (satélites, redes SIGINT, agencias multinacionales) que configuró la arquitectura informacional del mundo contemporáneo. E instauró una forma de racionalidad estratégica basada en la administración del conocimiento. La inteligencia ya no era un medio para librar guerras, sino un método para evitarlas. En esa transformación terminaría residiendo su dimensión epistemológica, caracterizado por el paso de la violencia física a la violencia semiótica, del dominio del espacio al dominio de la mente. Como señaló Kent (1965), la función suprema del conocimiento estratégico no es predecir el futuro, sino impedir el desastre.

La Guerra Fría convirtió esa máxima en una política de Estado y, sin saberlo, inauguró la era de la GC. Así, el saber estratégico se desplazó del control de las armas al control de las narrativas, del equilibrio nuclear a la manipulación semántica, inaugurando la era de la guerra informacional y cognitiva digital: un conflicto sin fronteras donde conocer equivale a dominar, y donde la epistemología del poder se confunde definitivamente con la arquitectura de la información. El fin de la Guerra Fría no representó una victoria militar, sino una victoria cognitiva. La URSS no fue derrotada a través de las armas, sino por la erosión de su propio relato. La desinformación, la propaganda y la censura ya no pudieron sostener el sistema ante el flujo de información global que Occidente dominaba. En términos de conocimiento estratégico, la caída del Muro de Berlín simbolizó el triunfo de la transparencia sobre el secreto, del flujo sobre el control de la información.

Inteligencia y guerras de quinta generación

La inteligencia ha dejado de ser un subsistema auxiliar de la estrategia militar, política y económica para convertirse en su núcleo operativo. En las guerras de quinta generación, la información ya no representa el mundo: lo construye. La batalla contemporánea se libra en el terreno de la interpretación, donde la ventaja no depende únicamente de quién posee más datos, sino de quién define su sentido. El poder se mide por la capacidad de modelar percepciones, anticipar reacciones y alterar las cogniciones colectivas mediante operaciones que integran tecnología, cultura y psicología.

La guerra de quinta generación representa la culminación del proceso evolutivo de la guerra hacia dominios intangibles y conectivos. A los escenarios tradicionales terrestre, marítimo, aéreo y espacial se suman ahora el ciberespacial y

el cognitivo, donde la información, la percepción y la emoción se convierten en instrumentos de combate. El mecanismo de derrota ya no depende de la destrucción física del adversario, sino de su implosión interna mediante el ciberchoque, entendido como la parálisis simultánea de sus sistemas informáticos, comunicacionales y mentales (Álvarez et al., 2017).

Los actores de esta nueva forma de conflicto no operan de manera jerárquica, sino en redes distribuidas, interconectadas y adaptativas, capaces de coordinar acciones cinéticas y no cinéticas en múltiples planos de la realidad. En este contexto, la guerra deja de ser un enfrentamiento visible entre ejércitos y se transforma en una competencia por el control del entorno informacional y de la mente humana. En consecuencia, la inteligencia evoluciona hacia un ecosistema adaptativo de conocimiento estratégico, sustentado en la convergencia entre ciberinteligencia (CYBINT), inteligencia social mediática (SOCMINT), inteligencia cognitiva (COGINT) y la inteligencia reflexiva. Estas dimensiones combinan lo técnico y lo simbólico, lo humano y lo algorítmico, en una red donde la decisión se convierte en el principal objetivo de influencia.

El marco conceptual del *poder astuto*, formulado por Álvarez et al. (2018), sintetiza esta nueva lógica, al integrar el poder inteligente con el engaño, la manipulación y la adaptabilidad estratégica para dominar el espacio cognitivo. En las GC, el poder astuto no solo defiende la mente, sino que la utiliza como arma. Desde esta perspectiva, la inteligencia contemporánea ya no busca únicamente conocer al enemigo, sino inducirlo a decidir dentro de un marco diseñado por quien observa. La comprensión de esta transformación exige analizar, primero, cómo la inteligencia ha pasado del entorno informacional al dominio cognitivo, donde la comunicación, los algoritmos y la automatización reconfiguran la manera misma de producir conocimiento estratégico.

De la información al dominio cognitivo: inteligencia, comunicación y algoritmos

El tránsito de la información al dominio cognitivo ha redefinido la esencia misma de la inteligencia. Si durante la Guerra Fría el conocimiento estratégico se estructuraba como una pirámide jerárquica y secretista, en la actualidad adopta la forma de un entramado distribuido, donde el dato circula en tiempo real y el poder se mide por la capacidad de interpretarlo antes que por el monopolio de poseerlo. La información ya no es una sustancia externa al conflicto, sino su terreno constitutivo. Como advierte Zegart (2022), la digitalización ha diluido la frontera entre

el espionaje y la sociedad civil, haciendo que los algoritmos, las plataformas y los flujos de datos se conviertan en los nuevos espacios de disputa estratégica.

Esta transformación ha modificado la ontología de la inteligencia, que ya no se limita a producir conocimiento sobre el mundo, sino que interviene directamente en su creación. Pieter de Werd (2021) denomina a este proceso “inteligencia reflexiva”, aludiendo a la capacidad de los sistemas de información para observarse, corregirse y adaptarse de acuerdo con los efectos que generan. En este sentido, la inteligencia se comporta como un sistema cognitivo complejo, donde la retroalimentación constante sustituye a la linealidad de la información clásica. La veracidad de los datos importa menos que su capacidad de orientar la acción o de modificar la conducta de los sujetos a los que se dirige.

El surgimiento de las redes descentralizadas de información ha sustituido la lógica vertical de la guerra industrial por una estructura reticular más cercana al modelo biológico. Sparrow (1991) y Koschade (2006) demostraron que el análisis de redes aplicado a la inteligencia criminal y antiterrorista permite comprender la resiliencia de organizaciones descentralizadas como Jemaah Islamiyah¹⁰⁰, donde la redundancia de nodos garantiza la supervivencia del sistema. En la GC contemporánea, el enemigo ya no se concentra en un territorio o una jerarquía, sino en una constelación de actores distribuidos que aprenden, comparten y actúan en red. Por eso, la inteligencia moderna requiere de las arquitecturas analíticas capaces de capturar patrones, interacciones y dinámicas relacionales antes que posiciones fijas o jerarquías formales.

En este nuevo entorno, la comunicación deja de ser un instrumento subordinado a la inteligencia para convertirse en su componente estructural. Las redes sociales, los medios digitales y la interacción algorítmica entre usuarios generan un flujo constante de señales que, analizadas adecuadamente, permiten inferir estados de ánimo colectivos, intenciones políticas o vulnerabilidades cognitivas. Para Owen (2017), el monitoreo de los movimientos sociales a través de medios digitales ha transformado la vigilancia en un discurso de orden político, donde la observación y el control se justifican en nombre de la estabilidad; de ahí que el

¹⁰⁰ Jemaah Islamiyah es una organización islamista radical fundada a fines de la década de 1980 en el sudeste asiático por Abu Bakar Bashir y Abdullah Sungkar, con el objetivo de establecer un califato regional que abarcara Indonesia, Malasia, Singapur, el sur de Filipinas y el sur de Tailandia. Vinculada operativamente con Al Qaeda, fue responsable de varios atentados, entre ellos el ataque con bombas en Bali en 2002 que dejó más de 200 muertos. Su estructura en red, altamente descentralizada, permitió su supervivencia frente a la presión estatal y la convirtió en un caso paradigmático para el estudio del terrorismo en red y la inteligencia antiterrorista (Koschade, 2006).

análisis de entornos comunicacionales se haya convertido en una forma de inteligencia anticipatoria, cuyo objetivo es detectar tendencias antes de que se manifiesten abiertamente.

El paso siguiente en esta evolución es la automatización del conocimiento. Brantly (2018) advierte que en la era del aprendizaje automático, todo se convierte en inteligencia. Los sistemas de *machine learning* (ML) procesan volúmenes de datos imposibles para un analista humano y generan inferencias probabilísticas que modifican tanto la producción como la interpretación del conocimiento estratégico. Por lo tanto, este cambio introduce un dilema epistemológico, pues el juicio humano queda subordinado a modelos opacos que aprenden sin explicar, y el riesgo no es solo técnico, sino cognitivo, ya que los algoritmos pueden replicar sesgos, fabricar correlaciones ilusorias y amplificar creencias colectivas¹⁰¹, convirtiendo la inteligencia en una forma de automatización del error.

La consolidación de estas tecnologías ha favorecido la aparición de nuevas tipologías de redes de ciberinteligencia. Kalkman y Wieskamp (2019) clasifican estas redes en cuatro categorías, que reflejan la coexistencia de modelos centralizados y colaborativos en la gestión del conocimiento de seguridad (Tabla 13). Las *redes cooperativas* se fundamentan en la confianza entre actores que comparten voluntariamente datos y análisis, siendo útiles en contextos de colaboración internacional o interinstitucional. Las *redes jerárquicas* mantienen un flujo vertical de información controlado por una autoridad central, lo que garantiza coherencia operativa, aunque reduce flexibilidad. Las redes híbridas combinan coordinación central con nodos autónomos que intercambian inteligencia de manera lateral, lo que favorece la resiliencia ante ataques o interrupciones. Finalmente, las redes distribuidas funcionan sin un centro de control fijo, operando a través de múltiples nodos interconectados que actúan simultáneamente como productores y consumidores de conocimiento.

¹⁰¹ Los sistemas de aprendizaje automático tienden a replicar sesgos cognitivos cuando reproducen los patrones discriminatorios presentes en sus datos de entrenamiento, trasladando prejuicios humanos al cálculo estadístico. Asimismo, pueden fabricar correlaciones ilusorias al identificar relaciones espurias entre variables que coexisten sin vínculo causal, interpretando coincidencias como causalidades. Finalmente, tienden a amplificar creencias colectivas al reforzar, mediante bucles de retroalimentación algorítmica, aquellas narrativas o interpretaciones que dominan el entorno informacional, consolidando percepciones mayoritarias como si fueran verdades empíricas. Este conjunto de distorsiones constituye lo que Floridi (2015) ha descrito como una *degradación semántica del entorno informacional*, donde la abundancia de datos erosiona la calidad del conocimiento. En términos de inteligencia reflexiva, De Werd (2021) advierte que tales errores se internalizan dentro de los propios sistemas de observación, produciendo una ilusión de objetividad que oculta los mecanismos de poder cognitivo sobre los que opera la inteligencia automatizada.

Tabla 13. *Tipología de redes de ciberinteligencia*

Tipo de red	Estructura organizativa	Características principales	Ventajas estratégicas	Limitaciones o vulnerabilidades
Redes cooperativas	Basadas en la colaboración horizontal y en la confianza mutua entre actores estatales, privados o académicos.	Intercambio voluntario de datos e información; gestión compartida del conocimiento y apoyo recíproco.	Fomentan la cooperación internacional, la interoperabilidad y la construcción de confianza entre instituciones.	Dependencia de la reciprocidad y riesgo de filtraciones si falla la seguridad informacional.
Redes jerárquicas	Estructura vertical con autoridad central y flujos descendentes de información.	Procesos de inteligencia unificados bajo supervisión; centralización del análisis y la toma de decisiones.	Garantizan coherencia analítica, control de calidad y alineación doctrinal.	Menor flexibilidad ante entornos cambiantes y respuesta más lenta ante amenazas dinámicas.
Redes híbridas	Combinan elementos jerárquicos y cooperativos, permitiendo interacción lateral entre nodos autónomos.	Integran actores públicos y privados en una arquitectura mixta de control y colaboración.	Elevada resiliencia estructural, adaptabilidad y sinergia entre niveles estratégicos y operativos.	Riesgo de duplicación de esfuerzos, tensiones de coordinación y problemas de interoperabilidad técnica.
Redes distribuidas	No poseen un centro de control fijo; cada nodo actúa simultáneamente como emisor, receptor y analista.	Flujo continuo de información entre múltiples nodos interconectados; autoorganización y autonomía decisional.	Alta redundancia, velocidad de respuesta y resistencia ante ataques o interrupciones.	Dificultad para verificar la calidad de la información y ausencia de mecanismos claros de trazabilidad o rendición de cuentas.

Fuente: Elaboración propia según Kalkman y Wieskamp (2019)

En guerras de quinta generación, esta diversidad es esencial para garantizar agilidad adaptativa. Las redes cooperativas permiten compartir información entre agencias, las híbridas integran datos públicos y privados, y las distribuidas conectan actores estatales y no estatales en una misma arquitectura de vigilancia y respuesta. La inteligencia deja así de ser un monopolio estatal para convertirse en un proceso de coproducción global.

