# Inteligencia posnormal: gestión de riesgos en la zona gris

*Jesús Hernández Álvarez*

**Resumen**

Este artículo cuestiona el paradigma tradicional de la inteligencia, surgido durante la Guerra Fría, analizando su transformación en el contexto de un entorno global en rápida evolución, caracterizado por la incertidumbre y la complejidad de los tiempos posnormales, abogando por un nuevo paradigma más adaptativo, multidisciplinar y cooperativo, que integre fuentes abiertas y una comunidad de inteligencia extendida.

Se explora la ciencia posnormal como marco conceptual para abordar problemas con hechos inciertos, valores en conflicto y decisiones urgentes, así como la evolución desde el ciclo de inteligencia tradicional hacia un enfoque de gestión de riesgos, integrando las funciones de inteligencia y gobernanza, en la búsqueda de una visión compartida del problema de seguridad a gestionar.

Asimismo, se subraya la importancia de comprender y mitigar las limitaciones cognitivas como los sesgos, fomentando el pensamiento sistémico y la modelización compleja asistida por IA para mejorar la conciencia situacional. Por último, se destaca la necesidad de proteger el ámbito cognitivo como un activo crucial frente a las estrategias híbridas en la zona gris, delineando posibles vectores de innovación para los Servicios de Inteligencia e Información del Estado en un entorno posnormal, lo que daría lugar a varios escenarios de evolución.

**Palabras clave**

Innovación, Servicios de inteligencia, Servicios de información, Evolución, Gobernanza.

## *Post-normal intelligence: risk management in the gray area*

**Abstract**

*This article questions the traditional intelligence paradigm that emerged during the Cold War, analyzing its transformation in the context of a rapidly evolving global environment characterized by the uncertainty and complexity of post-normal times. It advocates for a new, more adaptive, multidisciplinary, and cooperative paradigm that integrates open sources and an extended intelligence community.*

*It explores post-normal science as a conceptual framework for addressing problems with uncertain facts, conflicting values, and urgent decisions. It also explores the evolution from the traditional intelligence cycle to a risk management approach, integrating intelligence and governance functions in the pursuit of a shared vision of the security problem to be managed.*

*It also highlights the importance of understanding and mitigating cognitive limitations such as biases, fostering systems thinking and complex AI-assisted modeling to improve situational awareness. Finally, the need to protect the cognitive domain as a crucial asset against hybrid strategies in the gray zone is highlighted, outlining possible vectors of innovation for State Intelligence and Information Services in a post-normal environment, which would give rise to several evolutionary scenarios.*

**Keywords**

*Innovation, Intelligence services, Information services, Evolution, Governance.*

## 1 Introducción

Cuando se habla de innovación en el ámbito de la seguridad y la defensa, se suele pensar rápidamente en la de tipo tecnológico. En este sentido, es cierto que la innovación, que requiere una combinación de avances incrementales y tecnologías emergentes con capacidades disruptivas, actualmente se está centrando en los macrodatos y el análisis avanzado, la inteligencia artificial (IA), los sistemas autónomos, las tecnologías cuánticas, las tecnologías del espacio, las armas hipersónicas, las biotecnologías y tecnologías de mejora humana y los materiales avanzados y nuevas técnicas de fabricación (Martín Palma, 2023).

Además, en un entorno de tensiones geopolíticas, hay que resaltar el conflicto como motor de cambio, sobre todo, en cinco áreas: cambios sociológicos, tecnológicos, doctrinales, políticos y económicos. En este sentido, se podría entender el conflicto como el resultado de una mala adaptación a cambios previos, en un ciclo continuo de desadaptación-conflicto-adaptación (Frías Sánchez, 2023)

En este contexto y en lo que se refiere a la inteligencia, el presente artículo se centra más en aspectos doctrinales, conceptuales y metodológicos que en aspectos tecnológicos, que pueden ser relevantes en la transformación de los procesos y estructuras de los Servicios de Inteligencia e Información del Estado.

La Estrategia de Seguridad Nacional de 2021 se enfoca en una serie de vectores de transformación que, en los últimos años, han experimentado una aceleración notable y que han venido a cambiar el entorno estratégico. Se señala que el orden global y el paradigma socioeconómico liberal se encuentran en un periodo de cambio, sin que aún se haya definido con claridad el nuevo panorama del sistema internacional. Los principales vectores de transformación identificados son: el contexto geopolítico, el entorno socioeconómico, la transformación digital y la transición ecológica.

Igualmente, el sistema de prospectiva de la Unión Europea identifica catorce megatendencias que están moldeando el mundo en el momento de redactar este artículo. Estas incluyen la aceleración del cambio tecnológico y la hiperconectividad, el agravamiento de la escasez de recursos, la naturaleza cambiante del trabajo, una reconfiguración del paradigma de la seguridad, el cambio climático y la degradación ambiental, la continuación del proceso de urbanización, la diversificación de la educación y el aprendizaje, la ampliación de las desigualdades, la expansión de la influencia del este y del sur, el aumento del consumo, los crecientes desequilibrios demográficos, la creciente influencia de nuevos sistemas de gobierno, la relevancia de la migración y los cambios en los desafíos de salud.

Aunque estas tendencias globales y vectores de transformación pueden parecer distantes, sus efectos son palpables en la vida cotidiana y, en ocasiones, de manera dramática. Basta con recordar algunos acontecimientos significativos de los últimos cinco años: la pandemia de 2020, la retirada de tropas occidentales de Afganistán y el regreso al Gobierno de los talibanes en 2021, la invasión rusa de Ucrania en febrero de 2022, el lanzamiento de la IA generativa ChatGPT en noviembre de 2022, el ataque de Hamás en octubre de 2023, el intercambio de misiles entre Israel e Irán en 2024, la victoria de Donald Trump en las elecciones de EE. UU. en noviembre de 2024, la creciente polarización ideológica del nuevo Parlamento Europeo a finales de 2024, la caída del régimen sirio en diciembre de 2024 y el acercamiento del presidente de EE. UU. a Rusia en 2025.

La concentración de estos hechos y circunstancias de relevancia internacional en un periodo tan breve de tiempo nos convierte en testigos directos de un mundo en rápida transformación. Este cambio estructural en el sistema internacional está haciendo temblar las placas tectónicas de nuestra realidad, que, aunque parecían sólidas, se han estado deslizando de manera inadvertida hacia un futuro incierto.

La incertidumbre generalizada que producen estos hechos no hace sino reforzar la percepción del ciudadano de a pie de que el mundo es demasiado complejo para comprenderlo y es imposible analizarlo «racionalmente». Sin embargo, las organizaciones de inteligencia, que tienen como principal misión despejar estas mismas incertidumbres y complejidades para ofrecer los mejores cursos de acción, también se encuentran en mayor o menor medida abrumadas por la tarea.

Con este panorama de fondo, ha cobrado fuerza un concepto estratégico de primer orden, la *Zona Gris*, un espacio dentro del espectro del conflicto que está entre la competencia pacífica y la guerra, caracterizado por la ambigüedad, las estrategias multidimensionales (híbridas), intereses sustanciales en juego y la implementación gradual de estrategias para conseguir objetivos a largo plazo (Jordán, 2018). Este espacio es una zona del espectro de los conflictos donde predominan las actuaciones situadas al margen del principio de buena fe entre Estados (*bona fide*) que, pese a alterar notablemente la paz, no cruzan los umbrales que permitirían o exigirían una respuesta armada (Ministerio de Defensa, 2018).

Este escenario de confrontación ya está identificado por la Estrategia de Seguridad Nacional 2021 en mayor o menor medida, puesto que esta pone en relación las estrategias híbridas con los riesgos y amenazas en varios niveles de correspondencia: muy alta para la tensión estratégica y regional, el espionaje e injerencias desde el exterior, las campañas de desinformación, las amenazas a las infraestructuras críticas, la vulnerabilidad del ciberespacio, la inestabilidad económica y financiera y, por último, la

vulnerabilidad energética. En un nivel menor de relación con las estrategias híbridas, se situarían el terrorismo y la radicalización violenta, la vulnerabilidad del espacio marítimo, la vulnerabilidad del espacio aeroespacial, el crimen organizado y la delincuencia grave y, por último, la proliferación de armas de destrucción masiva.

En este contexto de confrontación en la zona gris en el que los componentes fundamentales de la Seguridad Nacional, concretamente la Defensa Nacional, la Seguridad Pública y la Acción Exterior, están tan interrelacionados, surge una pregunta: *¿es necesaria algún tipo de innovación por parte de los Servicios de Inteligencia e Información del Estado, de acuerdo con el ámbito de sus competencias, para seguir apoyando permanentemente al Sistema de Seguridad Nacional, proporcionando elementos de juicio, información, análisis, estudios y propuestas necesarios para prevenir y detectar los riesgos y amenazas y contribuir a su neutralización*? (art. 9 de la Ley de Seguridad Nacional).

La facilidad para formular esta pregunta contrasta con la dificultad para responderla, algo que este artículo no pretende hacer con rigor, sino que busca solo introducir una serie de elementos para alimentar la reflexión estratégica.

## 2 Ciencia posnormal

Es conocido que el ciclo de Inteligencia comparte con el método científico su enfoque sistemático y analítico, pero difieren en objetivos y aplicación. Mientras la ciencia busca verdades universales mediante el planteamiento inicial de hipótesis falsables y la posterior experimentación reproducible, la Inteligencia genera conocimiento práctico para decisiones urgentes, trabajando con datos incompletos y priorizando la acción sobre la perfección metodológica. Ambos usan procesos estructurados, pero el Ciclo de Inteligencia es más flexible, permitiendo saltar etapas ante emergencias.

