

INTELIGENCIA ANTICIPATORIA: SISTEMAS QUE PREDICEN ANTES DE QUE EXISTAN LOS DATOS

Arquitectura estratégica en tiempos de incertidumbre profunda

I. EL GIRO INVISIBLE EN LA INTELIGENCIA.

De acumular datos a atreverse a imaginar el futuro.

Durante gran parte del siglo XX, la inteligencia estratégica descansaba sobre una idea que casi nadie se cuestionaba: el futuro sería una prolongación del pasado. Tal vez con variaciones, con ajustes y con alguna que otra sorpresa puntual. El método que se usaba era claro y aparentemente sólido: que miráramos hacia atrás, detectemos patrones, identificáramos las tendencias, y las extendiéramos hacia adelante. Un modelo inductivo que nos ofrecía seguridad en un mundo que parecía obedecer ciertas regularidades.

Pero ese suelo comenzó a agrietarse. No de golpe, sino de alguna manera silenciosa, que casi no podríamos apreciar. A medida que la complejidad del sistema global se aceleraba -interconectado, digitalizado, hiperreactivo- la idea de que el pasado nos podía servir como mapa confiable del mañana empezó a perder fuerza. El problema ya no era la falta de datos. De hecho, nunca habíamos tenido tantos. El problema era más profundo: el marco desde el que interpretábamos esos datos.

1.1 La ruptura epistemológica

Buena parte de este cambio puede entenderse a través del trabajo de **Robert Rosen**, especialmente en su obra '*Anticipatory Systems*'. Rosen introduce una distinción, que, aunque parece técnica, nuestra forma por completo nuestra manera de comprender la inteligencia:

- **Sistemas reactivos:** aquellos que cambian tras recibir un estímulo externo.
- **Sistemas anticipatorios:** aquellos que modifican su estado presente en función de predicciones internas sobre el futuro.

La diferencia no es meramente funcional. Es ontológica. Implica un cambio de la naturaleza misma del sistema, la inteligencia deja de limitarse a describir lo

que ocurre y comienza a proyectarnos lo que podría ocurrir. Ya no espera a que el entorno cambie para reaccionar; incorporó un modelo interno del entorno que le permite actuar antes de que el cambio se materialice.

En otras palabras, podemos decir que deja de ser un espejo del mundo para convertirse en una arquitectura que lo prefigura. Y esto nos transforma por completo la manera en que concebimos la estrategia.

1.2 Complejidad y tiempos posnormales

Este giro se vuelve aún más evidente en el marco conceptual de los *'Tiempos Posnormales'*, desarrollado por **Ziauddin Sardar** que trabajado estratégicamente por **Jordi Serra del Pino**. Se trata de contextos definidos por rasgos que hoy resultan casi familiares

- No linealidad
- Aceleración
- Interdependencia sistémica
- Colapso de ortodoxias

Vivimos en sistemas complejos adaptativos, como los describía **John Holland** en 1992. En estos sistemas, pequeñas perturbaciones pueden desencadenar efectos desproporcionados. Una decisión marginal puede convertirse en un fenómeno global. **Una señal débil puede anticipar una ruptura estructural**. La famosa sensibilidad a las condiciones iniciales deja de ser una curiosidad matemática para convertirse en un desafío estratégico real. En este contexto, la extrapolación lineal pierde potencia explicativa. No porque tengamos un análisis histórico que deje de tener valor, sino porque ya no basta. El entorno cambia más rápido que nuestras categorías.

En **inteligencia estratégica**, esto se manifiesta en lo que se conoce como sorpresa estratégica, es un fenómeno ampliamente analizado tras el ataque del 11-S y otros episodios disruptivos. Lo más inquietante es que en muchos casos la información estaba disponible. Las señales ya existían. El fallo no fue la ausencia de datos, sino la incapacidad para integrarlos dentro de un modelo que permitiera comprender su significado.

Ahí está la verdadera quiebra: no es en cuánto sabemos, sino en cómo estructuramos lo que sabemos para anticipar lo que todavía no ha ocurrido.

II. DE LA INTELIGENCIA REACTIVA A LA INTELIGENCIA ANTICIPATORIA

Como hemos ido cambiando, y por qué ya no basta con reaccionar.