Esta apertura del campo informacional explica la expansión de la OSINT¹⁰². De acuerdo con Block (2023), la inteligencia de fuentes abiertas no es una innovación

¹⁰² OSINT (*Open Source Intelligence*) se refiere a la obtención, análisis y uso de información disponible públicamente con fines de seguridad o toma de decisiones estratégicas. Incluye datos procedentes de medios de comunicación, redes sociales, publicaciones académicas, bases gubernamentales abiertas, imágenes satelitales y fuentes digitales accesibles. A diferencia de las disciplinas secretas de inteligencia, la OSINT se basa en la transparencia informacional y en la capacidad analítica para transformar el conocimiento público en ventaja estratégica. Según Block (2023), su desarrollo histórico evidencia la progresiva democratización del

reciente, sino la culminación de un proceso histórico en el que la sociedad civil fue apropiándose progresivamente de los medios de comunicación y de los flujos de conocimiento público. Desde la prensa impresa del siglo XIX hasta las plataformas digitales contemporáneas, cada revolución mediática amplió el acceso a la información y redujo el monopolio estatal sobre la observación del mundo. Durante la Guerra Fría, los analistas ya producían evaluaciones estratégicas a partir de materiales disponibles públicamente (como los discursos, estadísticas económicas, fotografías satelitales), demostrando que el poder informacional no dependía solo del secreto, sino también de la capacidad interpretativa.

En la era digital, este principio se radicaliza. La abundancia de datos, la ubicuidad de las redes y las herramientas de análisis accesibles a cualquier usuario han convertido a la ciudadanía, los medios y las organizaciones independientes en actores activos de la producción de inteligencia. Por lo tanto, la OSINT encarna una forma de democratización del conocimiento estratégico, pero también introduce nuevos riesgos de manipulación, sobreexposición y desinformación que obligan a repensar los límites entre lo público y lo confidencial (Tabla 14).

Tabla 14. *Cronología histórica del desarrollo del OSINT*

Periodo histórico	Hito o transformación principal	Características y relevancia estratégica
Década de 1940	Creación del <i>Foreign Broadcast Information Service</i> (FBIS) en 1941	Durante la Segunda Guerra Mundial, Estados Unidos estableció el FBIS para recopilar y analizar emisiones radiales extranjeras. Este modelo marcó el origen institucional de la inteligencia de fuentes abiertas al integrar monitoreo mediático con análisis lingüístico y político.
Décadas de 1950-1970	Consolidación de la OSINT durante la Guerra Fría	Las agencias de inteligencia comenzaron a utilizar prensa, publicaciones científicas y material audiovisual para evaluar la capacidad industrial y militar de los adversarios. Se institucionaliza la idea de que la observación pública puede generar conocimiento estratégico.
Década de 1980	Difusión del concepto "open source" en el ámbito tecnológico y de seguridad	La expansión de los medios satelitales y la informatización de los archivos públicos transformaron el acceso a la información global. Aparece la noción de inteligencia civil complementaria al espionaje clásico.
Década de 1990	Digitalización y expansión de Internet	El nacimiento de la web global convierte a la OSINT en un componente esencial del ciclo de inteligencia. Surgen las primeras empresas privadas de análisis de información pública, como Jane's o Stratfor, y se multiplican las bases de datos en línea.

Continúa tabla...

poder informativo y la creciente competencia entre actores estatales, privados y ciudadanos por el control de la interpretación de los hechos.

Periodo histórico	Hito o transformación principal	Características y relevancia estratégica
Década de 2000	Auge de las redes sociales y del análisis en tiempo real	Plataformas como Twitter, YouTube y Facebook crean un flujo incesante de información georreferenciada y audiovisual. La OSINT se fusiona con la inteligencia social mediática (SOCMINT) y se integra en operaciones militares y humanitarias.
Década de 2010	Automatización del análisis de fuentes abiertas	La incorporación de algoritmos de minería de texto, aprendizaje automático y visualización de datos permite procesar grandes volúmenes de información pública. La frontera entre analista humano y sistema automatizado comienza a difuminarse.
Década de 2020 en adelante	OSINT algorítmica y ecosistemas colaborativos de inteligencia	Las comunidades civiles, medios de verificación y analistas independientes emplean IA y geolocalización para investigar conflictos en tiempo real (por ejemplo, Bellingcat). El OSINT se consolida como una práctica global de transparencia y control social, pero también como un terreno de disputa cognitiva en la guerra informacional.

Fuente: Elaboración propia según Block (2023)

Dentro de esta lógica emergente, la inteligencia social mediática o SOCMINT¹⁰³ ocupa un lugar central. Omand et al. (2012) la definieron como el aprovechamiento sistemático de la información que circula en redes sociales para la seguridad nacional. Dover (2019) amplía esta definición al reconocer que el poder de la SOCMINT reside en su capacidad para equilibrar las oportunidades de vigilancia con la necesidad de legitimidad democrática. A diferencia del espionaje tradicional, la SOCMINT no se basa en la intrusión, sino en la observación abierta de la interacción social, lo que la convierte en un laboratorio del comportamiento colectivo. Su verdadero valor radica en la posibilidad de detectar, a partir de la conversación digital, las variaciones emocionales y semánticas que anticipan estallidos sociales, campañas de desinformación o cambios de percepción pública.

Por consiguiente, la inteligencia contemporánea se construye en la intersección entre tecnología, cognición y comunicación. Ya no es un ejercicio reservado a analistas o agencias, sino un ecosistema en el que cada usuario contribuye, conscientemente o no, a la producción de conocimiento estratégico. En las guerras de

¹⁰³ SOCMINT (*Social Media Intelligence*) es la disciplina que aplica métodos de inteligencia al análisis de información generada en redes sociales y plataformas digitales. Su propósito es identificar patrones de comportamiento, dinámicas emocionales y narrativas emergentes dentro de comunidades virtuales. Omand, et al. (2012) la definen como la primera forma de inteligencia originada en un entorno enteramente civil, donde la interacción digital reemplaza al espionaje tradicional como fuente principal de observación social. Posteriormente, Dover (2019) subraya que su valor estratégico reside en la posibilidad de detectar cambios en el sentimiento público y anticipar crisis políticas, pero advierte que su práctica plantea dilemas éticos y legales vinculados con la vigilancia de la ciudadanía y la privacidad informacional.

quinta generación, los algoritmos no sustituyen a los espías, sino que los complementan, ampliando su alcance y velocidad analítica. Las redes sociales actúan como sensores distribuidos y la mente humana se convierte en el objetivo final de la superioridad informacional. El dominio cognitivo emerge así como el nuevo teatro de operaciones, donde vencer significa controlar la atención, condicionar la interpretación y alterar el flujo de la verdad.

Ciberinteligencia, vigilancia global y control reflexivo

El salto hacia la ciberinteligencia representa una ampliación del campo operativo de la inteligencia. Ya no se trata únicamente de proteger las infraestructuras informáticas, sino de comprender y anticipar comportamientos que emergen del espacio digital. Como advierte Price (2015), la ciberinteligencia combina disciplinas técnicas, analíticas y conductuales para producir conocimiento accionable sobre amenazas en evolución. En las guerras de quinta generación, este conocimiento se integra con la seguridad nacional, la economía y la política exterior, convirtiendo el ciberespacio en un terreno donde la información, la infraestructura y la mente se entrelazan.

Mattern et al. (2014) describen tres niveles operacionales de la ciberinteligencia: 1) el táctico, orientado a la detección de intrusiones y vulnerabilidades; 2) el operacional, centrado en comprender las campañas y patrones de ataque; y 3) el estratégico, enfocado en anticipar la intención y la capacidad de los adversarios. Este modelo demuestra que la ciberinteligencia no es simplemente una actividad reactiva, sino una disciplina que busca generar alertas anticipadas a partir del análisis integrado de información técnica, conductual y geopolítica. La *kill chain cibernética*¹⁰⁴ ilustra ese principio, en el cual cada ataque es una secuencia de acciones que puede interrumpirse si se identifica su patrón preparatorio. Detectar el momento en que el adversario pasa de la observación a la intención constituye el verdadero objetivo de la inteligencia digital.

¹⁰⁴ El concepto de *kill chain cibernética* fue desarrollado por Eric Hutchins, Michael Cloppert y Rohan Amin en el seno del Lockheed Martin Computer Incident Response Team (2011) como una adaptación del modelo militar tradicional de secuencia de ataque a los entornos digitales. Describe las fases que un adversario debe completar para ejecutar con éxito una intrusión informática: reconocimiento del objetivo, armamento o preparación de herramientas, entrega del vector de ataque, explotación de vulnerabilidades, instalación de malware, establecimiento de comando y control, y ejecución de acciones sobre el objetivo. La utilidad de este enfoque reside en que cada eslabón de la cadena ofrece una oportunidad de detección o interrupción, permitiendo transformar la defensa cibernética en una práctica de inteligencia proactiva. En el contexto de la ciberinteligencia, la *kill chain* no solo identifica la progresión técnica del ataque, sino que revela su dimensión cognitiva, ya que cada fase implica decisiones, aprendizajes y adaptaciones por parte del agresor.

Cabe señalar que la evolución reciente de la ciberinteligencia ha incorporado un componente automatizado que redefine el papel del analista de inteligencia. Como explica Kuzmiakova (2025), la *cyber threat intelligence* contemporánea se sustenta en sistemas de automatización que combinan minería de amenazas, correlación de indicadores y análisis de comportamiento adversario mediante aprendizaje automático. Kuzmiakova (2025) advierte que la automatización no busca reemplazar el juicio humano, sino aumentar su capacidad para identificar patrones ocultos y reducir los tiempos de respuesta ante incidentes complejos. En consecuencia y en este nuevo ecosistema, la inteligencia deja de depender exclusivamente de la interpretación individual para convertirse en una arquitectura de detección colaborativa entre humanos y máquinas, donde cada alerta representa una hipótesis que debe ser verificada por la razón analítica.

En la práctica, esta convergencia técnica y analítica requiere un marco de trabajo preciso. Tilmar (2024) sostiene que la ciberinteligencia efectiva comienza en la cadena forense digital, donde la recolección, preservación y análisis de datos constituyen el punto de partida de toda inferencia estratégica. Su enfoque operacional describe la *kill chain* cibernética y el *Diamond Model* como estructuras que permiten organizar el conocimiento y detectar vulnerabilidades antes de que se materialicen los ataques. Para Tilmar (2024), la clave no reside únicamente en descubrir evidencias, sino en “darles sentido”, al conectar trazabilidad digital con motivaciones humanas e intenciones tácticas del adversario. Esta dimensión interpretativa transforma la evidencia técnica en conocimiento estratégico, integrando la ciberforensia dentro del ciclo completo de inteligencia.

El contexto histórico de este proceso ha sido descrito con lucidez por Price (2015), quien rastrea el surgimiento de la ciberinteligencia desde los primeros sistemas informáticos militares de los años sesenta hasta su consolidación como disciplina autónoma del espionaje digital. Price destaca que la transición de la inteligencia humana (HUMINT) a la inteligencia cibernética (CYBINT) no implicó una ruptura, sino una traslación del *tradecraft* clásico al entorno digital. Las operaciones encubiertas, la infiltración de sistemas, la validación de fuentes o el control de agentes encuentran hoy su correlato en *bots*, *malware*, *honeypots* y *backdoors*, configurando una continuidad entre espionaje humano y automatizado. En este sentido, la ciberinteligencia moderna hereda la lógica del espionaje tradicional, pero la escala, la velocidad y la opacidad de los entornos digitales multiplican sus efectos cognitivos y geopolíticos.

La integración de estas perspectivas revela que la ciberinteligencia no es únicamente una función técnica, sino un ecosistema cognitivo adaptativo, donde la automatización, el análisis forense y la herencia del espionaje clásico confluyen para sostener la seguridad informacional del Estado. En la era algorítmica, la superioridad estratégica depende de la capacidad para aprender más rápido que el adversario, fusionando la inferencia humana con la predicción automatizada. Para Gentry (2022), la ciberinteligencia adquiere valor estratégico cuando actúa como un sistema de advertencia temprana capaz de reducir la incertidumbre antes de la agresión. La clave está en pasar de la vigilancia del evento al análisis del comportamiento. Esto exige integrar las variables técnicas (*malware*, infraestructura, metadatos), con las variables humanas (motivaciones, creencias, emociones). La combinación de ambos planos configura una inteligencia conductual y predictiva, en la que el ataque cibernético se interpreta como la expresión final de un proceso cognitivo identificable.