En cuanto al contexto y rigor, hay que decir que el método científico exige controles estrictos y replicabilidad, mientras la Inteligencia opera en entornos dinámicos donde la incertidumbre es inherente. Por ejemplo, un científico descartaría datos no verificables, pero un analista de Inteligencia podría usarlos para prevenir una amenaza inmediata asumiendo ciertos riesgos. En esencia, la Inteligencia adapta el rigor científico a realidades donde la velocidad y la utilidad operativa son críticas.

Sin embargo, la distancia entre la Inteligencia y la ciencia parece acortarse en los últimos años. El contexto de cambio al que a diario se enfrentan las organizaciones de Inteligencia también ha sido motivo de discusión científica no tanto desde un punto de vista técnico, sino epistemológico. En las últimas décadas han aparecido planteamientos teóricos y metodológicos

que cuestionan la forma habitual de hacer ciencia, como pueden ser el Modo 2, la ciencia posacadémica y la ciencia posnormal (Jiménez-Buedo and Vielba, 2009).

Durante los últimos tres siglos, de forma progresiva, se puso a la ciencia en un lugar central, atribuyéndole la capacidad de proporcionar evidencia cuantitativa, objetiva y neutral, así como un creciente poder explicativo. El modelo tradicional de resolución de problemas suponía la estricta separación entre hechos (el territorio de la ciencia) y valores (el territorio de la gobernanza), y concebía un proceso en el que, obtenida la verdad, se procedía a la acción política para el bien común. La idea era sencilla: a) cualquier problema práctico-político se puede traducir como un problema técnico-científico y b) la resolución del problema técnico-científico resuelve el problema práctico-político. (Hidalgo y Funtowicz, 2024).

Sin embargo, en el año 1993, Silvio Funtowicz y Jerome Ravetz acuñaron el término ciencia posnormal —CPN— para referirse a una nueva manera de afrontar los problemas científicos en situaciones concretas, situando su enfoque a caballo entre la ciencia y la gobernanza. La CPN se define por cuatro características principales: *los hechos son inciertos; existe una pluralidad de valores, usualmente en conflicto; lo que se pone en juego es potencialmente muy elevado y las decisiones son urgentes*. Como se puede ver, estos presupuestos son los que caracterizan muchos de los entornos de operaciones que los Servicios de Inteligencia y de Información vienen enfrentando desde hace años.

En este enfoque, la atención se desplaza de la búsqueda de una verdad única definida por la ciencia hacia la calidad de los procesos de construcción del conocimiento en relación con un propósito social y políticamente determinado. En este sentido, la CPN reconoce como paritario el conocimiento creado fuera del ámbito científico, incluyendo el conocimiento práctico, la experiencia, asumiendo que no basta solo con «saber qué», sino que también es necesario «saber cómo». Desde esta perspectiva, y en el ámbito de la seguridad y la defensa, podría interpretarse que la CPN estaría poniendo al mismo nivel a los científicos y a los analistas de Inteligencia en lo que a producción de conocimiento de calidad se refiere.

Esta concepción paritaria del conocimiento se materializaría, según los autores, en una «comunidad extendida de pares» o «comunidad extendida de evaluación», que amplía la evaluación de la calidad del conocimiento más allá de los expertos de cada una de las disciplinas científicas. En contextos posnormales, la participación, la inclusión y la diversidad de voces contribuyen a la evaluación de la calidad del conocimiento.

El desafío estaría en cómo crear esta extensión de la comunidad de pares en situaciones de conflicto real, reconociendo que las transformaciones

sociales emergen de estos procesos. La CPN propone una reforma donde la extensión democrática del derecho al conocimiento no solo es ética y políticamente eficaz, sino que también «potencia la calidad de la evidencia tecnocientífica» para la acción orientada al bien común.

En definitiva, la CPN plantea que el modelo moderno de resolución de problemas basado en la predicción y el control es obsoleto. Esto requiere asumir la imposibilidad de predecir y justificar la acción política únicamente sobre predicciones, orientándose hacia una «ciencia de la anticipación responsable» que se ocupe de la calidad de los procesos de funcionamiento de las instituciones. Así, y en última instancia, ante la inevitabilidad del error o la aparición de hechos inesperados, la atención debería centrarse en gestionar los fracasos «con legitimidad político-institucional».

La asunción de cierta inevitabilidad y la imposibilidad de la ciencia para hacer predicciones fiables frente a problemas altamente complejos ya fue apuntada en 2007 por Nassim Nicholas Taleb, quien revitalizó el concepto de «cisne negro» para referirse a eventos raros e impredecibles que tienen un impacto significativo, argumentando que estos eventos son inevitables y que nuestra percepción de ellos cambia después de que ocurran, tendiendo a creer que eran más predecibles o inevitables de lo que, en realidad, eran en el momento en el que se produjeron (sesgo retrospectivo). Además, y al igual que la CPN, este autor apuntó en 2012 que el esfuerzo social debe ir dirigido a reforzar nuestras capacidades para soportar lo impredecible, acuñando el concepto de «antifrágil» para describir sistemas que no solo resisten el caos, sino que también se benefician de él, mejorando en cada iteración de enfrentamiento a la adversidad.

Sin embargo, hay que tener en cuenta que a la metáfora del «cisne negro» se contrapone la del «elefante negro», que describe problemas evidentes y conocidos por todos, con consecuencias potencialmente devastadoras, pero que son ignorados, de manera que la falta de acción o voluntad para enfrentarlos convierte su impacto en una crisis inevitable, ¿podríamos identificar nuestros propios elefantes negros?

Hasta aquí, se podrían extraer algunas conclusiones parciales si se aplica el marco conceptual propuesto por la CPN al contexto de funcionamiento de los Servicios de Inteligencia e Información: a) reforzar la capacidad para generar conocimiento mediante la creación de una comunidad extendida de expertos teóricos y prácticos; b) poner el foco en la calidad de los procesos de generación de conocimiento mientras se asumen las dificultades para predecir la evolución de determinados entornos, y c) que los efectos perjudiciales de la complejidad y la incertidumbre han alcanzado tal nivel que ha sido objeto de estudio científico, lo que demuestra el punto de transformación en el que se encuentra el mundo que nos rodea.

Complementando el marco conceptual de la CPN surge la *Teoría de los Tiempos Posnormales* (Sardar, 2019), que define con más detalle las situaciones de aplicación de la CPN, caracterizándolas por las cuatro S (en inglés) y las tres C:

— 4S: velocidad (todo se acelera), escala (los eventos adquieren una dimensión global), simultaneidad (las crisis ocurren al mismo tiempo) y alcance (penetrando incluso las partes más remotas del planeta).

— 3C: complejidad (sistemas interconectados e interdependientes), contradicciones (demandas contrapuestas e intereses antagónicos) y caos (pequeños eventos pueden desencadenar cambios enormes e impredecibles).

Los tiempos posnormales, según el autor, se manifiestan en diversos ámbitos. En la política, se observa el auge del populismo, la polarización y la crisis de la gobernanza. En la economía, el capitalismo desenfrenado conduce a una creciente desigualdad y a una incertidumbre radical. La tecnología, si bien ofrece oportunidades, también presenta riesgos como la manipulación, la pérdida de privacidad y el aumento del caos. La sociedad se enfrenta a la erosión de la confianza en las instituciones, la fragmentación y la difusión de la posverdad. Incluso la religión experimenta nuevas formas y tensiones en este contexto.

La teoría centra su atención en tres conceptos: la incertidumbre, la ignorancia y el horizonte temporal (los llamados Tres Mañanas), de manera que cada tipo de incertidumbre está intrínsecamente asociado a una categoría específica de ignorancia, lo que ayuda a comprender mejor la naturaleza de lo desconocido en cada horizonte temporal:

— La *Incertidumbre Superficial*, propia del *Presente Extendido*, se vincula con la *Ignorancia Simple*. En este horizonte, si bien la dirección general de los cambios puede ser previsible, se desconoce la magnitud y la probabilidad exactas de los eventos. Esta ignorancia es simple en el sentido de que se refiere a la ausencia de conocimiento sobre aspectos específicos, pero se considera superable a través de la recopilación de información, la investigación y el aprendizaje. Este es el ámbito propio de la ciencia tradicional.

— La *Incertidumbre Poco Profunda*, característica de los *Futuros Familiares*, se relaciona con la *Ignorancia Vencible*. Aquí nos enfrentamos a una amplia gama de futuros posibles y la dirección del cambio es menos clara. La ignorancia es vencible porque, aunque no se sepa qué preguntas hacer en el presente, se reconoce que las respuestas a esas preguntas solo podrán encontrarse en el futuro, a medida que se experimente las consecuencias de las tendencias y los desarrollos actuales. Este es el ámbito propio de la aplicación de

conocimientos adaptados a cada situación por parte de consultores profesionales.