2.1 El modelo clásico: ciclo de inteligencia

Durante décadas, lo que conocemos cómo “**ciclo de inteligencia**” no ha sido solo un procedimiento técnico. Ha sido, en realidad, una forma de entender el mundo. Una arquitectura mental e institucional que ha moldeado la manera en que los estados perciben el riesgo, la amenaza y la seguridad.

Para su formulación moderna aparece sistematizada en obras como: *‘Intelligence: from secrets to policy’* de **Mark. M. Lowenthal**, aunque su lógica es mucho más antigua: tomar información dispersa y convertirla, mediante una secuencia ordenada en conocimiento útil para poder decidir. El ciclo parte de una idea sencilla y muy poderosa: **la realidad estratégica deja señales**. Y si esas señales se recogen, se procesan y se analizan correctamente, permitirá anticipar riesgos antes de que estallen.

Este modelo funcionó razonablemente bien en entornos estructurales estables. Durante la Guerra Fría, por ejemplo, la rivalidad entre bloques producía indicadores relativamente claros: movimientos de tropas, pruebas de misiles, comunicaciones interceptadas, cambios doctrinales visibles. El adversario estaba identificado, sus capacidades eran medibles y el conflicto se movía dentro de marcos relativamente previsibles.

En este contexto, la inteligencia era, sobre todo, acumulativa. El decisor político formulaba una pregunta -las conocidas “*Priority Intelligence Requirements*”- y la maquinaria institucional se activaba. Así se obtenía información de fuentes humanas, señales electrónicas, imágenes satelitales o fuentes abiertas. Esta información se depuraba, se estructuraba y finalmente analistas especializados la convertían en un informe. El conocimiento fluía de manera lineal: del dato la decisión. Pero esta arquitectura tiene supuestos que rara vez se verbalizan.

Primero, presupone que las **amenazas dejan huella** antes de desplegarse plenamente. Confía en que el entorno cambie de forma detectable y gradual. Segundo, asume que el pasado es una guía suficientemente fiable para interpretar el presente. La inteligencia clásica funciona, en esencia, como un sistema sofisticado de reconocimiento de patrones: podemos comparar lo que ocurre ahora con lo que ya ha ocurrido antes. El problema aparece cuando el entorno deja de comportarse de forma incremental.

En sistemas complejos -no lineales, interdependientes y acelerados- las rupturas pueden producirse sin aviso estadístico claro. Tras el 11-S, numerosos estudios mostraron algo inquietante: la información ya existía. **Las señales estaban ahí.** Lo que falló no fue el ciclo técnico, sino el marco mental que debía integrar señales dispersas en una narrativa coherente. El sistema funcionó administrativamente, pero falló cognitivamente.

Hay además otra limitación estructural: el ciclo depende de cómo se formula el problema inicial. Solo buscamos aquello que se considera relevante, si el fenómeno emergente ni siquiera entra en el horizonte conceptual del decisor, el sistema queda ciego. La **inteligencia reactiva** necesita que algo sea imaginable para poder investigarlo. En entornos de innovación disruptiva, el conflicto híbrido o transformación tecnológica acelerada, tenemos esta limitación y se vuelve crítica.

Y está también la cuestión del tiempo. El ciclo clásico tiene un ritmo, requiere recopilar, contrastar, validar. Este tempo era compatible con entornos estratégicos más lentos, pero hoy hablamos de ciberataques que se ejecutan en segundos, campañas de desinformación que se visualizan en hora y crisis políticas que escalan en cuestión de días. A veces la inteligencia llega... pero llega cuando el fenómeno ya está en marcha.

Nada de esto convierte al modelo clásico en obsoleto, sigue siendo indispensable para evaluar capacidades militares convencionales, programas armamentísticos o tendencias macroeconómicas consolidadas. Su disciplina metodológica y su trazabilidad son fortalezas indiscutibles. El problema no es el modelo en sí, es el mundo para el que fue diseñado.

El paradigma tradicional -estructurado en dirección, obtención, procesamiento, análisis y difusión- funciona bien cuando:

- El entorno es relativamente estable
- Las amenazas son recurrentes
- Existen patrones históricos sólidos

Pero cuando desaparecen la estabilidad, la gradualidad y la detectabilidad clara, el ciclo revela su naturaleza esencialmente reactiva. Transforma datos en conocimiento, pero no necesariamente transforma posibilidades en preparación estructural. Aquí nos aparece la necesidad de una capa adicional: una que no espere a que la señal sea visible para empezar a pensar estratégicamente.