El incremento de la interdependencia digital ha generado también una arquitectura global de vigilancia distribuida. El *Five Eyes* constituye la red cooperativa más avanzada para la interceptación de señales y el intercambio de inteligencia, combinando capacidades de vigilancia masiva con mecanismos de cooperación transnacional que trascienden los límites jurídicos tradicionales. Zegart (2022) explica que estas alianzas han desdibujado la frontera entre espionaje exterior y control interno, ampliando el poder estatal para observar tanto a sus adversarios como a sus propios ciudadanos.

La proliferación de actores privados ha reforzado este fenómeno. Work (2020) afirma que las empresas de inteligencia comercial se han convertido hoy en un pilar del ecosistema informacional contemporáneo, proporcionando análisis de amenazas y gestión de riesgos, así como el monitoreo de datos que complementan (y a veces sustituyen) las capacidades estatales. Este proceso produce una "hibridación del secreto", donde la información sensible circula entre las corporaciones, agencias y contratistas bajo lógicas de mercado. El conocimiento estratégico se transforma así en un recurso económico y la inteligencia en un servicio.

En este nuevo ecosistema, la frontera entre informar, persuadir y disuadir se ha vuelto difusa. Como demuestran Buluc et al. (2024), la antes rígida separación entre inteligencia y comunicación estratégica se quebró en los meses previos a la invasión rusa de Ucrania, cuando los gobiernos occidentales decidieron revelar selectivamente datos de inteligencia con el propósito explícito de moldear percepciones. Esta práctica, denominada inteligencia pública, representó un giro histórico:

la información clasificada fue utilizada no como insumo interno de decisión, sino como instrumento narrativo dirigido al público internacional, a la prensa y, sobre todo, al adversario. Su finalidad no era únicamente advertir o prevenir, sino influir anticipadamente en el marco interpretativo del conflicto, imponiendo una versión de la realidad antes de que los hechos se produjeran.

Tal como argumentan Buluc et al. (2024), esta estrategia de “divulgación disuasiva” respondió a una lógica propia de la GC: la lucha por el significado antecede a la lucha por el territorio. La revelación de inteligencia (presentada como transparencia), se convirtió en un acto performativo que buscaba legitimar la narrativa occidental y deslegitimar de antemano la narrativa rusa. En otras palabras, el secreto no se rompió, sino que se reconfiguró como arma simbólica; su valor no residía ya en ocultar información, sino en proyectarla de forma calibrada para alterar los cálculos, las emociones y las creencias del público y del enemigo.

Este episodio evidenció que la inteligencia contemporánea ya no se define solo por su capacidad de recolectar información privilegiada, sino por su habilidad de gestionar la credibilidad en entornos saturados de datos. En el contexto de la hipertransparencia digital, la autoridad cognitiva se convierte en el principal campo de disputa: quien logra imponer el relato sobre “qué es verdad” adquiere ventaja estratégica. Así, la inteligencia transita del dominio del secreto al de la persuasión estructural, donde los informes clasificados y las filtraciones controladas son componentes de una misma ecología de influencia. En este sentido, la inteligencia moderna actúa menos como una práctica de vigilancia y más como un arte de escenificación del conocimiento, un modo de intervenir en la percepción colectiva para orientar la acción política y militar.

Asimismo, el crecimiento de la vigilancia digital plantea un dilema epistemológico y ético. La expansión de los sistemas de recolección masiva de datos promete seguridad, pero también genera lo que De Werd (2021) denomina una “inteligencia reflexiva”, donde los mecanismos de observación se retroalimentan de sus propios efectos. En otras palabras, cuanto más se observa, más se modifica el entorno observado. La línea entre conocer y provocar se vuelve difusa, y esta reflexividad produce una forma de poder cognitivo que no solo analiza realidades, sino que las crea al definir qué debe considerarse amenaza.

El caso ruso ilustra la dimensión activa de esta lógica. Varzhanskyi (2024) muestra cómo la doctrina del control reflexivo busca inducir decisiones erróneas en el adversario mediante la manipulación de información verosímil. Las operaciones rusas en el conflicto con Ucrania demuestran que la desinformación no

pretende simplemente confundir, sino reconfigurar el proceso de percepción y análisis del enemigo.

Un ejemplo de ello ocurrió durante las semanas previas a la invasión en febrero de 2022, cuando Moscú difundió señales contradictorias sobre sus intenciones estratégicas, combinando anuncios públicos de retirada de tropas con una acumulación simultánea de fuerzas en la frontera oriental. Este patrón de comunicación fue diseñado intencionalmente para provocar interpretaciones equivocadas dentro de los servicios de inteligencia occidentales y ucranianos, generando así una falsa sensación de margen diplomático mientras se preparaba el ataque militar. De igual modo, la circulación masiva de narrativas sobre “operaciones de liberación” o supuestas agresiones ucranianas en Donbás buscó moldear la percepción internacional y justificar la acción militar bajo el marco de una defensa preventiva. El control reflexivo convierte así a la inteligencia en una forma de GC, donde el objetivo no es censurar el conocimiento, sino redirigirlo estratégicamente para que el adversario actúe conforme a los intereses del emisor.

El uso de las fuentes abiertas amplifica este fenómeno. Flamer (2023) analiza el modo en que organizaciones no estatales, como Hamas, emplearon la OSINT para obtener ventaja en inteligencia táctica, utilizando imágenes satelitales, redes sociales y medios abiertos para rastrear movimientos enemigos. Un ejemplo ilustrativo de esta dinámica ocurrió durante el conflicto de Gaza de 2012, cuando las brigadas al-Qassam monitorizaron las publicaciones de soldados israelíes en redes sociales y las imágenes difundidas por medios internacionales para inferir la ubicación de unidades y el tipo de armamento desplegado¹⁰⁵.

Flamer (2023) señala que los analistas de Hamas lograron correlacionar patrones de movimiento vehicular con fotografías geolocalizadas, permitiéndoles ajustar posiciones de lanzamiento de los cohetes y anticipar ataques aéreos. Este caso demuestra que la ciberinteligencia es un campo disputado, donde la asimetría tecnológica puede compensarse con agilidad informacional, ya que los datos públicos, combinados con análisis contextual, conocimiento local y creatividad

¹⁰⁵ Hamas, acrónimo de *Harakat al-Muqāwama al-Islāmiyya* (Movimiento de Resistencia Islámica), surgió en 1987 como una derivación de la Hermandad Musulmana durante la Primera Intifada palestina. Su brazo armado, las Brigadas Izz ad-Din al-Qassam, consolidó progresivamente una estructura de inteligencia interna denominada Majd (abreviatura de *Mudiriyyat al-Jihaz al-Amn al-Dakhili*), responsable de contrainteligencia, seguridad interna y recolección de información sobre las fuerzas israelíes. Según Flamer (2023), esta organización ha evolucionado hacia un sistema híbrido de vigilancia y análisis que combina métodos tradicionales de espionaje con la explotación sistemática de fuentes abiertas. Su capacidad para integrar la OSINT en operaciones tácticas demuestra cómo los actores no estatales pueden desarrollar ecosistemas de inteligencia adaptativos sin depender de infraestructura tecnológica avanzada.

operativa, pueden equilibrar temporalmente la balanza entre actores estatales y no estatales, convirtiendo a la OSINT en un multiplicador de poder cognitivo en la guerra contemporánea.

Sin embargo, el dominio tecnológico no basta para comprender el alcance de la ciberinteligencia. Duyvesteyn (2013) advierte que toda práctica de inteligencia se inscribe en una cultura estratégica, entendida como el conjunto de creencias, normas y hábitos que orientan la manera en que los Estados perciben y utilizan la información. Uhlmann (2022) confirma esta tesis al demostrar que, en el caso israelí, la securitización del conocimiento lingüístico árabe generó efectos paradójicos, ya que la dependencia excesiva de la traducción técnica debilitó la comprensión cultural del enemigo. En otras palabras, la inteligencia desprovista de contexto se vuelve miope. Por eso, Yelamos et al. (2022) subrayan la necesidad de una inteligencia cultural, capaz de integrar las dimensiones simbólicas, históricas y morales de las sociedades observadas.

Patton (2010) desarrolló esta idea en su propuesta de SOCINT¹⁰⁶, una disciplina emergente que busca comprender los entornos humanos y culturales en los que operan los actores estratégicos. A diferencia de la inteligencia tradicional, centrada en capacidades materiales y datos cuantificables, la SOCINT se orienta al estudio de los factores intangibles que configuran el comportamiento colectivo, como los valores, identidades, creencias, códigos morales, estructuras de parentesco, instituciones locales y mitologías políticas.

Su propósito es ofrecer una comprensión profunda de cómo las sociedades interpretan la autoridad, el conflicto y la legitimidad. De acuerdo con Patton (2010), la SOCINT debe combinar la observación etnográfica con el análisis geopolítico, integrando conocimiento antropológico y análisis estratégico para anticipar las reacciones sociales ante decisiones militares o campañas informativas. Esta perspectiva permitió a las fuerzas estadounidenses en Irak y Afganistán reconocer que

¹⁰⁶ La SOCINT (*Sociocultural Intelligence*) surgió a mediados de la década de 2000 como una extensión de la HUMINT dentro del Departamento de Defensa de los Estados Unidos, con el propósito de comprender los contextos sociales, culturales y religiosos en los que operan las fuerzas militares. Su desarrollo institucional se vinculó al *Human Terrain System* (HTS), programa implementado en Irak y Afganistán para integrar antropólogos, sociólogos y analistas culturales en las unidades de combate. Como explica Patton (2010), la SOCINT combina métodos de investigación etnográfica con análisis estratégico para identificar factores culturales que influyen en la toma de decisiones, la percepción de legitimidad y las dinámicas de insurgencia o cooperación. Aunque su aplicación operativa generó controversias éticas (especialmente por el riesgo de instrumentalizar el conocimiento antropológico con fines militares), la SOCINT consolidó la idea de que la cultura constituye una dimensión operativa de la seguridad, así como un componente esencial de la inteligencia contemporánea.

la superioridad tecnológica no garantizaba el control político si no se comprendían las lógicas culturales de resistencia, honor y religión. En consecuencia, la SOCINT se consolidó como un pilar de la HUMINT avanzada, capaz de transformar la recopilación de los datos en comprensión contextual.

Aunque a menudo se emplean indistintamente, CULINT¹⁰⁷ y SOCINT responden a enfoques analíticos distintos dentro de los estudios de inteligencia. La CULINT se centra en la comprensión de los códigos culturales y las normas de comportamiento que influyen en la comunicación, negociación e interacción entre individuos o grupos, siendo especialmente útil en las operaciones diplomáticas o en misiones de cooperación internacional (Earley & Ang, 2003). En cambio, la SOCINT amplía esa mirada hacia el análisis estructural de los sistemas sociales, políticos y religiosos que configuran los entornos humanos de conflicto; es decir, mientras la CULINT privilegia la competencia intercultural individual, la SOCINT examina la dinámica colectiva de las diversas comunidades y su relación con la legitimidad, el poder y la resistencia. En términos operativos, la primera busca mejorar la adaptación cultural de los agentes, mientras que la segunda proporciona inteligencia estratégica sobre factores sociopolíticos que condicionan la estabilidad o el cambio en un teatro de operaciones. En la actualidad, la relevancia de la SOCINT se extiende más allá del campo de batalla físico, aportando herramientas para interpretar las dinámicas de opinión, identidad y movilización que emergen en la infosfera.

En este contexto, la propuesta de Sharpe et al. (2024) lleva este razonamiento un paso más allá al plantear que la cultura debe ser reconocida formalmente como un sexto dominio de la guerra, junto a la tierra, mar, aire, espacio y ciberespacio. Su modelo C6ISR¹⁰⁸ amplía el paradigma tradicional C5ISR al incorporar la cultura

¹⁰⁷ CULINT (*Cultural Intelligence*) se define como la capacidad de adquirir y aplicar conocimiento sobre creencias, valores, comportamientos y contextos culturales para comprender, anticipar e influir en la conducta de personas o grupos en entornos interculturales. Según el U.S. Army Training and Doctrine Command (TRADOC, 2011), la CULINT busca mejorar la efectividad de las operaciones militares, diplomáticas y humanitarias mediante el desarrollo de sensibilidad cultural y adaptabilidad comunicativa. A diferencia de SOCINT, la CULINT se orienta principalmente a la interacción microcultural, enfatizando la empatía, competencia cultural y toma de decisiones situacional. Su aplicación contemporánea se extiende más allá del campo militar, influyendo también en el liderazgo internacional, la cooperación interinstitucional y la gestión de crisis en sociedades culturalmente diversas.