— La *Incertidumbre Profunda*, que define los *Futuros Impensados*, se asocia con la *Ignorancia Invencible*. En este horizonte, se desconoce por completo la naturaleza, la dirección y el impacto de los cambios, y nuestra propia forma de entender el mundo puede ser inadecuada. Esta ignorancia es invencible porque representa la ignorancia de nuestra propia ignorancia, aquello que no se sabe y que está fuera de los marcos de pensamiento convencionales. Abordar esta ignorancia requiere un replanteamiento fundamental de nuestras suposiciones y de la visión del mundo, siendo el ámbito propio de la ciencia posnormal, que recomienda potenciar la generación de conocimiento por parte de comunidades extendidas de expertos que se centren en la calidad de la generación del conocimiento, antes que en la predictibilidad del entorno.

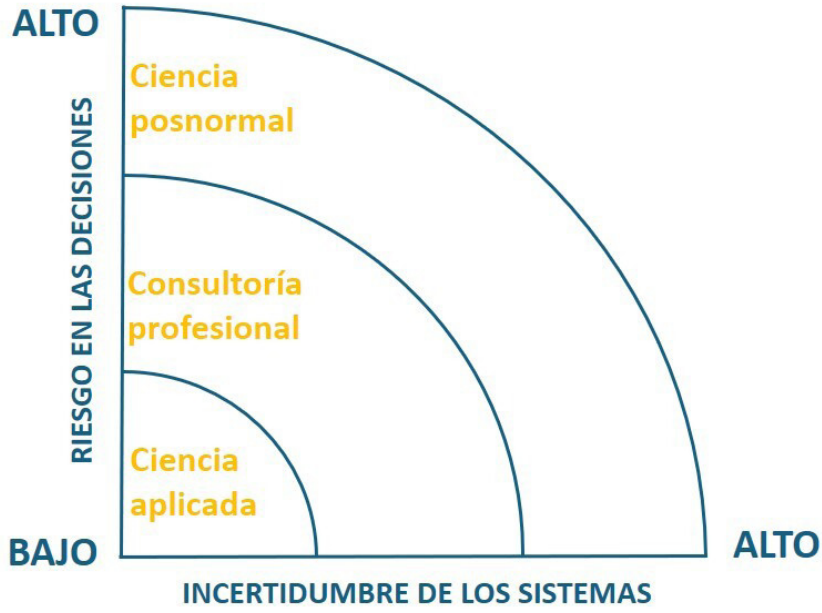


Figura 1: Relación entre incertidumbre y riesgo (elaboración propia)

En resumen, el nivel de profundidad de la incertidumbre refleja el grado en que nuestra ignorancia nos impide comprender el futuro. A medida que nos movemos del Presente Extendido hacia los Futuros Impensados, la incertidumbre se vuelve más profunda y el tipo de ignorancia al que nos enfrentamos se vuelve más fundamental, requiriendo estrategias cada vez más radicales para su comprensión y gestión.

Complementando las conclusiones parciales enumeradas con anterioridad se podría decir: a) que la ciencia posnormal es una especie de «extensión» de la ciencia tradicional; b) que una buena definición de las características de los problemas es clave para determinar la forma de abordarlos, situando las labores de inteligencia entre los límites de la consultoría experta y la ciencia posnormal; c) tratar de utilizar procedimientos propios de la ciencia aplicada a situaciones posnormales puede no ser el mejor enfoque.

## 3 Del ciclo de la inteligencia a la gestión del riesgo

Para una revisión crítica del ciclo de inteligencia, principal marco conceptual para comprender el proceso de producción de Inteligencia en seguridad y defensa se puede seguir a Javier Jordán (Jordán, 2016). Su análisis reconoce que el modelo del ciclo, a pesar de ser sencillo, lógico y fácil de comprender y recordar, así como de guardar cierta correspondencia con la organización interna de los servicios de inteligencia, es criticado por simplificar en exceso la realidad y no reflejar con precisión el proceso real de producción de inteligencia. El texto señala varias incongruencias entre el modelo ideal y la práctica real, ente otros: a) en la fase de dirección, los objetivos no siempre son claros y a menudo son los técnicos quienes impulsan el proceso; b) las fases de obtención y elaboración no son estrictamente secuenciales, sino que operan de forma paralela e interactiva; c) en la difusión, la información bruta puede llegar a los decisores sin análisis previo, y d) la inteligencia elaborada puede ser ignorada si contradice el marco ideológico del decisor político.

Además, cada fase del ciclo enfrenta limitaciones específicas, como restricciones presupuestarias, problemas de procesamiento de datos, limitaciones legales y dificultades de coordinación. Jordán menciona modelos alternativos, como el modelo de Treverton y Gabbard, que introduce la noción de «atajos» entre las fases; el modelo multiestratos de Lowenthal que subraya la importancia de la retroalimentación continua a lo largo del ciclo y, finalmente, describe la Inteligencia Centrada en el Objetivo (Target-Centric Intelligence) de Clark, que propone un enfoque en red donde todos los participantes colaboran en la construcción de una imagen compartida del objetivo. Los tres modelos alternativos reflejan la complejidad y la naturaleza no lineal del proceso real de Inteligencia. En conclusión, aunque el modelo tradicional del Ciclo de Inteligencia tiene valor pedagógico, es necesario considerar enfoques más flexibles que incorporen la interacción constante y la retroalimentación entre las diferentes etapas para comprender mejor el funcionamiento real de los servicios de Inteligencia.

Por otro lado, hay que decir que en las cuatro fases básicas del Ciclo no se tiene en cuenta el proceso de toma de decisiones en sí mismo, dado

que este acaba con la difusión de la Inteligencia hacia el decisor. Desde un punto de vista conceptual, existiría una clara brecha entre el conocimiento generado para resolver un problema de Inteligencia, las decisiones que se toman para resolverlo y el impacto de las decisiones en el propio problema. Recogiendo la propuesta de Clark, no se podría crear una imagen compartida del problema de Inteligencia si no existe un marco conceptual que englobe a todos los actores intervinientes, incluidos los que toman las decisiones.

Desde un enfoque policial, el Modelo 4-I (Intención, Interpretación, Influencia e Impacto) propuesto por Jerry H. Ratcliffe, desarrolla el marco conceptual para explicar la dinámica entre los actores clave en la producción y aplicación de inteligencia criminal, destacando cómo interactúan analistas, tomadores de decisiones y el entorno criminal (OSCE, 2020).


Figura 2. Modelo 4i (adaptado de Ratcliffe)

Sin embargo, no hay que olvidar que el Ciclo de Inteligencia, en última instancia, está subordinado a un proceso mayor de gestión de la seguridad y la defensa. Es precisamente en este punto donde la ciencia posnormal de Funtowicz y Ravetz plantea una nueva forma de afrontar los tiempos posnormales, justo en el punto donde el conocimiento científico/técnico y la gobernanza se dan la mano. Así, la pregunta no sería tanto ¿si el Ciclo de Inteligencia describe correctamente la actividad de los Servicios de Inteligencia e Información del Estado?, sino ¿cómo establecer un marco conceptual en el que se integre la actividad de estos junto con las actividades de gestión de los problemas de seguridad y defensa?

Una aproximación que puede poner en relación el conocimiento científico/técnico con el de los criterios de gobernanza podría ser la ofrecida por el marco conceptual establecido por la *norma UNE-ISO 31 000 Gestión de Riesgos*. La norma presenta las directrices generales para la gestión de cualquier riesgo por parte de organizaciones públicas o privadas, proponiendo un mapa de procesos.

Aplicando dicho mapa para la gestión por parte del Sistema de Seguridad Nacional (SSN) de los riesgos contemplados en la Estrategia de Seguridad Nacional y, entendiendo que los Servicios de Inteligencia e Información del Estado son un subsistema del SSN, se obtendría un marco conceptual que integraría tanto al subsistema de Inteligencia, como a los decisores y las medidas implementadas para reducir dichos riesgos, facilitando a todos los participantes compartir la misma visión del problema de seguridad a resolver como apuntaba Clark.

Basado en el que propone la norma UNE-ISO 31 000 a continuación se muestra el mapa de procesos (adaptado por el autor) que muestra la interrelación iterativa de procesos y su adaptación al funcionamiento del SSN:

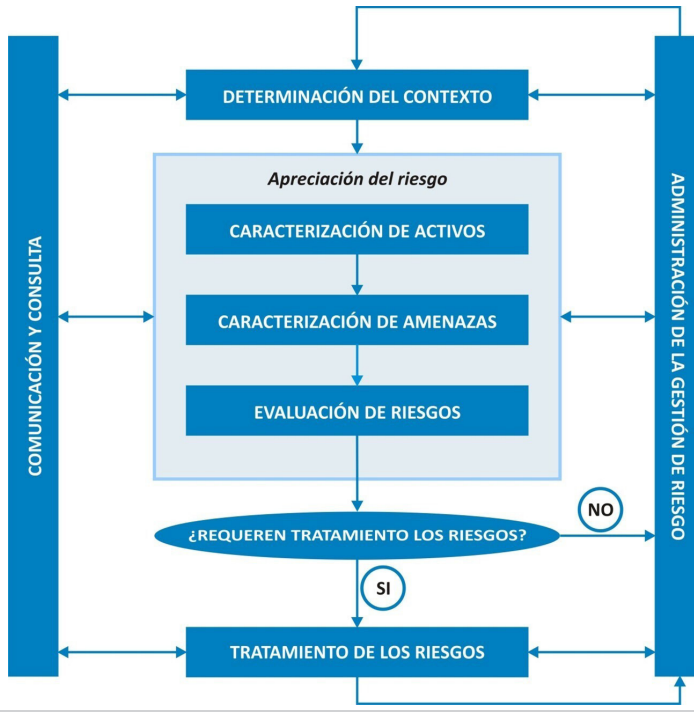


Figura 3: Mapa de procesos de gestión del riesgo (adaptado de norma UNE-ISO 31000)

— *Definición del contexto*: define el alcance de la gestión del riesgo, su ámbito geográfico, temporal y dominio donde se materializan los efectos, considerando factores internos al SSN y externos (entorno estratégico), estableciendo criterios de riesgo (umbrales de tolerancia) para evaluar su importancia, así como la definición de las normas y valores aplicables, también los actores del SSN implicados en cualquiera de los procesos de gestión de ese riesgo en concreto. En este proceso, estaría incluida la fase de Dirección del Ciclo de Inteligencia.