2.2 Eventos de baja frecuencia y alto impacto

Uno de los mayores desafíos para cualquier sistema de inteligencia no es lo que ocurre todos los días, sino lo que ocurre rara vez... pero cuando ocurre, cambia las reglas del juego.

El análisis de estos fenómenos extremos ha sido trabajado por **Nassim Nicholas Taleb** en '*The Black Swan*'. No se trata simplemente de "sorpresas", se trata de rupturas estructurales. Los sistemas reactivos fallan ante:

- Eventos no lineales
- Cambios abruptos
- Rupturas de régimen

¿Por qué? Porque su arquitectura descansa en la memoria estadística. Si algo ha ocurrido poco, recibe menos atención. Si no hay precedentes suficientes, se percibe como improbable. Pero en sistemas complejos, lo raro puede ser decisivo.

Un atentado terrorista masivo, una innovación tecnológica disruptiva, el colapso repentino de un régimen aparentemente estable o una pandemia global pueden tener baja frecuencia e histórica y sin embargo un impacto sistémico enorme. El error habitual es confundir **baja probabilidad con baja relevancia**. Las organizaciones tienden a gestionar lo probable, no lo posible, e invierten donde hay recurrencia. Asignan recursos donde hay actividad constante y esto genera vulnerabilidades frente a amenazas emergentes que aún no han demostrado frecuencia suficiente, y, sin embargo, en geopolítica contemporánea, un adversario irracional puede buscar precisamente eso: el punto cuya ruptura genere máxima desestabilización con recursos limitados. La **asimetría estratégica** consiste en producir alto impacto con mínima exposición. En el ámbito de la seguridad, los eventos de alto impacto pueden adoptar muchas formas:

- Ataques terroristas estratégicos.
- Ciberataques contra infraestructuras críticas.
- Uso inesperado de tecnologías emergentes.
- Colapsos estatales rápidos.

- Escaladas militares no previstas.

El 11-S no fue solo un atentado, fue un evento que reconfiguró el paradigma de seguridad occidental, alteró doctrinas, legislación, alianzas y presupuestos. La pregunta de fondo es incómoda: ¿puede un sistema de inteligencia prepararse para algo que por definición ocurre rara vez? La inteligencia anticipatoria cambia el foco, no se centra únicamente en la amenaza concreta, sino en la vulnerabilidad estructural del propio sistema. No preguntas solo “¿quién atacará?”, sino también “¿dónde somos frágiles?”. En Estados altamente interconectados, energía, finanzas, telecomunicaciones, transporte y estabilidad política están entrelazados, esta interdependencia aumenta la eficiencia... y también la fragilidad. Un evento raro puede activar cascadas de efectos secundarios, por eso la anticipación nos exige formular preguntas incómodas:

- ¿Qué pasaría si fallara simultáneamente infraestructuras críticas?
- ¿Qué actor podría beneficiarse de esa ruptura?
- ¿Qué tecnología emergente podría amplificar el impacto?
- ¿Qué narrativa explotaría la crisis resultante?

Estas preguntas no nacen de datos ya consolidados, nacen de imaginación estratégica disciplinada, el desafío también es político, invertir en prevenir algo que quizá nunca ocurra es difícil de justificar, la prevención silenciosa no genera titulares, la reacción en cambio, sí. La **inteligencia anticipatoria** exige aceptar costes presentes para reducir riesgos futuros inciertos, supone asumir que el futuro no será simple prolongación del pasado. Un **sistema optimizado** solo para la frecuente será eficiente, hasta que deje de serlo. Uno que integra lo improbable en su arquitectura mental reduce la magnitud del shock cuando llega la ruptura.