¹⁰⁸ Desde una perspectiva doctrinal, el modelo C6ISR (*Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Reconnaissance and Targeting*) constituye una ampliación conceptual del esquema C5ISR, al incorporar la cultura como dominio operativo y eje cognitivo del poder militar. Esta adición reconoce que toda estructura de mando, control e inteligencia se encuentra mediada por factores culturales que determinan cómo los actores perciben, interpretan y ejecutan la acción estratégica. En términos doctrinales, el C6ISR plantea que la cultura no solo condiciona la conducción del mando y la toma de decisiones, sino que puede emplearse como instrumento de superioridad cognitiva, orientado a influir en la voluntad, la cohesión y

como eje cognitivo que estructura la percepción, la decisión y la acción estratégica. Según Sharpe et al. (2024), la cultura no solo condiciona cómo los Estados comprenden la seguridad o la amenaza, sino también cómo organizan sus sistemas de mando, formulan sus doctrinas y procesan la información. Este enfoque coincide con la lógica de la SOCINT, pero la trasciende al elevar la cultura al rango de dominio operativo en sí mismo, es decir, un entorno donde se libran las batallas por el significado, la identidad y la legitimidad. En la era de la GC, la superioridad no depende exclusivamente de la tecnología ni de la información, sino de la capacidad de controlar los marcos culturales de interpretación que guían el comportamiento humano y colectivo. El modelo C6ISRT reconoce que los sistemas C2 modernos deben integrar la dimensión cultural como variable de mando, ya que las operaciones contemporáneas se desarrollan simultáneamente en el terreno físico, informacional y simbólico.

Desde esta perspectiva, la cultura actúa como un multiplicador cognitivo de poder, capaz de reforzar la cohesión interna, sostener la narrativa nacional y desarticular las narrativas adversarias. Comprender la cultura como dominio (no solo como variable contextual) permite anticipar los efectos psicológicos y sociales de las operaciones de información, fortalecer la resiliencia institucional y orientar las estrategias de influencia desde una comprensión profunda de los valores y símbolos que estructuran la conducta de los pueblos. En suma, el marco C6ISRT propone un salto doctrinal: pasar de la inteligencia cultural como apoyo contextual a la cultura como espacio de combate cognitivo, donde se decide la legitimidad y la voluntad de los actores estratégicos.

En síntesis, la integración de estos enfoques define el núcleo de la ciberinteligencia contemporánea. El espionaje ya no se limita a la intrusión en sistemas, sino que se extiende al modelado de entornos informativos y a la manipulación de percepciones. El conocimiento estratégico se convierte en un instrumento de ingeniería cognitiva que combina algoritmos, narrativas y cultura. En este escenario, la superioridad informacional depende de la capacidad para fusionar tres niveles de análisis: 1) el técnico, que revela cómo se estructura el ataque; 2) el conductual, que muestra por qué se ejecuta; y 3) el cognitivo, que explica cómo puede inducirse o desviarse la decisión del adversario.

la legitimidad del adversario. De este modo, la doctrina emergente asume que comprender y operar dentro de los marcos culturales constituye una capacidad tan decisiva como controlar los dominios físico, cibernético o informacional.

La ciberinteligencia, en su forma más avanzada, encarna el principio de la guerra reflexiva. Cada dato recolectado es a la vez un vector de información y una potencial arma cognitiva. La vigilancia global se transforma en un sistema de re-actualización estratégica, donde la observación, la interpretación y la influencia se confunden en un mismo proceso. Como concluye De Werd (2021), el desafío no es solo conocer al otro, sino reconocer cómo el acto de conocer lo transforma.

Hacia un Sistema de Alerta y Vigilancia del Ambiente Cognitivo (SAVAC)

En la era de la hiperconectividad, el conocimiento estratégico ya no puede limitarse tan solo a observar las acciones del adversario, sino que debe comprender los procesos mentales, culturales y emocionales que las originan. En este contexto surge la COGINT¹⁰⁹, una técnica de recolección de inteligencia emergente que se orienta a analizar los patrones cognitivos que determinan la interpretación del mundo y las decisiones dentro de él. A diferencia de formas tradicionales de inteligencia, centradas en los hechos observables, la COGINT busca mapear las estructuras de percepción, sesgos colectivos y narrativas dominantes que configuran el comportamiento de individuos, grupos y sociedades. De acuerdo con De Werd (2021), este tipo de inteligencia reflexiva asume que la información no solo describe la realidad, sino que la produce; conocer implica transformar lo conocido. La COGINT, en consecuencia, no se limita a recopilar datos sobre el pensamiento del otro, sino que estudia cómo ese pensamiento puede ser modelado, anticipando reacciones y diseñando respuestas cognitivas antes de que se manifiesten como acciones hostiles.

La COGINT constituye la evolución natural de las disciplinas clásicas de inteligencia hacia el dominio cognitivo. Mientras la inteligencia tradicional (HUMINT, SIGINT, OSINT o GEOINT) se centra en rastrear trazas externas de la acción humana, la COGINT busca mapear la arquitectura decisional de individuos y grupos mediante la integración de datos psicométricos, biométricos y conductuales. Como

¹⁰⁹ COGINT (*Cognitive Intelligence*) no pertenece aún a la clasificación doctrinal formal de las agencias de inteligencia (como HUMINT, SIGINT o OSINT), pero ha comenzado a consolidarse en el campo académico y militar para designar el estudio sistemático de los procesos mentales, emocionales y culturales que intervienen en la formación del juicio estratégico. Su raíz conceptual puede rastrearse en la filosofía de la información de Floridi (2015), quien plantea que los humanos son organismos informacionales (*inforgs*) insertos en ecosistemas de datos, y en la noción de inteligencia reflexiva propuesta por De Werd (2021), que analiza cómo el conocimiento altera los sistemas que lo generan. En el ámbito de la GC, Henschke (2024) extiende esta idea al dominio de la influencia, argumentando que la comprensión de la mente como entorno operacional requiere fusionar neurociencia, análisis cultural y ciberinteligencia.

señalan Conde y Whiskeyman (2025), la COGINT es el resultado de la convergencia entre la neurociencia, la inteligencia artificial y las ciencias del comportamiento, orientada a comprender cómo se configuran, manipulan y protegen los procesos mentales en entornos de conflicto no cinético. Su propósito no es solo describir la cognición, sino operacionalizarla, convirtiendo los patrones mentales en un campo de batalla donde se disputan la percepción, la voluntad y la interpretación (Tabla 15).

En este sentido, la COGINT no sustituye a las disciplinas anteriores, sino que las trasciende al incorporar las variables cognitivas que las sustentan. Si la GEOINT mapea el terreno físico, la COGINT mapea el terreno mental, convirtiendo la mente en un espacio operacional que puede ser explorado, defendido o explotado estratégicamente. La clave radica en que el conocimiento deja de ser un instrumento de observación y se convierte en un mecanismo de intervención sobre la conciencia.

Tabla 15. Evolución cronológica de los tipos de inteligencia en las guerras de quinta generación

Etapa	Técnica de recolección	Descripción y método	Ejemplo histórico o institucional	Tipo de inteligencia
Era digital (1990 -presente)	Intercepción satelital y vigilancia cibernética	Monitoreo masivo de flujos digitales, telecomunicaciones y tráfico de datos mediante sensores, satélites y programas de vigilancia electrónica.	Programas PRISM, XKeyscore, alianza Five Eyes.	SIGINT / CYBINT
	<i>Open source intelligence</i>	Recolección sistemática de información pública en medios digitales, redes sociales, bases de datos abiertas y documentos institucionales.	Creación del CIA Open Source Center (1990); EU Open Source Unit.	OSINT
	<i>Social media intelligence</i>	Análisis de interacciones, sentimientos, redes y narrativas en plataformas sociales mediante algoritmos de PLN y minería de datos.	Aplicaciones de SOCMINT en campañas antiterroristas y monitoreo electoral (Reino Unido, 2010).	SOCMINT
	Geointeligencia y <i>big data analytics</i>	Integración de imágenes satelitales, sensores ISR, georreferenciación y aprendizaje automático para el apoyo táctico y estratégico.	National Geospatial-Intelligence Agency (NGA); algoritmos ISR (2010-).	GEOINT / AI-INT
	Ciberinteligencia y ciberespionaje ofensivo	Recolección activa y defensiva en redes informáticas; identificación de amenazas APT, <i>malware</i> , vulnerabilidades y patrones de ataque.	Operación Stuxnet, SolarWinds, APT28/29.	CYBINT

Continúa tabla...

Etapa	Técnica de recolección	Descripción y método	Ejemplo histórico o institucional	Tipo de inteligencia
Era digital (1990 -presente)	<i>Sociocultural intelligence</i>	Análisis de factores culturales, sociales y simbólicos que condicionan la percepción y el comportamiento colectivo en entornos conflictivos.	Estudios socioculturales del US Army Human Terrain System; misiones en Irak y Afganistán (2006–2012).	SOCINT
	<i>Cultural intelligence</i>	Estudio sistemático de las dinámicas culturales, religiosas y lingüísticas que influyen en las operaciones militares, diplomáticas y de influencia.	Programas de Cultural Awareness y Cross-Cultural Competence del DoD (2000).	CULINT
	Neurointeligencia y minería cognitiva (incipiente)	Extracción de patrones cerebrales, emocionales y conductuales a partir de biometría, actividad digital y observación contextual.	Programas DARPA, Human Domain Analytics, NATO Human Data Project.	COGINT (<i>Cognitive Intelligence</i>)

Fuente: Elaboración propia

El desarrollo de la COGINT responde a la expansión del conflicto hacia el dominio mental. Como advierte Henschke (2024), las guerras contemporáneas no se definen por el control de territorios, sino por el control de significados. La mente humana (individual o colectiva), se convierte en el nuevo teatro de operaciones donde se disputan las narrativas de legitimidad, verdad y moralidad. Por ende, la COGINT constituye el fundamento técnico y epistemológico para construir sistemas de alerta temprana cognitiva, capaces de identificar alteraciones en flujos informativos y emocionales de una sociedad antes de que se traduzcan en crisis de seguridad o desestabilización política. Así, la inteligencia del siglo XXI no se mide por la cantidad de información acumulada, sino por la capacidad para reconocer los patrones semánticos que dirigen el comportamiento colectivo.

Sin embargo, la velocidad, el volumen y la opacidad de la información digital han superado la capacidad humana para procesarla. Brantly (2018) señala que la automatización del conocimiento, mediante técnicas avanzadas de aprendizaje automático, convierte toda información en inteligencia potencial, pero también en desinformación. Esta ambivalencia introduce, por lo tanto, un desafío crítico: ¿cómo distinguir, en un océano de señales, aquellas que configuran amenazas cognitivas emergentes? Es precisamente esta pregunta la que justifica el desarrollo del Sistema de Alerta y Vigilancia del Ambiente Cognitivo (SAVAC), una arquitectura original propuesta en este capítulo como mecanismo de anticipación, diagnóstico y respuesta frente a amenazas cognitivas emergentes.

El SAVAC parte de la premisa de que el dominio cognitivo constituye un ecosistema adaptativo donde interactúan individuos, tecnologías, medios y narrativas. Cada uno de estos elementos produce señales (a veces débiles o ruidosas), que pueden indicar la gestación de actividades de manipulación o desinformación. A diferencia de los sistemas tradicionales de inteligencia, centrados en la vigilancia de hechos físicos o digitales, el SAVAC se orienta al monitoreo del entorno semántico, identificando alteraciones en la coherencia discursiva, la propagación de sesgos o la sincronización anómala de emociones colectivas. Su objetivo no es solamente detectar la desinformación, sino comprender cómo ésta reorganiza los marcos cognitivos de una sociedad.

Los trabajos recientes de RAND confirman empíricamente tanto la urgencia como la viabilidad de este tipo de sistemas de alerta temprana. Mouton et al. (2025) muestran que las operaciones cognitivas de actores estatales hostiles a Occidente buscan precisamente explotar las vulnerabilidades estructurales del entorno informacional para minar la credibilidad, influencia y alianzas de Estados democráticos en el exterior, combinando propaganda clásica con tecnologías avanzadas y campañas coordinadas en el ciberespacio. Mouton et al. (2025) indican que la capacidad de monitorizar el ambiente informativo (mediante modelos capaces de detectar técnicas de propaganda y patrones anómalos en medios y plataformas digitales), se ha convertido en un requisito básico de seguridad nacional, y que herramientas de lenguaje avanzado, incluidos grandes modelos de lenguaje, pueden etiquetar de forma sistemática dispositivos propagandísticos y ofrecer indicadores tempranos de campañas hostiles. Esta evidencia respalda el supuesto central del SAVAC: sin un monitoreo estructurado del entorno semántico, las operaciones cognitivas adversarias permanecen invisibles hasta que sus efectos se consolidan en la opinión pública.