— *Comunicación y consulta*: implica a las partes tanto internas como externas al SSN relacionadas con la obtención e intercambio iterativo de información relevante aplicables al riesgo en cuestión. Este proceso sería asimilable al de Obtención del Ciclo de Inteligencia.

— *Apreciación del riesgo*: medidas de identificación, análisis y valoración del riesgo que puede implicar:

  - Caracterizar activos: identificación, análisis y valoración de los activos en riesgo. Implica determinar la criticidad o importancia relativa de los mismos, así como sus vulnerabilidades, dando lugar a un mapa de activos a proteger.
  - Caracterizar amenazas: identificar, analizar y valorar las amenazas que generan el riesgo. Implicaría la determinación de su peligrosidad, capacidad e intención para materializar el riesgo, dando lugar a un cuadro de amenazas.
  - Evaluar el riesgo, que implicaría establecer las hipótesis pertinentes que ponen en relación el riesgo en cuestión con las amenazas y los activos. La evaluación del riesgo respecto a los criterios establecidos por el SSN permite establecer prioridades de actuación identificando los riesgos que se pueden asumir y aquellos que deben ser tratados.

  Este proceso sería asimilable a la fase de Elaboración del Ciclo de Inteligencia e iría íntimamente ligada a la elaboración de productos de inteligencia para su Difusión a los responsables del siguiente proceso.

— *Administración y Gestión del Riesgo*: proceso en el que los responsables de la gestión y administración del riesgo en sus distintas perspectivas hacen un seguimiento y revisión de este, tomando las decisiones pertinentes apoyados por los informes de inteligencia recibidos.

— *Tratamiento del riesgo*: proceso por el que se establecen las condiciones para aplicar las medidas, así como su propia aplicación, tanto de carácter operativo como estratégico, orientadas a prevenir o

evitar la aparición del riesgo, la protección de los activos, la neutralización de las amenazas, así como las medidas tendentes a reducir los efectos o impacto del riesgo en caso de producirse.

Desde el punto de vista de la gestión pública, la definición de un mapa de procesos único para todo el SSN abre la puerta a establecer políticas claras de calidad en el funcionamiento de cada proceso, con independencia de los actores que participen en cada uno de ellos, lo que sin duda alguna redundaría en la calidad del conocimiento generado, lo que a su vez apunta en la dirección indicada por la ciencia posnormal.

Es importante recordar que el mapa de procesos es un modelo genérico que se aplica a riesgos concretos con sus propias características, de esta forma, se podrían definir los mapas de procesos que fueran necesarios para gestionar los dieciséis riesgos y amenazas priorizados en la Estrategia de Seguridad Nacional.

Sin embargo, desde la perspectiva de la generación de comunidades extendidas de iguales, quedaría por determinar qué actores deberían incorporarse al mapa de procesos, a lo que se tratará de responder más adelante. En todo caso, y sobre todo en una creciente hostilidad en la zona gris donde se entremezclan la Defensa Nacional, la Seguridad Pública y la Acción Exterior, parece prioritario la intensificación de la colaboración entre todos los Servicios de Inteligencia y Seguridad del Estado.

## 4 Inteligencia y cognición

Otro de los campos en los que el desarrollo científico ha favorecido la innovación en lo que a producción de Inteligencia se refiere ha sido las ciencias cognitivas. La analogía del ordenador, ampliamente utilizada desde hace décadas, compara el funcionamiento de la mente humana con el de una computadora, sugiriendo que ambos sistemas procesan información de manera similar. Esta analogía, cuestionada desde algunos aspectos, ha servido de modelo conceptual para numerosos avances en las ciencias cognitivas que, en el ámbito de la Inteligencia, han tenido un especial impacto en la fase de Elaboración. A continuación, se hacen algunas reflexiones al respecto, apuntando ciertas vías de mejora, que, en términos generales, ya se han iniciado. Para ello, se hará una breve mención a los sesgos cognitivos, el pensamiento sistémico, los modelos mentales y la conciencia situacional.

### *4.1 Sesgos cognitivos*

Siguiendo la tesis doctoral de Claudio Payá (Payá Santos, 2017) sobre los sesgos cognitivos del analista de Inteligencia, se puede decir que los sesgos cognitivos son errores sistemáticos y predecibles en el procesamiento de la información, inherentes a la estructura de la mente humana y

que pueden afectar la objetividad del análisis. Estos sesgos no son simples errores aleatorios, sino patrones de pensamiento que pueden conducir a conclusiones erróneas, incluso cuando el analista es consciente de su posible influencia.

Es importante resaltar el trabajo de Herbert Simon y el concepto de «racionalidad limitada», que desafió los límites de la racionalidad humana, demostrando que las personas no siempre optan por la elección que maximiza sus intereses. Simon argumentó que, frente a la complejidad del mundo, los seres humanos no pueden alcanzar un ideal de racionalidad perfecta y que, en lugar de ello, las personas utilizan diversas estrategias para simplificar su entorno. Más adelante, los trabajos de Kahneman y Tversky sobre heurísticos y sesgos abundaron en los límites de la racionalidad proponiendo dos sistemas de razonamiento:

— *Sistema Uno*: intuitivo, rápido e inconsciente, basado en heurísticas y emociones, que opera automáticamente, proponiendo respuestas rápidas al Sistema Dos y que es propenso a errores sistemáticos o sesgos.

— *Sistema Dos*: deliberado, lento y consciente, basado en la lógica y el esfuerzo cognitivo. Aunque más preciso, también está limitado por la capacidad mental. Un Sistema Dos perezoso hace que se racionalicen directamente las propuestas automáticas generadas por el Sistema Uno.

En el contexto del análisis de Inteligencia, estos sesgos pueden tener un impacto significativo. Pueden llevar a un cierre prematuro, donde los analistas llegan a conclusiones rápidamente sin explorar todas las posibilidades. La presencia de incertidumbre, la posibilidad de engaño por parte de adversarios y la tendencia a buscar información que confirme las hipótesis preexistentes (sesgo de confirmación) son factores que exacerban la influencia de los sesgos. La presión del tiempo y la necesidad de precisión también pueden intensificar estas limitaciones cognitivas.

Para mitigar el impacto negativo de los sesgos cognitivos en el análisis de inteligencia, se suelen utilizar las *Técnicas de Análisis Estructurado (TAE),* ampliamente difundidas desde 2011 gracias a la obra de Richards J. Heuer y Randolph H. Pherson. Estas técnicas están diseñadas para hacer más transparentes los argumentos analíticos, las suposiciones y las lagunas de inteligencia, ayudando a prevenir respuestas automáticas que puedan comprometer la solidez del análisis. Las técnicas, que tienen distintas aplicaciones, proporcionan un marco estructurado y están diseñadas para: descomponer problemas complejos en pequeños problemas de análisis más manejables; explicitar el proceso de análisis para convertirlo en un trabajo colaborativo; desafiar las hipótesis de trabajo, forzando una

justificación consciente de las conclusiones, forzando la incorporación de hipótesis alternativas; estimular la capacidad de prever e imaginar lo inesperado, impulsando la consideración de nuevas perspectivas e ideas para evitar el pensamiento único, etc.

Si bien es verdad que las TAE han venido a proporcionar una buena caja de herramientas a los analistas de Inteligencia, no es menos cierto que por mucha pericia que tenga, un albañil necesita de un arquitecto para tener la visión global del proyecto en el que está trabajando. Esta globalidad nos lo proporciona el pensamiento sistémico.

### *4.2 Pensamiento lineal vs. sistémico*

Otra de las limitaciones del sistema cognitivo humano es la tendencia al pensamiento lineal. Sin embargo, en este contexto de creciente complejidad global, la manera en que se abordan y se resuelven problemas ha cobrado una importancia crítica. El pensamiento lineal, caracterizado por un enfoque secuencial y analítico, ha sido el paradigma dominante durante décadas. No obstante, el pensamiento sistémico, que considera las interrelaciones y los patrones emergentes, ha ganado prominencia como una alternativa más holística y global. Los resultados indican que el pensamiento lineal es más efectivo en problemas bien definidos y de alcance limitado, mientras que el pensamiento sistémico muestra ventajas significativas en la resolución de problemas complejos e interconectados, sobre todo cuando existe un enfoque transdisciplinar (Lorenzo-Penalva, 2023).

La Teoría General de Sistemas, base del pensamiento sistémico, fue desarrollada por Ludwig von Bertalanffy en la década de 1940 y formalizada en 1969, proponiendo una visión holística de los sistemas naturales y sociales. Este biólogo austriaco concibió un enfoque interdisciplinario que considera los sistemas como conjuntos de elementos interrelacionados, enfatizando las propiedades emergentes que surgen de estas interacciones: el sistema es más que la suma de sus partes.