2.3 Estimative Intelligence y prospectiva estratégica

Aquí entramos en un terreno especialmente delicado: cómo emitir juicios cuando la evidencia es incompleta. La literatura contemporánea sobre *estimative intelligence*, como el trabajo coordinado por **Christoph Meyer** en ‘*Estimative Intelligence in European Foreign Policymaking*’, muestra cómo los servicios europeos han integrado:

- Escenarios alternativos
- Evaluación probabilística estructurada
- Análisis de incertidumbre estratégica

La **estimación estratégica** no es predicción determinista, es una gestión rigurosa de la incertidumbre. Mientras la **inteligencia descriptiva** responde a “¿qué sabemos?”, la **inteligencia estimativa** responde a “¿qué es más probable que ocurra dadas las condiciones actuales?”. En la tradición anglosajona, esta disciplina se consolidó durante la Guerra Fría, figuras como Sherman Kent insistían en que la inteligencia debía ofrecer juicios razonados bajo incertidumbre, no certezas imposibles. La estimación implica integrar fuentes heterogéneas, evaluar intenciones además de capacidades y proyectar escenarios plausibles en el tiempo. Y siempre incómoda, porque introduce grados de probabilidad en un entorno político que prefiere afirmaciones tajantes. Si la estimación trabaja con probabilidades, la prospectiva estratégica trabaja con posibilidades. La prospectiva no pregunta solo “¿qué creemos que ocurrirá?”, también amplía el campo de visión, incluye trayectorias de baja probabilidad, pero alto impacto. En seguridad y defensa, hay una distinción clásica entre capacidades e intenciones. Las capacidades son observables, las intenciones se infieren. La *estimate intelligence* ópera precisamente en esa zona gris, no basta con saber que un actor puede lanzar un ciberataque masivo, hay que estimar si tiene voluntad política, incentivos estratégicos y condiciones para hacerlo.

Aquí la anticipación es un ejercicio de interpretación estratégica, no solo de recopilación de datos. En un modelo realmente anticipatorio, estimación y prospectiva se integran:

1. La prospectiva diseña **escenarios** múltiples.
2. La estimación evalúa probabilidades relativas.
3. Se construyen indicadores tempranos para monitorizar cuál escenario empieza a materializarse.
4. Se ajusta el análisis de forma dinámica.

Esto rompe la linealidad del ciclo clásico e introduce adaptación continua, aplicado a ataques híbridos, terrorismo o conflicto interestatal, este enfoque permite **anticipar escaladas antes de que crucen umbrales visibles**, modelar respuestas adversarias y evaluar usos inesperados de tecnologías emergentes, pero todo esto exige una transformación cultural profunda. Requiere analistas capaces de emitir juicios claros bajo presión, organizaciones dispuestas a considerar escenarios incómodos, protección frente a presiones ideológicas, debate estructurado y revisión constante de supuestos. Sin esta base, la

anticipación se convierte en especulación, o peor: en sesgo institucional sofisticado.

En el fondo, la diferencia es clara. El ciclo clásico transforma datos en informes, la *estimative intelligence* **transforma incertidumbre en juicio estratégico**, y la prospectiva estratégica amplía el campo de visión para que la ruptura no resulte totalmente inesperada. La inteligencia anticipatoria no elimina la incertidumbre, sino que la estructura, tampoco nos promete certezas, sino que nos ofrece preparación, y en un entorno marcado por competencia cognitiva, conflicto híbrido y aceleración tecnológica, la diferencia entre reaccionar y estimar -entre describir y prospectar- puede convertirse en la diferencia entre adaptación estratégica y shock sistémico.

III. INTELIGENCIA ANTICIPATORIA COMO INFRAESTRUCTURA GEOPOLÍTICA

Durante mucho tiempo, anticipar fue visto como una habilidad analítica más: algo útil, sofisticado incluso, pero accesorio. Hoy esto ha cambiado, la anticipación ha dejado de ser una técnica para convertirse en algo mucho más profundo: es un elemento de soberanía estratégica, no es un complemento de poder, sino una parte de su infraestructura.

3.1 Gobernanza anticipatoria

El concepto de *anticipatory governance*, desarrollado por **Leon Fuerth**, y adoptado en marcos institucionales como los impulsados por la Comisión Europea, parte de una premisa sencilla pero transformadora: **el futuro no se espera, sino que se trabaja**. No se produce pasivamente, sino que se estructura a través de decisiones presentes informadas por simulaciones y análisis prospectivos. La inteligencia anticipatoria pierde sentido si no modifica la acción política. Un sistema puede detectar señales débiles, modelar escenarios complejos y estimar riesgos emergentes, pero si quienes toman decisiones siguen actuando únicamente cuando la crisis ya es visible, la ventaja desaparece. La **gobernanza anticipatoria** nace precisamente para cerrar esta brecha: integrar la anticipación en el corazón del poder, y así, gobernar de forma anticipatoria no significa adivinar el futuro con precisión milimétrica sino diseñar instituciones capaces de actuar antes de que la crisis sea irreversible. Supone desplazar el eje desde la gestión de crisis hacia la **gestión de vulnerabilidades estructurales**.