De manera complementaria, Marcellino et al. (2020) han propuesto un enfoque de *scalable analytics* para la detección de los esfuerzos subversivos en redes sociales que resulta directamente extrapolable al diseño del SAVAC¹¹⁰. Mediante el *community lexical analysis* (CLA), combinan análisis de redes y de texto para seg-

¹¹⁰ *Scalable analytics* se refiere a un conjunto de métodos analíticos capaces de procesar y segmentar volúmenes masivos de datos (generalmente demasiado grandes, heterogéneos y dinámicos para ser analizados por métodos convencionales) de manera eficiente y escalable. En el contexto de la desinformación, implica el uso combinado de análisis de redes, técnicas de procesamiento del lenguaje natural y modelos estadísticos que pueden adaptarse al crecimiento constante de los datos, permitiendo identificar los patrones narrativos, las anomalías semánticas y las comunidades discursivas ocultas sin pérdida de rendimiento, incluso cuando el corpus se multiplica exponencialmente. En términos operativos, es lo que permite pasar de "monitorear cuentas individuales" a detectar esfuerzos coordinados y estructuras narrativas a gran escala.

mentar enormes volúmenes de datos en comunidades discursivas manejables, donde es posible identificar señales débiles de campañas cognitivas coordinadas. El CLA integra la estructura relacional de las interacciones con patrones léxicos compartidos para detectar “comunidades discursivas”: grupos de usuarios que no necesariamente están coordinados entre sí, pero que convergen en el uso de determinados vocabularios, marcos narrativos y estructuras semánticas. Al centrarse en estas unidades discursivas (y no en cuentas individuales), el método permite rastrear la evolución de narrativas, identificar anomalías léxicas y detectar, en fases tempranas, la emergencia de patrones de desinformación o influencia, incluso en aquellos contextos donde la escala y heterogeneidad de los datos exceden la capacidad analítica humana.

Su estudio de caso sobre la Copa Mundial de la FIFA 2018 demuestra con especial claridad el potencial del método. En esa ocasión, Marcellino et al. (2020) lograron identificar la formación temprana de grupos discursivos que, aunque aparentemente vinculados a las conversaciones deportivas, comenzaron a incorporar de manera progresiva marcos narrativos políticos y antiinstitucionales. Al aplicar el CLA, los investigadores detectaron que ciertos usuarios (ubicados mayoritariamente en *clusters* francófonos), compartían vocabularios y estructuras argumentativas que no guardaban necesariamente relación directa con el evento deportivo, sino con narrativas de protesta y resentimiento social que luego alimentarían el movimiento de los *gilets jaunes*¹¹¹.

Las señales eran aún débiles y no existía ninguna evidencia visible en la esfera pública, pero el análisis léxico secuencial mostraba una convergencia creciente en torno a repertorios semánticos asociados a indignación fiscal, antipolítica y rechazo a las élites. Semanas después, estas mismas comunidades ampliaron su actividad, tradujeron los marcos discursivos en llamados a la movilización y terminaron ocupando un espacio central en la protesta que, meses más tarde, dominaría la agenda internacional. Este hallazgo es crucial, ya que el método permitió reconocer la gestación de una narrativa antes de que existiera la protesta misma, proporcionando una capacidad de detección en fase embrionaria, muy anterior al análisis

¹¹¹ El movimiento de los *gilets jaunes* (“chalecos amarillos”) surgió en Francia a finales de 2018 como una protesta inicialmente contra el alza del impuesto al combustible, pero rápidamente se transformó en un movimiento social más amplio marcado por la indignación fiscal, el rechazo a las élites políticas, la percepción de injusticia económica y la desconfianza hacia las instituciones estatales. Su carácter descentralizado, su coordinación a través de redes sociales y su rápida expansión territorial lo convirtieron en un caso emblemático de movilización impulsada por dinámicas digitales y acumulación de agravios colectivos, con fuerte resonancia simbólica en la política europea contemporánea.

forense posterior que suele caracterizar los esfuerzos tradicionales de inteligencia. El SAVAC recoge precisamente esta intuición: la importancia de no limitar el análisis a piezas aisladas de desinformación (una cuenta falsa, un video manipulado o un rumor viral), sino de identificar esfuerzos integrales de manipulación que se manifiestan a nivel de agregados narrativos y comunidades discursivas. En otras palabras, detectar no solo “qué” circula, sino “cómo” se articula colectivamente una narrativa antes de que se traduzca en acción política o social.

En una línea similar, Marcellino et al. (2021) abordan el problema específico de las teorías de conspiración en línea (uno de los vectores más corrosivos de la desinformación contemporánea), y proponen modelos híbridos que combinan el análisis semántico profundo (*embeddings* tipo BERT)¹¹² con el análisis de *stance*¹¹³ para capturar no solo de qué se habla, sino cómo se habla. El hallazgo principal de Marcellino et al. (2021) es que solo este enfoque híbrido permite distinguir de manera fiable entre contenidos que simplemente mencionan una conspiración y aquellos contenidos que la promueven activamente, al tiempo que ofrece explicabilidad sobre las funciones persuasivas del lenguaje¹¹⁴. Esta lógica se incorpora al SAVAC en la forma de modelos que no se limitan solo a clasificar tópicos, sino que analizan los estilos retóricos, los marcadores de certeza, las estructuras argumentativas y los patrones de polarización afectiva, permitiendo así evaluar la intensidad cognitiva y el potencial desestabilizador de una narrativa antes de que alcance masas críticas de difusión.

¹¹² BERT (*Bidirectional Encoder Representations from Transformers*) es un modelo de lenguaje profundo desarrollado por Google que aprende representaciones contextuales del texto analizando simultáneamente el significado de las palabras desde la izquierda y la derecha. Esto le permite capturar matices semánticos, inferencias implícitas y relaciones complejas entre conceptos, facilitando la detección de patrones discursivos sutiles en grandes volúmenes de datos.

¹¹³ *Stance analysis* (análisis de postura) es una técnica de procesamiento del lenguaje natural que identifica la actitud subyacente del emisor frente a un tópico: apoyo, rechazo, duda, ironía, sospecha, entre otros. A diferencia de la simple clasificación temática, el *stance* revela la orientación intencional del discurso y permite distinguir entre quien menciona una teoría conspirativa y quien la promueve activamente. La postura retórica alude a la forma en que un mensaje posiciona al emisor respecto de una narrativa, no solamente a través del contenido semántico, sino mediante marcadores discursivos como modalizadores (“probablemente”, “seguro”), niveles de certeza, estructuras argumentativas, juicios de valor o apelaciones emocionales. Analizarla permite evaluar la fuerza persuasiva del discurso y su capacidad de contribuir a dinámicas de radicalización o difusión conspirativa.

¹¹⁴ La explicabilidad en este contexto se refiere a la capacidad de los modelos de aprendizaje automático para mostrar qué elementos lingüísticos concretos (palabras clave, construcciones sintácticas, moduladores afectivos, marcos narrativos o patrones argumentativos), contribuyen a que un mensaje resulte persuasivo, conspirativo o manipulador. En lugar de operar como “cajas negras”, estos modelos permiten identificar por qué clasifican un texto como problemático, revelando los mecanismos narrativos, emocionales o retóricos que impulsan la influencia. Esto es crucial en COGINT, ya que facilita el análisis profesional, la auditoría del algoritmo y la comprensión humana de las rutas persuasivas explotadas en campañas de desinformación.

Desde el punto de vista estructural, el SAVAC se organizaría como un sistema de procesamiento continuo del ambiente cognitivo que operaría a través de tres funciones interdependientes. La primera es la fusión de COGINT, encargada de articular los datos provenientes de fuentes abiertas, redes sociales y sistemas de comunicación con análisis de sentimiento, variación léxica y evaluación de patrones narrativos. Tras incorporar las lógicas derivadas de métodos como el CLA, esta fase no se limita a “sumar” información, sino que buscaría reconstruir la textura semántica del entorno, revelando así tensiones discursivas, emergencias afectivas y señales débiles que anticipan perturbaciones cognitivas de origen coordinado.

La segunda función correspondería a la evaluación reflexiva, es decir, un proceso de interpretación estratégica que combinaría juicio humano experto con análisis predictivo y aprendizaje automático. Aquí se integran las aproximaciones híbridas descritas por Marcellino et al. (2021), que permiten distinguir entre menciones inocuas y alineamientos retóricos peligrosos, así como los modelos de detección temprana de campañas malignas propuestos por Mouton et al. (2025). De este modo, la evaluación reflexiva no se limitaría a detectar patrones recurrentes de manipulación, sino que identificaría su dinámica temporal, su potencial de amplificación y sus puntos de inflexión, proyectando cómo una narrativa incipiente podría transformarse en un vector de polarización o desestabilización social.

La tercera función es la respuesta adaptativa, que diseñaría intervenciones narrativas, comunicativas y culturales orientadas a restaurar la coherencia perceptiva en los espacios afectados. Su fundamento es la lógica del poder astuto, que reconoce que la defensa cognitiva no se ejerce únicamente resistiendo, sino interviniendo estratégicamente en la construcción del sentido, desbordando al adversario mediante iniciativas que preserven la autonomía interpretativa de la sociedad sin recurrir a coerción directa (Álvarez et al., 2018). La respuesta adaptativa implica, por tanto, una combinación equilibrada de comunicación institucional, contramedidas narrativas y acciones de resiliencia cognitiva cuyo propósito no es controlar la información, sino proteger la capacidad colectiva de interpretar críticamente los hechos.

La arquitectura subyacente del SAVAC encuentra un paralelismo conceptual en el modelo SWARM (*Scalable Warning and Resilience Model*) desarrollado por Lilly et al. (2021). En su formulación original, SWARM propone una infraestructura distribuida de advertencia para el ciberespacio basada en la detección de señales débiles y la correlación de patrones anómalos mediante aprendizaje automático. Adaptado al dominio cognitivo, este enfoque adquiere una dimensión metacognitiva, debido a que ya no se limita a identificar comportamientos anómalos en

redes, sino que rastrea cómo la información (al interactuar con emociones, identidades y narrativas), genera configuraciones emergentes que alteran la percepción social. Por consiguiente, la información deja de ser simplemente un dato estático para convertirse en un organismo vivo que reacciona, se amplifica, se distorsiona o se reorganiza según las dinámicas de la comunidad discursiva en la que circula. Aplicados al SAVAC, los principios del SWARM permiten diagnosticar cómo un flujo informativo inicialmente marginal puede llegar a evolucionar hacia una narrativa disruptiva o incluso convertirse en un catalizador de movilización política.

Para operar con eficacia en este entorno, el SAVAC requiere una arquitectura reticular basada en la tipología de redes distribuidas descrita por Kalkman y Wieskamp (2019). A diferencia de sistemas jerárquicos o centralizados, las redes distribuidas permiten que cada nodo (agencias estatales, universidades, centros de investigación, unidades de comunicación estratégica o ciudadanos expertos), actúe simultáneamente como sensor, analista y difusor de conocimiento. Este modelo reduce la vulnerabilidad de ataques de desinformación dirigidos a un solo punto, promueve la resiliencia informacional mediante la cooperación horizontal y evita la concentración excesiva de autoridad interpretativa, lo cual es fundamental para la legitimidad social del SAVAC. Más que una plataforma tecnológica, cabe señalar que el sistema se concibe como una comunidad epistémica articulada para la defensa cognitiva, donde convergen inteligencia estatal, investigación civil y participación ciudadana, cada una aportando capacidades distintas para comprender, monitorear y proteger el entorno cognitivo nacional (Tabla 16).

Tabla 16. *Arquitectura funcional del SAVAC*

Nivel	Tipo de señales observadas	Componentes analíticos principales	Tecnologías y modelos de soporte	Procesos de inteligencia / anticipación	Productos estratégicos
1. Nivel táctico: Observación cognitiva y detección embrionaria	Señales débiles, anomalías léxicas, cambios súbitos en sentimiento, activación semántica, patrones sospechosos en comunidades discursivas	SOCMINT ampliado; OSINT cognitivo; análisis de sentimiento; detección de propaganda temprana (Mouton et al., 2025); identificación de comunidades léxicas (Marcellino et al., 2020)	Procesamiento del lenguaje natural (PLN); <i>community lexical analysis</i> (CLA); detección de bots y deepfakes; análisis de grafos; métricas de coordinación anómala	Monitoreo continuo de flujos informativos; segmentación de comunidades; identificación de patrones de amplificación inusual; clasificación de señales débiles antes de su viralización	Alertas cognitivas embrionarias; mapas dinámicos de comunidades discursivas; señales de advertencia temprana basadas en desviaciones semánticas

Continúa tabla...