El modelado de un sistema empieza por establecer su estructura, identificando primero sus elementos de forma analítica (descomposición), para, posteriormente, establecer las relaciones entre los mismos en un esfuerzo de síntesis (integración). Estas relaciones se suelen representar mediante un diagrama de influencias, positivas o negativas, hasta el punto de que casi todo lo que nos rodea se puede entender como un sistema, e incluso como un sistema dentro de un sistema mayor (sistemas anidados).

Observando detenidamente un sistema, se pueden identificar bucles de realimentación, ya sean positivos o negativos. Un bucle de realimentación no deja de ser una cadena cerrada de influencias que empiezan y acaban en una misma variable. Un bucle de realimentación positiva tiende

a desestabilizar el sistema hasta que encuentra algún tipo de límite, generalmente un bucle de realimentación negativa, que tiende a estabilizar el sistema. Esta visión no lineal de los sistemas permite empezar a intuir la complejidad de estos, a la que se suma el retardo que los impactos de unas variables tienen en otras (Aracil J, 1995).

Esta metodología se ha aplicado para el análisis de problemas de seguridad, como la lucha contraterrorista (Pajares de Mena, 2010). Por ejemplo, tomando la variable «oportunidad política» definida por Sidney Tarrow para explicar el surgimiento y fortalecimiento del terrorismo como variable explicativa (Tarrow, 1994), se puede definir un sistema básico de confrontación terrorista/antiterrorista en el que las variables que conforman las capacidades terroristas constituyen el bucle de realimentación positivo que desestabiliza el sistema dado que: a más desestabilización (oportunidad política para los terroristas)→ más radicalización→ más capacidad terrorista→ más ataques → más desestabilización. Por otro lado, el bucle de realimentación negativo, formado por las variables que soportan las capacidades contraterroristas, establece básicamente que: a más desestabilización (oportunidad política para los terroristas)→ más capacidades contraterroristas→ menos capacidades terroristas→ menos ataques→ menor desestabilización. En el caso de ETA, la variable de salida, n.º de víctimas mortales, mostraría el estado del sistema caracterizado por una gráfica sigmoidal, inicialmente ascendente cuando prima el bucle positivo terrorista y descendente cuando prima el bucle negativo contraterrorista (Penalva Lucas, 2023).

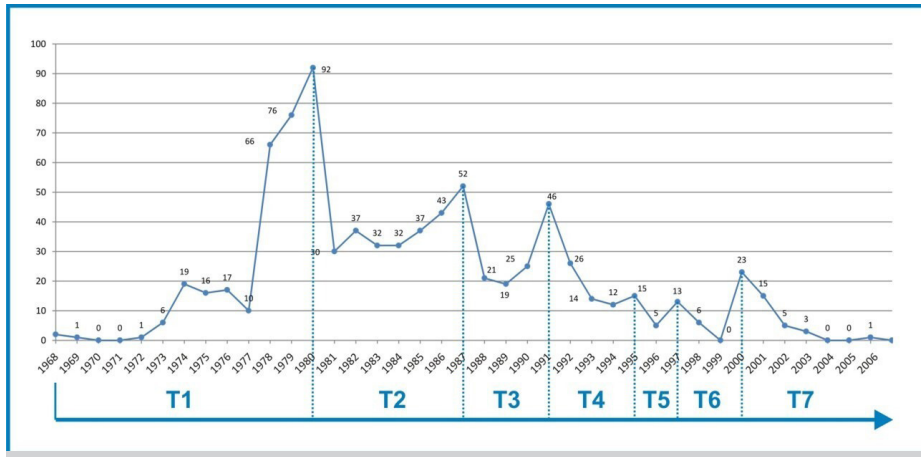


Figura 4: Víctimas mortales de ETA (elaboración propia)

Por otro lado, la dinámica de sistemas, especialmente los equilibrios inestables entre bucles de realimentación positivos y negativos, proporciona la metodología para explicar el hecho de que tras las revueltas árabes que se iniciaron a finales de 2010, surgiera la conformación de una

ventana de oportunidad para que surgiera DAESH, el grupo terrorista más letal conocido hasta la fecha. El surgimiento de una nueva «oportunidad política», en términos de Tarrow, ocasionada por dichas revueltas hicieron que los equilibrios terrorismo/contraterrorismo conseguidos hasta la fecha en algunos países del mundo árabe se vieran rápidamente modificados.

La desaparición, transformación o reducción de capacidades de los aparatos de seguridad de algunos de estos países supuso la desaparición de los límites de contención de una actividad terrorista latente en la zona. A la inestabilidad social y política generada por las revueltas en esos países, los grupos terroristas añadieron su propia desestabilización, realimentando el sistema hasta el punto llevar el caos a niveles de guerra civil en alguno de ellos. Por su parte, los aparatos de seguridad de estos países, incapaces de compensar las dinámicas ya generadas, tuvieron que ser apoyados por la Comunidad Internacional para contener la insurgencia terrorista, sobre todo, en Siria/Irak.

Los retardos en la toma de decisiones y en las estrategias a seguir, la falta de compromiso internacional inicial por la cantidad de recursos necesarios para gestionar de forma eficaz las distintas crisis, así como la incorporación de actores internacionales con sus propias dinámicas enfrentadas como Irán-Arabia Saudí, EE. UU. y Rusia, ofrecieron al yihadismo internacional el tiempo suficiente (retardo) para configurarse y adaptarse a una nueva realidad dando como resultado el surgimiento de DAESH.

Por otro lado, hay que considerar que las lógicas acción-reacción, relativamente simples en el caso de un sistema terrorista/contraterrorista, favorecen, en cierta manera, la predicción de la evolución del sistema. Sin embargo, si se quiere determinar la estructura de un sistema más complejo y ser capaz de predecir en cierto modo su comportamiento futuro, es importante establecer las normas que rigen las relaciones entre sus partes, así como las limitaciones existentes. Un buen ejemplo pueden ser las relaciones sistémicas que se pueden encontrar en el plano de las *relaciones internacionales*, en el que el motor de la dinámica del sistema internacional se verá condicionado por las relaciones de poder relativo entre los distintos actores componentes de este. Siguiendo las tesis neorrealistas de Kenneth Waltz, el sistema se mantendrá estable en la medida en que las estrategias de los actores sean estables porque no haya incentivos para cambiarlas, considerando las acciones de los demás. Los principios que regirían el sistema de relaciones internacionales (Jordán, 2022) son básicamente:

1. Anarquía: la ausencia de una autoridad central es el principio ordenador del sistema internacional. Esto significa que no hay una autoridad que regule las relaciones entre los Estados, lo que lleva a un entorno de autodefensa donde cada Estado debe asegurar su propia supervivencia.

2. Unidades Funcionalmente Similares: los Estados son unidades funcionalmente similares, ya que no se especializan en funciones específicas como lo hacen en sistemas jerárquicos. Esto se debe a que ningún Estado quiere depender de otros para su supervivencia.
3. Distribución de Capacidades: la estructura del sistema internacional también se define por la distribución de capacidades entre los Estados. Esta distribución puede ser bipolar, multipolar o unipolar, lo que afecta a la estabilidad del sistema.
4. Seguridad como Objetivo Principal: los Estados buscan asegurar su supervivencia y seguridad por encima de otros objetivos. Esto limita la cooperación y crea competencia por la seguridad.
5. Equilibrio de Poder: los Estados tienden a equilibrar el poder entre sí para mantener la estabilidad en el sistema internacional.

Independientemente de la existencia de otros modelos sobre relaciones internacionales, el modelo de Waltz ayuda a ejemplificar el modelado de sistemas complejos de los que se pueden derivar problemas de seguridad, pero que vienen sustentados por un marco conceptual previo que determina las normas de funcionamiento del sistema establecidas por la investigación científica. En este sentido, la modelización basada en modelos conceptuales sólidos es básica.

### *4.3 Modelos mentales vs. modelos conceptuales*

Relacionado con el apartado anterior, hay que tener en cuenta desde el punto de vista cognitivo los *modelos mentales*, que son representaciones internas y personales de la realidad externa que utilizan los individuos para comprender el mundo, razonar y tomar decisiones. Son construcciones idiosincráticas, incompletas, inestables y básicamente funcionales que se basan en la percepción individual y están influenciados por factores como la experiencia, el conocimiento previo, las creencias y las emociones del analista. Su principal objetivo es la funcionalidad, lo que a menudo prima sobre la exactitud. En contraste, los *modelos conceptuales* son representaciones externas, bien delimitadas, definidas y compartidas por una comunidad científica. Son coherentes con el conocimiento aceptado por esa comunidad y se distinguen de los modelos mentales por su carácter objetivo y consensuado.

En el análisis de Inteligencia, los analistas, de forma inevitable, elaboran y emplean modelos mentales para simplificar la complejidad de la realidad. Sin embargo, esta misma característica puede convertirse en una fuente significativa de error, puesto que la naturaleza subjetiva

e incompleta de los modelos mentales puede llevar a que diferentes analistas desarrollen representaciones distintas de un mismo fenómeno. Además, la resistencia al cambio de estos modelos puede dificultar la adaptación a nueva información, provocando que se ignoren o se interpreten de forma sesgada datos que no encajan con el modelo preexistente. Este sesgo de confirmación puede llevar a los analistas a sobrevalorar la información que confirma sus modelos y a descartar la que los contradice. En última instancia, el uso de modelos mentales incompletos, limitados o inadecuados puede conducir a hipótesis, estimaciones y predicciones erróneas, lo que puede resultar en fallos de Inteligencia con graves consecuencias.