Del Estado reactivo al Estado adaptativo

Históricamente, el Estado moderno se ha configurado para responder, ofrecer legislación tras atentados, reformas tras crisis financieras, reestructuraciones tras conflictos, este modelo genera aprendizaje, sí, pero siempre después del daño. La **gobernanza anticipatoria** propone algo distinto: propone incorporar el **análisis prospectivo** en la formulación de políticas antes de que la ruptura ocurra, no se limita al ámbito de la inteligencia nacional, implica:

- Planificación estratégica interministerial, no simbólica
- Evaluación continua de riesgos sistémicos.
- Integración de análisis científico-tecnológico en decisiones regulatorias.
- Simulaciones estratégicas en ámbitos críticos.

El cambio es cultural y estructural. La anticipación deja de ser un informe confidencial y se convierte en parte del proceso político ordinario.

Seguridad nacional y gobernanza anticipatoria

En el ámbito de seguridad y defensa, la gobernanza anticipatoria implica que la inteligencia no se limite a informar amenazas, sino que contribuya a rediseñar **resiliencia estructural**.

Por ejemplo:

- Si se identifican vulnerabilidades críticas en infraestructuras energéticas, la gobernanza anticipatoria no espera un ataque; invierte en redundancia y segmentación.
- Si se modelan escenarios de desinformación masiva, se desarrollan marcos regulatorios y capacidades de alfabetización digital antes de que la campaña alcance su punto álgido.
- Si se detectan trayectorias de radicalización, se activan políticas preventivas coordinadas entre seguridad, educación y servicios sociales.

La anticipación se convierte en política pública transversal.

Anticipación y legitimidad

Pero es aquí donde aparece una tensión inevitable, debiendo actuar antes de que una amenaza sea visible puede generar sospechas, si el riesgo no se materializa, las medidas preventivas pueden parecer exageradas.

La gobernanza anticipatoria exige equilibrio entre:

- Protección preventiva.
- Respeto a libertades de los civiles
- Transparencia institucional.
- Rendición de cuentas.

Demasiada anticipación nos puede derivar en sobre-reacción, muy poca, en vulnerabilidad estructural. La clave no está en reaccionar por impulso, sino en institucionalizar procesos rigurosos que integren **análisis, supervisión y debate democrático**.

Resiliencia como principio central

En este modelo, la seguridad ya no la podemos entender solo como neutralización de amenazas externas, se redefine como resiliencia sistémica. Un Estado que piensa de forma anticipatoria:

- Diversifica cadenas de suministro críticas.
- Protege infraestructuras digitales estratégicas
- Fomenta la cultura estratégica en su élite política.
- Invierte en innovación tecnológica soberana.
- Diseña protocolos de respuesta antes de que el escenario se materialice.

La pregunta ya no es solo “¿quién nos atacará?”, sino “¿qué partes de nuestro sistema colapsarían si algo falla?”, es un desplazamiento del foco: el adversario hacia la arquitectura propia.

Competencia geopolítica y ventaja acumulativa

En entornos de rivalidad estratégica entre potencias, la gobernanza anticipatoria se convierte en una **ventaja estructural**, el actor que integra prospectiva tecnológica en su política industrial, que ajusta doctrinas militares antes de que cambie el equilibrio tecnológico y que coordina inteligencia con planificación económica, obtiene una superioridad acumulativa. La anticipación no es solo defensa, es **posicionamiento**. En la competencia -ya sea tecnológica, económica, informativa- el poder no podemos medirlo únicamente por capacidades actuales, sino por capacidad de adaptación futura.

El riesgo del cortoplacismo político

Uno de los mayores frenos a este modelo que tenemos es el horizonte temporal de la política, los ciclos electorales premian resultados visibles a corto plazo, la anticipación, en cambio, implica invertir hoy para evitar daños que quizá nunca lleguen a ser visibles. Esta tensión genera **vulnerabilidad estratégica**, cuando la planificación estructural se sacrifica en favor de la rentabilidad política inmediata, la reacción suele llegar tarde, la gobernanza anticipatoria requiere algo que no siempre abunda: cultura estratégica a largo plazo.