Nivel	Tipo de señales observadas	Componentes analíticos principales	Tecnologías y modelos de soporte	Procesos de inteligencia / anticipación	Productos estratégicos
2. Nivel operacional: Fusión cognitiva e interpretación reflexiva	Patrones narrativos, sesgos explotables, estilos retóricos, intensidad cognitiva, postura discursiva	COGINT; CYBINT contextual; análisis semántico profundo; análisis de <i>stance</i> ; detección de teorías conspirativas (Marcellino et al., 2021)	Modelos híbridos BERT + análisis de postura retórica; IA explicable (XAI); modelamiento de comportamiento; correlación multimodal	Fusión de inteligencia humana y algorítmica; evaluación reflexiva de campañas; identificación de rutas persuasivas; clasificación de esfuerzos coordinados; evaluación del potencial desestabilizador	Diagnósticos de vulnerabilidad cognitiva; matrices de riesgo narrativo; perfiles de intensidad cognitiva; informes profundos de incidencia
3. Nivel estratégico: Evaluación anticipatoria y simulación cognitiva	Dinámicas de polarización, contagio informacional, marcos identitarios, desplazamientos emotivos	SOCINT; análisis cultural profundo; análisis geopolítico; comprensión narrativa contextual	Simuladores cognitivos (DARPA, AFRL); sistemas expertos de apoyo a la decisión; modelos de propagación narrativa; análisis longitudinal	Simulación de escenarios cognitivos; proyección de narrativas; identificación de puntos de inflexión; evaluación del impacto nacional de campañas hostiles	Estrategias de resiliencia cognitiva; contramedidas narrativas contextualizadas; narrativas preventivas; recomendaciones estratégicas para toma de decisiones
4. Nivel sistémico: Coordinación nacional y respuesta integral	Cambios macrodiscursivos, sincronización de actores, tendencias estructurales del ecosistema informacional	SAVAC como red distribuida; integración multinivel; diplomacia informacional; poder astuto	Arquitecturas distribuidas SWARM ² ; nube segura; sistemas de gestión del conocimiento; plataformas de coordinación interinstitucional	Coordinación civil-militar-académica; implementación de contramedidas reflexivas; diseño de campañas de resiliencia social; contranarrativas estratégicas	Sistema nacional de alerta cognitiva; fortalecimiento de soberanía informacional; estabilidad perceptiva del ecosistema mediático; informes interinstitucionales de gran estrategia cognitiva

Fuente: Elaboración propia

La arquitectura presentada en la Tabla 16 permite comprender cómo el SAVAC opera como un sistema de vigilancia cognitiva distribuido que traduce señales dispersas del entorno informacional en inteligencia accionable para la toma de decisiones estratégicas. Cada uno de sus niveles cumple una función diferenciada (pero integrada), dentro del ciclo cognitivo de la anticipación, el análisis y la respuesta, asegurando que el sistema pueda transitar desde la observación microdiscursiva hasta la formulación de las políticas nacionales de defensa cognitiva.

En el nivel táctico, el SAVAC actúa sobre la superficie visible del ecosistema digital, ya que monitorea en tiempo real redes sociales, plataformas de mensajería,

foros y espacios de interacción pública, utilizando herramientas avanzadas de PLN, análisis de sentimiento, detección de anomalías y filtros algorítmicos capaces de identificar patrones incipientes de manipulación¹¹⁵. Este nivel no opera sobre hipótesis preconcebidas, sino sobre aquellos indicios basados en fluctuaciones léxicas, coordinación sospechosa entre actores, picos emocionales o aparición de vocabularios anómalos que, como muestran Marcellino et al. (2020), frecuentemente anticipan la consolidación de comunidades discursivas que luego se activan políticamente. Por consiguiente, el objetivo central del nivel táctico es capturar las señales débiles antes de que se diluyan en el ruido informacional.

Por su parte, el nivel operacional constituye el núcleo analítico del sistema. Aquí, las señales captadas en el nivel táctico se someten a procesos de fusión cognitiva que integran SOCMINT, COGINT, CYBINT contextual y modelos de aprendizaje automático explicable. Es en esta capa en donde se aplican metodologías como el CLA o los modelos híbridos de análisis semántico y postura retórica propuestos por Marcellino et al. (2021), para distinguir entre las conversaciones ordinarias, las narrativas emergentes y las operaciones coordinadas de manipulación. El nivel operacional no solo identifica qué narrativas están creciendo, sino cómo y por qué lo hacen, evaluando su intensidad cognitiva, su capacidad de contagio y los sesgos que podrían amplificarlas dentro de grupos específicos. Su función es convertir datos dispersos en diagnósticos de vulnerabilidad cognitiva.

Ahora bien, el nivel estratégico constituye el espacio donde el SAVAC adquiere su dimensión prospectiva. Basado en los modelos de simulación cognitiva, análisis sociocultural y evaluaciones geopolíticas, este nivel proyecta la posible evolución de narrativas disruptivas y estima su impacto sobre la estabilidad política, militar o social. En otras palabras, en lugar de limitarse a describir fenómenos, el

¹¹⁵ Las herramientas avanzadas de procesamiento del lenguaje natural (PLN), análisis de sentimiento, detección de anomalías y filtros algorítmicos constituyen el conjunto básico de tecnologías para la vigilancia del entorno informativo. El PLN es un conjunto de métodos computacionales que permiten a los sistemas interpretar, transformar y analizar lenguaje humano en grandes volúmenes de texto; incluye tokenización, análisis sintáctico, extracción de entidades, modelado temático y *embeddings* semánticos. Los análisis de sentimiento son técnicas que clasifican la valencia emocional de un mensaje (positiva, negativa, neutra) e identifican marcadores afectivos como indignación, miedo, euforia o resentimiento, útiles para anticipar activaciones colectivas. La detección de anomalías son algoritmos que identifican patrones inusuales en el comportamiento de redes o narrativas, como picos súbitos de actividad, sincronización sospechosa entre cuentas, aparición de vocablos atípicos o cambios bruscos en la estructura semántica. Los filtros algorítmicos de manipulación incipiente son modelos entrenados para detectar señales tempranas de operaciones coordinadas, tales como repetición inorgánica de mensajes, uso sistemático de *hashtags*, redistribución masiva en ventanas temporales reducidas o similitud léxica entre actores no conectados entre sí. Estas herramientas permiten al SAVAC observar el entorno cognitivo con granularidad temporal y semántica, identificando perturbaciones mínimas que pueden escalar hacia operaciones de desinformación organizadas.

nivel estratégico genera escenarios posibles, identifica puntos de inflexión y permite valorar qué tipo de contramedidas (narrativas, institucionales o comunicacionales), son necesarias para evitar que una señal débil se transforme en una crisis informacional. Es aquí donde el SAVAC se convierte en un instrumento de conciencia situacional cognitiva que opera bajo la lógica de la anticipación y no de la reacción.

Finalmente, el nivel sistémico constituye la capa de integración nacional del SAVAC. En este nivel se articula la red distribuida de actores estatales, centros de investigación, empresas tecnológicas, medios de comunicación y organizaciones civiles que actúan como nodos del sistema. Inspirado en la lógica de redes distribuidas descrita por Kalkman y Wieskamp (2019), este nivel garantiza que la defensa cognitiva no sea la responsabilidad exclusiva de una sola entidad, sino el resultado de un ecosistema cooperativo de vigilancia y resiliencia. Es también en esta capa donde se formula la respuesta adaptativa, compuesta por contranarrativas, campañas preventivas, acciones reflexivas y protocolos de coordinación interinstitucional que buscan restablecer la coherencia perceptiva en los sectores afectados.

El SAVAC propone, además, un modelo de cooperación civil-militar-cognitiva, en el cual la defensa nacional se concibe como una tarea colectiva. Las universidades, los medios de comunicación, las empresas tecnológicas y las organizaciones sociales participan como sensores distribuidos del sistema, aportando datos y análisis desde sus propios ámbitos. Siguiendo la advertencia de Zegart (2022), en la que las líneas entre inteligencia estatal y privada se desdibujan, esta red colaborativa garantiza que la detección de amenazas cognitivas no dependa de una sola institución, sino de la sinergia entre múltiples actores. El sistema, en este sentido, no busca controlar la información, sino proteger la integridad del ecosistema informacional. Es decir, el SAVAC no es un mecanismo de censura ni de control político, sino un instrumento epistemológico y estratégico para preservar la integridad del ecosistema informativo en sociedades democráticas. Su eficacia depende, por lo tanto, de su legitimidad basada en transparencia, proporcionalidad y respeto por los derechos informativos de los ciudadanos, que, como advierte Owen (2017), son condiciones necesarias para que un sistema de esta naturaleza no derive en prácticas abusivas.

Por consiguiente, la verdadera fortaleza del SAVAC se manifiesta en su capacidad para convertir información en defensa anticipatoria. Al detectar señales débiles (como la expansión temprana de una narrativa de odio, la aparición de comunidades discursivas coordinadas o la intensificación de marcadores retóricos

conspirativos), el sistema permite actuar antes de que se generen daños irreversibles sobre la cohesión social, la confianza institucional o la estabilidad política. En términos funcionales, el SAVAC opera como un sistema inmune cognitivo: reconoce patrones perturbadores, los interpreta y activa respuestas para contenerlos o neutralizarlos.

En última instancia, la evolución del SAVAC apunta hacia la convergencia entre la COGINT y la inteligencia artificial estratégica. La automatización del análisis semántico, la detección de patrones de influencia y la modelación de escenarios cognitivos permitirán desarrollar sistemas autónomos capaces de ofrecer alertas explicables en tiempo real. Sin embargo, tal como observa De Werd (2021), delegar el juicio exclusivamente a algoritmos implica un dilema epistemológico: cuanto mayor sea la automatización, más necesario se vuelve diseñar mecanismos que garanticen la interpretabilidad y supervisión humana. El desafío del futuro será concebir un sistema de defensa cognitiva donde la IA amplíe (pero no reemplace) el discernimiento estratégico.

En síntesis, el SAVAC representa la contribución central de este capítulo y una propuesta pionera en el campo de la inteligencia cognitiva. Su arquitectura combina tradición analítica, teoría contemporánea del conflicto informacional y herramientas avanzadas de procesamiento del lenguaje para anticipar, interpretar y responder a amenazas cognitivas emergentes. En un entorno donde la información puede erosionar instituciones, polarizar sociedades o desencadenar crisis políticas, la defensa nacional comienza por la mente. Es precisamente allí donde el SAVAC ofrece su mayor valor: transformar el conocimiento en alerta, y la alerta en estabilidad.

Conclusiones

La historia de la inteligencia es, en última instancia, la historia de cómo las sociedades han aprendido a pensar estratégicamente frente a la incertidumbre. Desde los mensajeros del mundo antiguo hasta las redes neuronales del siglo XXI, su evolución refleja la aspiración humana de comprender el entorno antes de actuar sobre él. Pero, como recuerda Gentry (2019), el valor de la inteligencia no puede medirse únicamente por su contribución visible a las victorias militares. Su verdadera importancia radica en su capacidad para reducir la fricción cognitiva del entorno estratégico y para generar marcos interpretativos que orientan la acción. La

inteligencia no es solo un instrumento del poder, también se constituye como una forma de conocimiento que define qué se percibe como amenaza, oportunidad o realidad.

A lo largo del tiempo, la inteligencia ha transitado desde la observación empírica hasta la manipulación informacional, desde el registro de los hechos hasta la ingeniería del sentido. Cada etapa de su desarrollo ha incorporado nuevas formas de mediación entre el saber y el hacer, revelando que su función esencial no es acumular datos, sino darles coherencia. En la era cognitiva, este proceso se ha acelerado: la información ya no solo describe el mundo, sino que lo produce activamente a través de la interpretación, el discurso y la decisión. El conocimiento estratégico se convierte así en un poder performativo, capaz de modelar realidades antes incluso de que estas se materialicen.

Sin embargo, este poder epistémico conlleva un riesgo. Tal como advierten Spoor y De Werd (2023), los sistemas de inteligencia actuales operan dentro de entornos no lineales y adaptativos, donde las causas y los efectos ya no pueden predecirse con precisión. En estos escenarios de alta complejidad, modelos tradicionales (por ejemplo, aquellos basados en el ciclo lineal de recolección, análisis, difusión y retroalimentación) resultan insuficientes. En consecuencia, la inteligencia contemporánea requiere, más que procedimientos, procesos de *sensemaking*¹¹⁶: estructuras dinámicas que integren lo técnico, lo humano y lo cognitivo en un continuo de aprendizaje.