Por lo tanto, es crucial que los analistas sean conscientes de sus propios modelos mentales y de cómo estos pueden influir en su análisis. En este sentido, la solución propuesta se centra en el entrenamiento para reconocer los propios modelos mentales, comprender cómo influyen en el procesamiento de la información, mantener una mente abierta, cuestionar las creencias y valorar diferentes perspectivas (Antonio Martínez-Sánchez, 2014) y, sobre todo, incorporar modelos conceptuales sólidos generados por la comunidad científica y compartirlos con la Comunidad de Inteligencia.

### *4.4 Conciencia situacional*

Como última referencia al ámbito cognitivo tras los sesgos, el pensamiento sistémico y los modelos mentales, hay que hablar de la conciencia situacional (CS) que afecta fundamentalmente a los responsables de la toma de decisiones. Para ello, se sigue el modelo de Mica Endsley (Endsley, 2000) que la define como «la percepción de los elementos en el entorno dentro de un volumen de tiempo y espacio, la comprensión de su significado y la proyección de su estado en el futuro cercano», de tal manera que la CS es un estado de conocimiento crucial para una toma de decisiones eficaz en entornos dinámicos. Sin embargo, hay que decir que la CS es un estado de conocimiento separado de la toma de decisiones ya que es posible tener una CS perfecta y tomar una decisión incorrecta, o viceversa. A pesar de todo, una buena CS aumenta la probabilidad de tomar buenas decisiones. También hay que decir que el verdadero reto radica en encontrar la información necesaria cuando se necesita, asumiendo que más datos no equivale a más información.

Si bien es cierto que el concepto de CS es muy usado en tareas con un alto componente de destrezas motrices y rendimiento en entornos muy dinámicos, como pilotos, controladores aéreos y medicina, la aplicación que se va a hacer de la CS está más enfocada hacia una CS de los decisores que tienen que resolver problemas de seguridad. La CS se estructura en tres

niveles interdependientes en los que los elementos cognitivos tienen un gran peso:

— Nivel 1: percepción de los elementos en la situación actual. Este nivel implica la detección y monitorización de la información relevante del entorno por parte del decisor, que no está libre de sesgos.

— Nivel 2: comprensión de la situación actual. Este nivel va más allá de la simple percepción e implica la integración, interpretación y evaluación del significado de los elementos percibidos en relación con las metas y objetivos del decisor.

— Nivel 3: proyección del estado futuro. El nivel más alto de CS implica la capacidad de anticipar eventos y dinámicas futuras basándose en la comprensión actual de la situación, lo que permitiría una toma de decisiones oportuna en el momento actual, pero anticipando sus efectos sen el futuro inmediato.

En el corazón del modelo de Endsley, se encuentran los modelos mentales, que, como ya se ha dicho, son estructuras de conocimiento almacenadas en la memoria a largo plazo que representan la comprensión de un individuo sobre un sistema o entorno y las relaciones entre sus componentes. Además de guiar la atención (Nivel 1) y facilitar la distinción entre las señales de interés y el ruido, los modelos mentales proporcionan un marco para la interpretación y la integración de la información percibida, facilitando la comprensión (Nivel 2), ayudando a determinar la relevancia de la información en relación con las metas. Los modelos mentales también son esenciales para la proyección (Nivel 3), ya que permiten anticipar estados futuros del sistema basándose en su estado actual y la comprensión de su dinámica interna.

Con todo, los esfuerzos deben ir encaminados a mejorar de manera continua la CS de los decisores, abordando estos factores cognitivos y apoyando la interiorización de modelos conceptuales precisos y adaptativos. Si bien, hay que ser consciente de que la labor va a ser especialmente compleja, si no imposible, en circunstancias posnormales cuando los hechos son inciertos; existe una pluralidad de valores en juego, usualmente en conflicto; lo que se pone en riesgo es potencialmente muy elevado; y las decisiones son urgentes.

## 5 Sistemas evolutivos

Llegados a este punto, parece claro que los Servicios de Inteligencia e Información del Estado deben transformarse y adaptarse al nuevo entorno de operaciones tal y como vienen haciendo desde hace años. Quizá uno de los casos más claros sea cómo España ha luchado contra el terrorismo

desde sus inicios en el siglo XIX, evolucionando para enfrentar las oleadas terroristas identificadas por Rapoport que han afectado a nuestro país: la anarquista (siglos XIX-XX), la de la nueva izquierda (segunda mitad del XX) y la religiosa (siglo XXI).

Sin embargo, las características de los tiempos posnormales, como la velocidad, la escala, simultaneidad y alcance de los cambios (4S), así como la complejidad, contradicciones y el caos (3C) que lo acompañan, hacen dudar del alcance y velocidad de la transformación necesaria para adaptarse a un entorno tan incierto.

Ante la incertidumbre que acompaña a la situación, puede ser útil seguir al prospectivista Jan Huston y su *Teoría de los Sistemas Evolutivos* (Huston, 1992, 2005) que postula que todos los sistemas en evolución, como los biológicos o sociales, experimentan cambios y transformaciones siguiendo una secuencia fundamental de cinco etapas:

— *Emergencia*: el inicio o aparición de un nuevo sistema.

— *Desarrollo*: un periodo de crecimiento y organización interna del sistema.

— *Madurez*: la fase en la que el sistema alcanza un estado de funcionamiento óptimo dentro de sus parámetros existentes.

— *Desestabilización*: una etapa caracterizada por el aumento de la complejidad interna y la creciente dificultad para mantener la estabilidad. Se identifican situaciones *críticas*, en las que el sistema es cada vez más sensible a los cambios, y *supercríticas*, en las que el sistema experimenta una complejidad excesiva e inmanejable.

— *Ruptura Transformacional*: un punto crítico donde el sistema se transforma, lo que puede resultar en su extinción o en el surgimiento de un sistema nuevo y diferente. Las opciones de transformación se limitan a tres niveles: superior (con potencial para una nueva secuencia evolutiva), lateral e inferior (ambas conduciendo a la extinción a diferentes ritmos).

En el caso que nos ocupa, se asume que los Servicios de Inteligencia e Información del Estado, entendidos como un subsistema del SSN, estarían saliendo de una fase de Madurez hacia una fase de Desestabilización ocasionada por el nuevo entorno estratégico, marcado por una reorganización del Sistema Internacional y una creciente tensión geopolítica que está afectando a los sistemas de seguridad, defensa e inteligencia a nivel europeo y mundial.

Antes de la ruptura transformacional, un sistema desestabilizado atraviesa fases de criticidad y supercriticidad, volviéndose cada vez más

sensible a los cambios internos y externos hasta experimentar una complejidad excesiva. Durante la fase supercrítica, el tipo de acciones predominantes determina el resultado de la transformación:

— *Acciones de Optimización*: se centran en explotar el funcionamiento del sistema existente con las mismas acciones conservadoras que llevaron a la supercriticidad. Esto limita las opciones transformacionales a niveles laterales o inferiores, conduciendo eventualmente a la extinción.

— *Acciones de Amplificación*: implican la exploración de acciones nuevas o novedosas para posibilitar opciones de alcanzar un nivel superior, caracterizadas por nuevas estructuras organizativas y simplificación de procesos capaces de absorber la complejidad.

En los sistemas evolutivos, procesar información es vital para la adaptación: mayor capacidad de análisis permite anticipar cambios y diseñar respuestas flexibles. Cuando un sistema alcanza un umbral crítico (sobrecarga informativa o incompatibilidad con estructuras existentes), se desestabiliza, generando caos que fuerza su reorganización en un orden más complejo. La desestabilización no es un fracaso, sino una fase de innovación donde el sistema evoluciona al ser capaz de integrar y gestionar de forma eficiente cada vez más información.

Algunos autores apuntan a conceptualizar las amenazas a la Seguridad Nacional como sistemas complejos sociales, proponiendo el uso de técnicas analíticas estructuradas (TAE), el modelado de sistemas y la inteligencia artificial (IA) como principales herramientas para su estudio (Gil Armario, 2024). Considerando que las amenazas actuales se caracterizan por su dinamismo, interdependencia, complejidad tecnológica y estrategias híbridas, el autor apunta a un cambio de paradigma en la inteligencia, en el que se pase de un modelado de los sistemas de forma cualitativa mediante TAE a un modelado mixto, mediante el modelado asistido por IA y con equipos multidisciplinares para enfrentar los desafíos del siglo XXI.

En este punto, surgen varias preguntas: ¿qué tipo de acciones deberían adoptar los Servicios de Inteligencia e Información del Estado para evolucionar hacia estados superiores de eficiencia que garanticen su adaptación? ¿acciones de *optimización?*, es decir, más de lo mismo mediante pequeños avances incrementales ¿acciones de *amplificación* mediante cambios más disruptivos y atrevidos? ¿Sabríamos distinguir qué medidas son de un tipo y de otro? ¿es suficiente con la integración de la IA en los procesos de trabajo? ¿más TAE? ¿mejores modelos conceptuales? ¿mejor modelado de sistemas complejos? ¿un nuevo mapa de procesos de gestión del riesgo? ¿una reestructuración de los Servicios de Inteligencia e Información del Estado?