La propuesta de Spoor y De Werd (2023) de concebir la inteligencia como un sistema complejo adaptativo ofrece un marco útil para repensar su epistemología. En este paradigma, el analista ya no es un observador externo, sino un agente inmerso en la red de significados que analiza. Su tarea no consiste en eliminar la incertidumbre, sino en aprender a navegarla mediante la interacción entre datos, contextos y juicios; esto implica reconocer que la inteligencia no solo interpreta el entorno, sino que también lo transforma a través de la propia interpretación. De ahí que deba pasar de un modelo predictivo a uno reflexivo, en el cual la capacidad de adaptación sea más valiosa que la certeza.

Desde esta perspectiva, la inteligencia se convierte en un laboratorio epistemológico del siglo XXI, un espacio donde confluyen información, cognición y estrategia. Gentry (2019) insiste en que los efectos de la inteligencia rara vez pueden

¹¹⁶ *Sensemaking* (Weick, 1995) se refiere al proceso mediante el cual los individuos y organizaciones construyen significado frente a la ambigüedad. En el contexto de la inteligencia, describe la capacidad de convertir datos fragmentarios en una comprensión compartida que guía la acción estratégica.

aislarse de otras variables operacionales; empero, su influencia se manifiesta en la manera en que reconfigura el campo de decisión. Las guerras no se ganan únicamente con la inteligencia, pero ninguna victoria sostenible es posible sin ella. En su dimensión más profunda, la inteligencia actúa como una forma de mediación entre el conocimiento disponible y el conocimiento necesario, y entre la complejidad del mundo y la coherencia que exige la acción.

El análisis histórico hecho en este capítulo permite comprender que la evolución de la inteligencia ha sido también una evolución del pensamiento estratégico. En la modernidad, la inteligencia contribuyó a racionalizar la guerra; en la posmodernidad, a simbolizarla; y en la actualidad, a hibridarla con los dominios digital y cognitivo. Por consiguiente, la CYBINT, SOCMINT, SOCINT y COGINT expresan esa transformación, caracterizada por la fusión entre técnica y mente, entre tecnología y narrativa, entre información y emoción. En otras palabras, el campo de la inteligencia ha dejado de ser simplemente un aparato de observación para convertirse en un ecosistema de la interpretación, en donde la frontera entre analizar y participar se disuelve.

En este nuevo escenario, la pregunta ya no es cuánta información se posee, sino qué tipo de sentido se construye con ella. La saturación de datos y la automatización del análisis mediante algoritmos introducen una paradoja: cuanto más sabemos, menos comprendemos. De ahí la urgencia de lo que Spoor y De Werd (2023) denominan una *inteligencia reflexiva*¹¹⁷, capaz de cuestionar sus propios marcos cognitivos y adaptarse a los entornos en constante cambio. El conocimiento ya no puede entenderse como una estructura jerárquica, sino como una red que aprende.

Con base en lo anterior, el futuro de la inteligencia dependerá de su capacidad para integrar tres principios rectores. El primero es la complejidad, entendida no como desorden, sino como un patrón emergente de interdependencias; es decir, la inteligencia debe aprender a leer mejor la incertidumbre como un lenguaje operativo. El segundo es la reflexividad, que implica reconocer la influencia del observador en la realidad observada y la necesidad de un pensamiento crítico sobre las propias herramientas analíticas. El tercero es la adaptabilidad, que sustituye la

¹¹⁷ Inteligencia reflexiva designa la capacidad de un sistema de inteligencia para evaluar y ajustar sus propios supuestos, métodos y sesgos cognitivos. Esta idea deriva de la noción de "reflexividad epistémica" en sistemas complejos y ha sido desarrollada por Spoor y De Werd (2023) como requisito para el aprendizaje institucional continuo.

obsesión por la predicción por una cultura orientada al aprendizaje continuo y la resiliencia cognitiva.

Estas transformaciones tienen implicaciones doctrinales profundas. El modelo clásico de ciclo de inteligencia (formulado para entornos lineales), debe evolucionar hacia un modelo orgánico, en el que la recolección, análisis y diseminación coexistan en retroalimentación permanente. La inteligencia militar del futuro deberá funcionar más como un ecosistema de nodos interconectados que como una jerarquía de funciones. En ese sentido, las doctrinas del *sensemaking* y de la inteligencia en red ofrecen caminos prometedores para superar las limitaciones estructurales de la burocracia informacional.

En esta misma línea, desarrollos recientes en teoría de inteligencia refuerzan la necesidad de abandonar definitivamente los modelos secuenciales tradicionales. Hershkovitz (2025) demuestra que el ciclo de inteligencia, concebido como un proceso lineal de fases claramente diferenciadas, resulta insuficiente para operar en entornos caracterizados por la sobreabundancia de datos, la interconectividad y la simultaneidad de funciones. En su lugar, propone modelos dinámicos y multidisciplinarios en los que la recolección, el análisis y la acción ocurren de manera concurrente dentro de redes adaptativas. Desde esta perspectiva, la inteligencia deja de ser un flujo ordenado de información para convertirse en un proceso emergente de construcción de sentido, donde múltiples actores (humanos y algorítmicos) interactúan en tiempo real. Esta transformación no solo implica un ajuste metodológico, sino una ruptura epistemológica: la inteligencia ya no puede entenderse como un ciclo, sino como un sistema complejo de producción de conocimiento en red.

En consecuencia, así como la guerra contemporánea ha dejado de ser un fenómeno estrictamente físico para devenir en una confrontación cognitiva y algorítmica, la inteligencia también ha dejado de ser un proceso lineal para convertirse en una arquitectura adaptativa de interpretación. Comprender esta doble transformación (del conflicto y del conocimiento) es esencial para evitar que los modelos analíticos del pasado se conviertan en vulnerabilidades estratégicas en el presente.

Gentry (2019) también recuerda que el conocimiento estratégico es una forma de poder que puede fracasar si se divorcia del juicio. La abundancia de datos no garantiza decisiones acertadas; lo que las garantiza es la capacidad de interpretar la información dentro de un contexto humano y moral, y esta es quizás la paradoja fundamental de la era digital: la inteligencia se automatiza, pero el juicio sigue siendo irremplazablemente humano; en este punto, la inteligencia deja de ser un mero

proceso técnico y se convierte en un acto ético, en la medida en que decide qué verdades vale la pena creer y qué riesgos justifican la acción.

En síntesis, la inteligencia del siglo XXI se redefine como un sistema adaptativo de conocimiento estratégico. Su esencia ya no está en la acumulación de secretos, sino en la orquestación de significados. Comprender las guerras, el poder y las sociedades en clave informacional exige aceptar que la verdad es un territorio disputado y que el control de las percepciones es el nuevo campo de batalla. Frente a esta realidad, el desafío no es producir más inteligencia, sino producirla mejor; es decir, una inteligencia que piense sobre sí misma, que aprenda de sus errores, que reconozca la complejidad del mundo y que preserve, incluso en la era algorítmica, la lucidez del juicio humano.

Referencias

- Álvarez, C. (2023). El fracaso de la integración político-militar durante la guerra de Vietnam: ¿dos tipos de liderazgo divergentes? En S. Uribe-Cáceres & D. López-Niño (Eds.), *Aproximación teórica a las nociones de la guerra y el liderazgo estratégico* (pp. 105-125). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602526.05>
- Álvarez, C., Barón, P., & Monroy, V. (2018). Poder astuto: Estrategia del empleo del poder en el siglo XXI. En C. Álvarez & A. Fernández (Eds.), *Hacia una gran estrategia en Colombia: Construcción de política pública en seguridad y defensa* (pp. 171-268). Sello Editorial ESMIC. <https://doi.org/10.21830/9789585692862>
- Álvarez, C., Santafé, J., & Urbano, O. (2017). *Metamorphosis Bellum: ¿mutando a guerras de quinta generación?* En C. Álvarez (Ed.), *Escenarios y desafíos de la seguridad multidimensional en Colombia* (pp. 145-247). Sello Editorial ESDEG. <https://doi.org/10.25062/9789585652835>
- Andrew, C. (2010). *The defence of the realm: The authorized history of MI5*. Vintage.
- Andrew, C. (2018). *The secret world: A history of intelligence*. Yale University Press.
- Andrew, C., & Mitrokhin, V. (1999). *The sword and the shield: The Mitrokhin archive and the secret history of the KGB*. Basic Books.
- Bertelsen, O. (2021a). Introduction: A blind spot of active measures. En O. Bertelsen (Ed.), *Russian active measures: Yesterday, today, tomorrow* (pp. 15-36). ibidem-Verlag.
- Bertelsen, O. (2021b). The KGB operation "Retribution" and John Demjanjuk. En O. Bertelsen (Ed.), *Russian active measures: Yesterday, today, tomorrow* (pp. 93-136). ibidem-Verlag.
- Black, I., & Morris, B. (1991). *Israel's secret wars: A history of Israel's intelligence services*. Grove Weidenfeld.

- Block, L. (2023). The long history of OSINT. *Journal of Intelligence History*, 23(2), 95-109. <https://doi.org/10.1080/16161262.2023.2224091>
- Boyd, J. (1987). *A discourse on winning and losing*. Air University Press.
- Brantly, A. (2018). When everything becomes intelligence: Machine learning and the connected world. *Intelligence and National Security*, 33(4), 562-573. <https://doi.org/10.1080/02684527.2018.1452555>
- Buluc, R., Arcos, R., & Ivan, C. (2024). When spies go public! Lessons learnt from the instrumentalization of intelligence for strategic communication in the run-up to the Russian-Ukrainian war. *Intelligence and National Security*, 40(1), 42-57.
- Chickering, R. (2006). World War I and the theory of total war: Reflections on the British and German cases, 1914-1915. En R. Chickering & S. Förster (Eds.), *Great War, total war: Combat and mobilization on the Western Front, 1914-1918* (pp. 35-56). Cambridge University Press.
- Clark, R., & Mitchell, W. (2019). *Deception: Counterdeception and counterintelligence*. Sage.
- Clausewitz, C. von. (1984). *On war*. Princeton University Press.
- Conde, J., & Whiskeyman, A. (2025). The emergence of cognitive intelligence (COGINT) as a new military intelligence collection discipline. *International Journal of Intelligence and CounterIntelligence*, 1-27. <https://doi.org/10.1080/08850607.2025.2571497>
- Dahl, R. (1957). The concept of power. *Behavioral Science*, 2(3), 201-215. <https://doi.org/10.1002/bs.3830020303>
- Dearlove, R. (2010). National security and public anxiety: Our changing perceptions. En L. Johnson (Ed.), *The Oxford handbook of national security intelligence* (pp. 33-42). Oxford University Press.
- De Werd, P. (2021). Reflexive intelligence and converging knowledge regimes. *Intelligence and National Security*, 36(4), 512-526.
- Dover, R. (2019). SOCMINT: A shifting balance of opportunity. *Intelligence and National Security*, 35(2), 216-232. <https://doi.org/10.1080/02684527.2019.1694132>
- Duyvesteyn, I. (2013). *Intelligence and strategic culture*. Routledge.
- Dylan, H., Gioe, D., & Goodman, M. (2020). *The CIA and the pursuit of security: History, documents and contexts*. Edinburgh University Press.
- Earley, P., & Ang, S. (2003). *Cultural intelligence: Individual interactions across cultures*. Stanford University Press.
- Flamer, N. (2023). The enemy teaches us how to operate: Palestinian Hamas use of open-source intelligence (OSINT) in its intelligence warfare against Israel (1987-2012). *Intelligence and National Security*, 38(7), 1171-1188. <https://doi.org/10.1080/02684527.2023.2212556>
- Floridi, L. (2010). *Information: A very short introduction*. Oxford University Press.
- Floridi, L. (2011). *The philosophy of information*. Oxford University Press.