## 6 Un nuevo paradigma en la Inteligencia

Desde posiciones ajenas a la ciencia posnormal, son varias las voces que reclaman desde hace años una revisión del marco conceptual sobre el que se ha venido sustentando la Inteligencia tradicional (Lahneman, 2010) (Arcos, Antón, 2010), si bien recientemente se han recogido esas y otras aportaciones (Ivars Pérez, 2023), para apuntar propuestas sobre un nuevo paradigma de inteligencia, sin embargo, en la exposición se seguirá, en especial, a Lahneman.

En el ámbito de la seguridad y la defensa, la Inteligencia ha sido históricamente una herramienta crucial para los Estados en la garantía de su supervivencia y la consecución de objetivos políticos. Sin embargo, las amenazas a los Estados han evolucionado significativamente a lo largo del tiempo, influenciadas por el devenir histórico, los avances tecnológicos y eventos trascendentales como el fin de la Guerra Fría y la globalización. Esta situación ha llevado a que diversos autores hayan concluido que el paradigma tradicional de la Inteligencia está obsoleto y es necesario uno nuevo.

La Inteligencia tradicional o Viejo Paradigma se desarrolló de manera significativa durante la Guerra Fría y la labor de los analistas se asemejaba a la resolución de un rompecabezas centrado en el descubrimiento de secretos, con un interés limitado en la información de fuentes abiertas. Las amenazas, originadas por adversarios estatales con pautas de comportamiento simétricas y nítidas, hacían que predominara la Inteligencia militar.

Sin embargo, el contexto actual, debido a su complejidad, contradicción y caos, difiere sustancialmente del periodo de la Guerra Fría. El concepto de seguridad se ha ampliado para integrar factores económicos, migratorios, informativos, energéticos, etc. Las amenazas han devenido transnacionales y multicausales, con actores estatales, no estatales e incluso institucionales, lo que dificulta la distinción entre amenazas internas y externas. La velocidad del cambio es alta y la predictibilidad baja, lo que exige una adaptación de los métodos de Inteligencia.

Ante este nuevo escenario, Lahneman plantea un Nuevo Paradigma de la Inteligencia, basado en la interpretación adaptativa de la información, en un enfoque más proactivo, multidisciplinar y cooperativo. Ello implica la construcción de modelos complejos con información principalmente procedente de fuentes abiertas, lo que requeriría extender la comunidad de Inteligencia y la inclusión de diversos actores de la Administración Pública, la sociedad civil y el mundo empresarial para lograr un enfoque holístico e integrador en el análisis de la realidad, lo que supondría un alto nivel de intercambio de información de forma voluntaria y una gran confianza mutua. El autor apuesta por la integración de dos flujos principales de información, la tradicionalmente secreta proporcionada por la comunidad de Inteligencia

y otro flujo de información abierta pero evaluada, de manera que resulte en información confiable de alto valor. En definitiva, Lahneman destaca el dilema entre el secreto del paradigma tradicional y la apertura necesaria para una interpretación adaptativa de una realidad que evoluciona rápido y que deja un gran rastro de información útil al alcance de todos.

Por su parte, otros autores han fusionado las ideas de Lahneman con los conceptos de los tiempos posnormales (Serra and Sardar, 2017), dando como resultado una síntesis interesante que da una conclusión clara, la necesidad de ampliar el número de actores implicados en la producción de inteligencia. Si por un lado la ciencia posnormal reconoce como paritario el conocimiento creado fuera del ámbito científico, incluyendo el conocimiento práctico, por otro Lahneman aboga por ampliar la comunidad de Inteligencia fusionando información procedente de fuentes abiertas con alto valor añadido.

## 7 El ámbito cognitivo como activo a proteger

Por último, se introduce un último elemento de discusión en cuanto a la necesidad de transformación de los Servicios de Inteligencia e Información del Estado se refiere: *el ámbito cognitivo*. El nuevo entorno de operaciones se caracteriza por la incorporación del ámbito cognitivo a los dominios de operaciones, sumándose al terrestre, aeroespacial, marítimo y ciberespacio. En esencia, se puede considerar el multidominio como un concepto innovador que EE. UU. desarrolló para adaptarse a los nuevos escenarios operativos, en los que hay que coordinar los efectos de las distintas capacidades militares en distintos planos o dominios para alcanzar ventajas operacionales o estratégicas (Gutierrez de León, 2023).

Por su parte, la doctrina de las Fuerzas Armadas concibe el ámbito cognitivo como «[...] el ámbito intangible inherente al ser humano, considerado de forma individual, socializada u organizada y es consustancial a su capacidad de juicio y de toma de decisiones. Este ámbito alcanza a las voluntades de todas las personas afectadas por el conflicto y a los sistemas de inteligencia artificial, por lo que impregna al resto de ámbitos. Su principal limitación es que para operar en él se manejan aspectos intangibles y de difícil evaluación, como los valores, las percepciones, la conciencia, las actitudes y los prejuicios. Se entiende por percepción la interpretación subjetiva, elaboración personal o representación mental, fruto de la interiorización de la información y los estímulos recibidos del entorno. Este ámbito permite a las Fuerzas Armadas alcanzar objetivos que quedan fuera del alcance de otros, mediante el empleo de técnicas de comunicación, la ciencia psicológica y otras ciencias sociales.» (Ministerio de Defensa, 2018).

Su introducción en la discusión no atiende a la necesidad de desarrollar operaciones militares en el ámbito cognitivo, para lo que se puede seguir

a Donoso (Donoso, 2020), sino por la necesidad de adaptar las capacidades del SSN para protegerlo, habida cuenta de que el sistema de creencias y valores de una sociedad democrática es uno de sus principales activos. El ámbito cognitivo, fortaleza de las democracias liberales, ha devenido en vulnerabilidad en el contexto de la revolución digital, lo que está siendo aprovechado por actores hostiles en un contexto de confrontación en la zona gris. Así, la adaptación de los Servicios de Inteligencia e Información del Estado a este nuevo entorno es crucial; debiendo encontrar estrategias efectivas para gestionar los riesgos de desinformación, radicalización, polarización, desafección política, pérdida de confianza en las instituciones, negacionismo científico, etc., todo ello en un contexto de libertad ideológica propio de una democracia liberal, lo que lo convierte en un auténtico desafío posnormal a nuestra seguridad.

## 8 Conclusiones: escenarios de innovación

Al principio del artículo nos preguntábamos si es necesaria algún tipo de innovación por parte de los Servicios de Inteligencia e Información del Estado, de acuerdo con el ámbito de sus competencias, para seguir apoyando permanentemente al Sistema de Seguridad Nacional, proporcionando elementos de juicio, información, análisis, estudios y propuestas necesarios para prevenir y detectar los riesgos y amenazas y contribuir a su neutralización. En mi humilde opinión, que representa solo al autor y no a la institución a la que pertenece, durante el artículo se han identificado varias vías de mejora, muchas de ellas complementarias.

Dada la creciente hostilidad en la zona gris, donde se entremezclan la Defensa Nacional, la Seguridad Pública y la Acción Exterior, parece prioritaria la intensificación de la colaboración entre todos los Servicios de Inteligencia y Seguridad del Estado.

Si se asumen mínimamente los planteamientos posnormales se podría reforzar la capacidad para generar conocimiento mediante la creación de una comunidad extendida de expertos teóricos y prácticos; poner el foco en la calidad de los procesos de generación de conocimiento mientras se asumen las dificultades para predecir la evolución de determinados entornos y; aprender a identificar los tipos de incertidumbre a los que nos enfrentamos para adecuar las estrategias a seguir. En este sentido, sería interesante explorar el papel que la Oficina Nacional de Asesoramiento Científico (ONAC) podría llegar a tener, si bien es cierto que se tendría que complementar con la colaboración con los departamentos de seguridad e inteligencia de sectores estratégicos, muchos de ellos de carácter privado.

Desde el punto de vista de la gestión de procesos, resultaría interesante encontrar un punto de unión entre las actividades de Inteligencia (Ciclo de Inteligencia) y la gestión de los problemas de seguridad (gobernanza), centrando la atención en la calidad de los procesos de elaboración de conocimiento. En este sentido, el enfoque de la gestión del riesgo puede ser una vía que explorar, permitiendo el modelado de un sistema de riesgos interrelacionados que favorecería la conciencia situacional.

En lo que a Inteligencia y cognición se refiere, la reducción del impacto de las limitaciones cognitivas vendría de la mano de las TAE; las mejoras en la modelización de los sistemas, especialmente con la ayuda de la IA y; la incorporación de marcos conceptuales sólidos que puedan ser compartidos por los Servicios de Información e Información del Estado. Todo ello iría encaminado a mejorar no solo la elaboración de Inteligencia, sino la construcción de una consciencia situacional en el decisor que favorezca la toma de decisiones más adecuadas a cada situación.

En lo que se refiere al estado evolutivo de la Comunidad de Inteligencia española, está claro que todos sus componentes están tratando de adaptarse a un nuevo entorno estratégico. En este sentido, la innovación mediante avances incrementales parece una estrategia viable en circunstancias normales, pero se corre el riesgo de que los tiempos posnormales nos sorprendan con los deberes a medio hacer y con poco tiempo para reaccionar. Por otro lado, los cambios arriesgados y disruptivos tampoco son propios en la Administración Pública, donde la vocación de continuidad y estabilidad es un valor seguro que garantiza el funcionamiento del Estado a largo plazo. En todo caso, más allá de las adaptaciones de cada actor, la respuesta global del SSN no puede ser más que sistémica y debe tener en cuenta creciente interacción de los componentes fundamentales de la Seguridad Nacional en un contexto de creciente hostilidad que no se ve en Europa desde hace ochenta años.