- Floridi, L. (2015). Hyperhistory and the philosophy of information policies. En L. Floridi (Ed.), *The Onlife manifesto: Being human in a hyperconnected era* (pp. 51-64). Springer.
- Foucault, M. (1995). *Discipline and punish: The birth of the prison*. Vintage Books.
- Gentry, J. (2019). Intelligence in war: How important is it? How do we know? *Intelligence and National Security*, 34(6), 833-850. <https://doi.org/10.1080/02684527.2019.1611205>
- Gentry, J. (2022). Cyber intelligence: Strategic warning is possible. *International Journal of Intelligence and CounterIntelligence*, 36(3), 729-754.
- Gill, P. (2010). Theories of intelligence. En L. Johnson (Ed.), *The Oxford handbook of national security intelligence* (pp. 43-58). Oxford University Press.
- Gill, P., & Phythian, M. (2013). From intelligence cycle to web of intelligence: Complexity and the conceptualisation of intelligence. En M. Phythian (Ed.), *Understanding the intelligence cycle* (pp. 35-54). Routledge.
- Gioe, D. V., Lovering, R., & Pachesny, T. (2020). The Soviet legacy of Russian active measures: New vodka from old stills? *International Journal of Intelligence and CounterIntelligence*, 33(3), 514-539. <https://doi.org/10.1080/08850607.2020.1725364>
- Graham, T., & Hansen, K. (2007). *Spy satellites and other intelligence technologies that changed history*. University of Washington Press.
- Hammes, T. (2006). *The sling and the stone: On war in the 21st century*. Zenith Press.
- Harris, R. (2021). *OSS: The secret history of America's first Central Intelligence Agency*. Tantor and Blackstone Publishing.
- Haslam, J. (2015). *Near and distant neighbours: A new history of Soviet intelligence*. Oxford University Press.
- Hershkovitz, S. (2025). Developing intelligence models for the digital era. *Intelligence and National Security*, 40(6), 1037-1058. <https://doi.org/10.1080/02684527.2025.2565952>
- Henschke, A. (2025). *Cognitive warfare: Grey matters in contemporary political conflict*. Routledge.
- Herman, M. (1996). *Intelligence power in peace and war*. Cambridge University Press.
- Heuer, R. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence.
- Hosaka, S. (2020). Repeating history: Soviet offensive counterintelligence active measures. *International Journal of Intelligence and CounterIntelligence*, 35(3), 429-458. <https://doi.org/10.1080/08850607.2020.1822100>
- Hughes, J. (2017). *The secret state: A history of intelligence and espionage*. W. W. Norton & Co.
- Hulnick, A. (2006). What's wrong with the intelligence cycle. *Intelligence and National Security*, 21(6), 959-979. <https://doi.org/10.1080/02684520601046291>
- Hulnick, A. (2013). Intelligence theory: Seeking better models. En M. Phythian (Ed.), *Understanding the intelligence cycle* (pp. 150-159). Routledge.
- Jeffery, K. (2010). *MI6: The History of the Secret Intelligence Service 1909–1949*. Bloomsbury Publishing.

- Johnson, L. (2010). National security intelligence. En L. Johnson (Ed.), *The Oxford handbook of national security intelligence* (pp. 3-32). Oxford University Press.
- Kahn, D. (1996). *The codebreakers: The comprehensive history of secret communication from ancient times to the Internet*. Scribner.
- Kalkman, J., & Wieskamp, L. (2019). Cyber intelligence networks: A typology. *The International Journal of Intelligence, Security, and Public Affairs*, 21(1), 4-24. <https://doi.org/10.1080/23800992.2019.1598092>
- Keegan, J. (2003). *Intelligence in war: Knowledge of the enemy from Napoleon to Al-Qaeda*. Knopf.
- Kent, S. (1965). *Strategic intelligence for American world policy*. Archon Books.
- Koschade, S. (2006). A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence. *Studies in Conflict & Terrorism*, 29(6), 559-575. <https://doi.org/10.1080/10576100600798418>
- Kuzmiakova, A. (2025). *Automating cyber threat intelligence: Tools and techniques for enhanced security posture*. Arcler Press.
- Lefebvre, V. (1977). *The structure of awareness: Toward a symbolic logic of human behavior*. Sage Publications.
- Ley Estatutaria 1621. (2013). *Por medio de la cual se dictan normas sobre inteligencia y contrainteligencia y se expiden otras disposiciones*. Congreso de la República de Colombia. <https://tinyurl.com/26ljog8l>
- Lilly, B., Moore, A., Hodgson, Q., & Weishoff, D. (2021). *RAND's scalable warning and resilience model (SWARM): Enhancing defenders' predictive power in cyberspace*. RAND Corporation.
- Lockheed Martin Computer Incident Response Team. (2011). *Intelligence-driven computer network defense: Informed by analysis of adversary campaigns and intrusion kill chains*. Lockheed Martin Corporation.
- Lowenthal, M. (2022). *Intelligence: From secrets to policy* (9.^a ed.). CQ Press.
- Luhmann, N. (2013). *Introduction to systems theory*. Polity Press.
- MacGaffin, J., & Oleson, P. (2015). Decision advantage, decision confidence: The why of intelligence. *Intelligencer Journal*, 21(3), 41-46.
- Magee, A. (2023). Counterintelligence black swan: KGB deception, countersurveillance, and active measures operation. *International Journal of Intelligence and CounterIntelligence*, 37(1), 232-264. <https://doi.org/10.1080/08850607.2023.2192374>
- Mandrick, B., & Smith, B. (2022). Philosophical foundations of intelligence collection and analysis: A defense of ontological realism. *Intelligence and National Security*, 37(6), 809-819. <https://philarchive.org/rec/SMIPFO-4>
- Marcellino, W., Marcinek, K., Pezard, S., & Matthews, M. (2020). *Detecting malign or subversive information efforts over social media: Scalable analytics for early warning*. RAND Corporation.

- Marcellino, W., Helmus, T., Kerrigan, J., Reininger, H., Karimov, R., & Lawrence, R. (2021). *Detecting conspiracy theories on social media: Improving machine learning to detect and understand online conspiracy theories*. RAND Corporation.
- Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and CounterIntelligence*, 27(4), 702-719. <https://doi.org/10.1080/08850607.2014.924811>
- Matthews, P. (2013). *SIGINT: The secret history of signals intelligence in the World Wars 1914-1945*. The History Press.
- McDowell, D. (2009). *Strategic intelligence: A handbook for practitioners, managers and users*. Scarecrow Press.
- Merriam, J. (2023). One move ahead: Diagnosing and countering Russian reflexive control. *The Journal of Slavic Military Studies*, 36(1), 1-27. <https://doi.org/10.1080/13518046.2023.2201113>
- Miller, S. (2022). National security intelligence activity: A philosophical analysis. *Intelligence and National Security*, 37(6), 791-808. <https://doi.org/10.1080/02684527.2022.2076329>
- Mouton, C., Lucas, C., & Ee, S. (2025). *Defending American interests abroad: Early detection of foreign malign information operations*. RAND Corporation.
- Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, 27(6), 801-823. <https://doi.org/10.1080/02684527.2012.716965>
- Owen, S. (2017). Monitoring social media and protest movements: Ensuring political order through surveillance and surveillance discourse. *Social Identities*, 23(6), 688-700. <https://doi.org/10.1080/13504630.2017.1291092>
- Phythian, M. (2013). Introduction: Beyond the intelligence cycle? En M. Phythian (Ed.), *Understanding the intelligence cycle* (pp. 17-23). Routledge.
- Pili, G. (2020). *Why do we really need philosophy in intelligence studies? Let's give philosophy a chance with the next stage of the philosophy of intelligence* [Manuscrito no publicado].
- Price, D. (2015). A guide to cyber intelligence. *Journal of U.S. Intelligence Studies*, 21(1), 55-60.
- Quist, T. (2022). What philosophy can do for intelligence. *Intelligence and National Security*, 37(6), 777-790. <https://doi.org/10.1080/02684527.2022.2076328>
- Rønn, K. (2022). The multifaceted norm of objectivity in intelligence practices. *Intelligence and National Security*, 37(6), 820-834. <https://doi.org/10.1080/02684527.2022.2076331>
- Richards, J. (2013). Pedalling hard: Further questions about the intelligence cycle in the contemporary era. En M. Phythian (Ed.), *Understanding the intelligence cycle* (pp. 55-66). Routledge.
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
- Risso, L. (2015). *Propaganda and intelligence in the Cold War: The NATO information service*. Routledge.

- Samuels, R. (2019). *Special duty: A history of the Japanese intelligence community*. Cornell University Press.
- Sharpe, J., Trichas, M., & Terrill, D. (2024). Culture: A sixth domain and the introduction of the 'C6ISRT' framework. *Defence Studies*, 25(1), 22-46. <https://doi.org/10.1080/14702436.2024.2397520>
- Sheldon, R. (2005). *Intelligence activities in ancient Rome: Trust in the gods, but verify*. Routledge.
- Singh, G. (2005). *Fourth generation war: Paradigm for change*. Naval Postgraduate School.
- Sparrow, M. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*, 13(3), 251-252. [https://doi.org/10.1016/0378-8733\(91\)90008-H](https://doi.org/10.1016/0378-8733(91)90008-H)
- Sperber, D., Clément, F., Heintz, C., Mascaro, O., Mercier, H., Origgi, G., & Wilson, D. (2010). Epistemic vigilance. *Mind & Language*, 25(4), 359-393. <https://psycnet.apa.org/doi/10.1111/j.1468-0017.2010.01394.x>
- Spoor, B., & De Werd, P. (2023). Complexity in military intelligence. *International Journal of Intelligence and CounterIntelligence*, 36(4), 1122-1142. <https://doi.org/10.1080/08850607.2023.2209493>
- Stout, M. (2014). Intelligence in World War I: 1914-1918. *Journal of U.S. Intelligence Studies*, 20(3), 35-38.
- Sulick, M. (2015). Intelligence in the Cold War. *Journal of U.S. Intelligence Studies*, 21(1), 47-52.
- Sun Tzu. (2008). *The art of war*. Tuttle Publishing.
- Thomas, T. (2004). Russia's reflexive control theory and the military. *The Journal of Slavic Military Studies*, 17(2), 237-256. <https://doi.org/10.1080/13518040490450529>
- Tilmar, A. (2024). *Practical cyber intelligence: A hands-on guide to digital forensics*. Wiley.
- Tucídides. (1972). *History of the Peloponnesian War*. Penguin Classics.
- Uhlmann, A. (2022). Military intelligence and the securitization of Arabic proficiency in Israel: The limits of influence and the curse of unintended consequences. *Intelligence and National Security*, 37(4), 541-555. <https://doi.org/10.1080/02684527.2022.2065605>
- U.S. Army Training and Doctrine Command. (2011). *TRADOC handbook no. 525-92: Cultural and sociocultural understanding*. U.S. Army TRADOC G-2.
- Van Herpen, M. (2021). The many faces of the new information warfare. En O. Bertelsen (Ed.), *Russian active measures: Yesterday, today, tomorrow* (pp. 37-60). ibidem-Verlag.
- Varzhanskyi, I. (2024). Reflexive control as a risk factor for using OSINT: Insights from the Russia-Ukraine conflict. *International Journal of Intelligence and CounterIntelligence*, 37(2), 419-449. <https://doi.org/10.1080/08850607.2023.2228489>
- Warner, M. (2002). Wanted: A definition of intelligence. *Studies in Intelligence*, 46(3), 15-22. <https://tinyurl.com/2cjqpelv>

- Warner, M. (2013). The past and future of the intelligence cycle. En M. Phythian (Ed.), *Understanding the intelligence cycle* (pp. 24-34). Routledge.
- Warner, M. (2014). *The rise and fall of intelligence: An international security history*. Georgetown University Press.
- Weber, M. (1947). *The theory of social and economic organization*. Free Press.
- Wheeler, D. (2011). A guide to the history of intelligence in the age of empires, 1500-1800. *Journal of U.S. Intelligence Studies*, 18(3), 53-56.
- Wheeler, D. (2012). A guide to the history of intelligence: 1800-1918. *Journal of U.S. Intelligence Studies*, 19(1), 47-50.
- Wheeler, D. (2013). Intelligence between the World Wars: 1919-1939. *Journal of U.S. Intelligence Studies*, 20(1), 73-76.
- Whitesmith, M. (2022). Justified true belief theory for intelligence analysis. *Intelligence and National Security*, 37(6), 835-849. <https://doi.org/10.1080/02684527.2022.2076332>
- Wilkinson, T. (2013). *The rise and fall of ancient Egypt*. Random House.
- Wirtz, J. (2010). The sources and methods of intelligence studies. En L. Johnson (Ed.), *The Oxford handbook of national security intelligence* (pp. 59-69). Oxford University Press.
- Work, J. (2020). Evaluating commercial cyber intelligence activity. *International Journal of Intelligence and CounterIntelligence*, 33(2), 278-308. <https://doi.org/10.1080/08850607.2019.1690877>
- Yelamos, C., Goodman, M., & Stout, M. (2022). Intelligence and culture: An introduction. *Intelligence and National Security*, 37(4), 475-481. <https://doi.org/10.1080/02684527.2022.2065610>
- Zegart, A. (2022). *Spies, lies, and algorithms: The history and future of American intelligence*. Princeton University Press.