En cuanto al equilibrio de información cerrada/abierta, el uso de fuentes abiertas para elaborar Inteligencia, tanto operativa como estratégica, se ha incrementado sobremanera en los últimos años, si bien resulta interesante la propuesta de aumentar la reserva de Inteligencia mediante expertos ajenos a la Comunidad de Inteligencia, generando un flujo de información confiable de carácter abierto.

Por último, dada la creciente importancia del ámbito cognitivo en las estrategias híbridas que se desarrollan en la zona gris, se propone la mejora de la protección del ámbito cognitivo en un contexto de revolución digital, desarrollando estrategias adaptadas a una sociedad liberal democrática que permitan gestionar adecuadamente los riesgos de desinformación, radicalización, polarización, etc.

Llegados a este punto, se pueden resumir una serie de vectores de innovación que pueden orientar el futuro de transformación de los Servicios de Inteligencia e Información del Estado:

- Integración de procesos de Inteligencia y gobernanza: gestión del riesgo como marco conceptual de las políticas públicas de seguridad.
- Foco en lo que se puede hacer (elefantes negros) y no tanto en lo que es difícil de predecir (cisnes negros): calidad y resiliencia de los procesos de Inteligencia.
- Marcos conceptuales sólidos compartidos por la Comunidad de Inteligencia.
- Gestión de las incertidumbres (superficial, poco profunda y profunda) de la manera más idónea: ciencia aplicada vs. posnormalidad.
- Integración de las ciencias cognitivas: TAE, modelado de sistemas, etc.
- Integración de procesos y mejora de la Conciencia Situacional de los decisores.
- Comunidades extendidas de Inteligencia.
- Simplificación y eficiencia de las estructuras de Inteligencia.
- Ámbito cognitivo como nuevo ámbito de confrontación: mejora de las capacidades de análisis y estrategias de acción en entornos democráticos.
- Fusión de capacidades de Inteligencia en la zona gris: coordinación y colaboración de los componentes fundamentales de la Seguridad Nacional.
- Innovación tecnológica: especialmente integración de la IA en procesos rutinarios, modelado de sistemas, etc.
- Flujos de información: generación de conocimiento mediante fuentes abiertas confiables.

Muchos de estos vectores de innovación ya forman parte de las líneas de acción de los Servicios de Inteligencia e Información del Estado, si bien, otros posiblemente no. La combinación de estos vectores ya sea de forma incremental o mediante saltos disruptivos pueden llegar a generar tres escenarios (Curry y Hodgson, 2008):

1. **Horizonte 1. Sistema dominante**: representa el presente y las prácticas mayoritarias ya vigentes en el SSN y su subsistema de Inteligencia. Se caracteriza por un alto grado de estabilidad y efectividad estratégica, aunque con el tiempo puede perder su adecuación al entorno posnormal, enfrentando dificultades de adaptación.

2. **Horizonte 2. Transición e innovación**: es un periodo intermedio entre el horizonte 1 y 3. Se caracteriza por la coexistencia de elementos del sistema dominante con innovaciones disruptivas. Este horizonte es ambiguo y turbulento, lleno de experimentación, creatividad y debates sobre el cambio. Algunas innovaciones pueden ser absorbidas por el sistema dominante, mientras que otras logran abrir camino hacia transformaciones más profundas.
3. **Horizonte 3. Futuro transformador**: representa una visión transformadora y un nuevo paradigma que, en su caso, reemplaza al sistema dominante actual. Este horizonte surge como respuesta a las deficiencias del horizonte 1, incorporando las innovaciones exitosas del 2. Aunque, inicialmente, es una posibilidad apenas percibida, con el tiempo se consolida como el nuevo sistema dominante gracias a su capacidad para adaptarse mejor al entorno cambiante.

En todo caso, el propio camino de transformación que recorra el subsistema de Inteligencia entra dentro de las incertidumbres poco profundas que solo el tiempo despejará.

## Bibliografía

Antonio Martínez-Sánchez, J. (2014). *The Use of Mental Models as a Source of Error in the Analysis of Intelligence*.

Aracil, J. (1995). *Dinámica de sistemas*.

Arcos, R. y Antón, J. (2010). *Reservas de Inteligencia: hacia una Comunidad ampliada de Inteligencia*.

Curry, A. y Hodgson, A. (2008). *Seeing in Multiple Horizons: Connecting Futures to Strategy*, *Journal of Futures Studies*.

Donoso, D. (2020). Aspectos psicológicos en el ámbito cognitivo de las operaciones militares. *Implicaciones del ámbito cognitivo en las Operaciones Militares*, pp. 21-45.

Endsley, M. R. (2000). *Situation Awareness Analysis and Measurement*. Lawrence Erlbaum Associates. [Consulta: 2025]. Disponible en: https://www.researchgate.net/publication/292771806

Frías Sánchez, C. (2023). El conflicto como motor de cambio. En: Ministerio de Defensa (ed.). *XXX Curso Internacional de Defensa. Los motores de cambio de la seguridad y la defensa*. Madrid, Ministerio de Defensa, pp. 153-162.

Gil Armario, J. M. (2024). La comprensión de las amenazas a la Seguridad Nacional como sistemas complejos sociales. Aplicación de las técnicas analíticas estructuradas, modelado de sistemas e inteligencia artificial. *Cuadernos de Inteligencia*. 2, pp. 49-74.

Gutiérrez de León, B. (2023). Las operaciones multidominio. En: Ministerio de Defensa (ed.). *XXX Curso Internacional de Defensa. Los motores de cambio de la seguridad y la defensa*. Madrid, Ministerio de Defensa, pp. 131-152.

Hidalgo, C. y Funtowicz, S. (2024). Epistemología política. Ciencia con la gente. *Revista iberoamericana de ciencia tecnología y sociedad*. 19(55), pp. 215-228. DOI: https://doi.org/10.52712/issn.1850-0013-454

Huston, J. (1992). *What are the greatest challenges for evolutionary theory in our times?*

Huston, J. (2005). *Which Way is Up?*

Ivars Pérez, J. (2023). Una aproximación teórica al viejo y nuevo paradigma de inteligencia para la seguridad. *Disjuntiva. Crítica de les Ciències Socials*. 4(1), p. 39. DOI: https://doi.org/10.14198/disjuntiva2023.4.1.3

Jiménez-Buedo, M. y Vielba, I. R. (2009). ¿Más allá de la ciencia académica?: Modo 2, ciencia posacadémica y ciencia posnormal. *Arbor*, pp. 721-737. DOI: https://doi.org/10.3989/arbor.2009.738n1048

Jordán, J. (2016). *Una revisión del ciclo de Inteligencia*. [Consulta: 2025]. Disponible en: http://www.seguridadinternacional.es

Jordán, J. (2018). The international conflict in the gray zone: A theoretical proposal from the offensive realism perspective. *Revista Española de Ciencia Politica*. 48, pp. 129-151. DOI: https://doi.org/10.21308/recp.48.05

Jordán, J. (2022). *Teorías realistas para comprender la política internacional*, *Global Strategy Report*, *N.º 4*. [Consulta: 10 marzo 2025]. Disponible en: https://global-strategy.org/teorias-realistas-para-comprender-la-politica-internacional/

Lahneman, W. J. (2010). The Need for a New Intelligence Paradigm. *International Journal of Intelligence and CounterIntelligence*. 23(2), pp. 201-225. DOI: https://doi.org/10.1080/08850600903565589

Lorenzo-Penalva, J. (2023). Inteligencia estratégica, transdisciplinariedad y sistemas complejos adaptativos. *Cuadernos de Inteligencia*. 1, pp. 51-61.

Martín Palma, R. J. (2023). Las tecnologías del futuro de la seguridad y la defensa. En: Ministerio de Defensa (ed.). *XXX Curso Internacional de Defensa. Los motores de cambio de la seguridad y la defensa*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2018). *PDC-01 (A) Doctrina para el empleo de las FAS*. [Consulta: 2025]. Disponible en: https://publicaciones.defensa.gob.es/

OSCE. (2020). *Guía de la OSCE sobre actividad policial basada en la inteligencia*. [Consulta: 22 febrero 2025]. Disponible en: https://www.osce.org/es/secretariat/455536

Pajares de Mena, M. D. M. (2010). *Dinámica de organizaciones terroristas domésticas*.

Paya Santos, C. (2017). *Aproximación transversal a los sesgos cognitivos del analista de inteligencia*.

Penalva Lucas, J. (2023). Análisis de modelos matemáticos aplicados a la lucha contra el terrorismo y los extremismos violentos. *Revista Política y Estrategia*. 140, pp. 35-62. DOI: https://doi.org/10.26797/rpye.vi140.1008

Sardar, Z. (2019). *The Postnormal Times Reader*. [Consulta: 2025]. Disponible en: https://www.cppfs.org/

Serra, J. y Sardar, Z. (2017). Intelligence in Postnormal Times. *World Futures Review*. 9(3), pp. 159-179. DOI: https://doi.org/10.1177/1946756717709277

Tarrow, S. (1994). *El poder en movimiento: Movimientos sociales, acción colectiva y política*.