Romper los silos institucionales

La anticipación también fracasa cuando la información queda compartimentada, las amenazas contemporáneas no respetan las fronteras administrativas, combinan economía, tecnología, información y seguridad. Un modelo eficaz necesita:

- Un intercambio fluido entre inteligencia, defensa, economía y tecnología
- Equipos interdisciplinarios reales
- Simulaciones conjuntas de escenarios
- Actualización constante de hipótesis estratégicas

La fragmentación institucional es enemiga de la anticipación.

3.2 Inteligencia artificial y seguridad

En este contexto, la inteligencia artificial deja de ser una herramienta técnica para convertirse en un multiplicador estratégico, instituciones como el **Instituto Español de Estudios Estratégicos** analiza en el '*Cuaderno de Estrategia 226*' cómo la IA se integra en ámbitos como:

- Detección temprana de amenazas híbridas
- Modelado de crisis geopolíticas
- Anticipación de conflictos multidominio

La ventaja contemporánea no es solo informativa, es temporal, **quién anticipa gana tiempo**, y el tiempo es capacidad que se obtiene para poder adaptarse. La IA permite procesar volúmenes masivos de información en tiempo real e identificar patrones invisibles para que los humanos podamos realizar el análisis, puede generar escenarios contrafactuales, entrenar sistemas frente a amenazas que aún no existen y detectar correlaciones débiles que, combinadas, revelan trayectorias emergentes.

Aplicada correctamente, la anticipación deja de ser exclusivamente humana y pasa a integrarse en la propia arquitectura operativa del Estado, las decisiones pueden apoyarse en simulaciones constantes, actualizadas dinámicamente, pero este avance nos trae riesgos evidentes. La dependencia excesiva de algoritmos puede crear "**cajas negras**" difíciles de poder ser auditadas. La automatización en contextos de alta tensión puede provocar escaladas no deseadas si no existe la supervisión humana de manera rigurosa. La velocidad que ofrece la **IA** puede convertirse en precipitación si no está bien acompañada de **un juicio estratégico**.

En sistemas de seguridad, la IA permite:

- **Procesar grandes volúmenes de información** en tiempo real, identificando patrones invisibles para el análisis humano.
- **Generar datos sintéticos y escenarios contrafactuales**, entrenando sistemas de defensa frente a amenazas que aún no existen en el mundo real.
- **Detección temprana de amenazas híbridas**, como ciberataques coordinados, campañas de desinformación o movimientos estratégicos encubiertos, mediante algoritmos de inferencia sobre señales débiles.

En última instancia, la inteligencia artificial no sustituye la deliberación política ni el análisis humano, sino que los suplementa. Su valor no reside únicamente en predecir, sino en integrar esas predicciones dentro de políticas resilientes, coordinadas y supervisadas. La **ventaja estratégica** no está solo en saber antes, está en transformar ese conocimiento que tenemos de manera temprana en decisiones estructurales coherentes.

Ahí es donde la inteligencia anticipatoria deja de ser un ejercicio analítico y se convierte en infraestructura geopolítica real: cuando la capacidad de imaginar escenarios, modelar rupturas y adaptarse antes que otros pasa a formar parte del diseño mismo del Estado.

IV. EL PROBLEMA CENTRAL: PREDECIR SIN DATOS

Aquí se encuentra la tensión más incómoda de toda la inteligencia anticipatoria, la pregunta que tarde o temprano, aparece en cualquier discusión seria: “¿Cómo anticipar fenómenos que aún no han dejado rastro empírico?”. A primera vista, parece una contradicción, pero precisamente ahí se juega el núcleo epistemológico de este enfoque.

4.1 Modelización formal

Cuando no hay datos suficientes, la respuesta intuitiva suele ser “esperemos a tener más datos”, la **inteligencia anticipatoria** plantea lo contrario: si esperamos a que haya datos sólidos, quizá ya sea demasiado tarde. La solución moderna no consiste en qué acumulemos más historia, sino en que construyamos modelos formales que representen la lógica interna de los sistemas antes de que las señales visibles aparezcan. Modelizar es, en el fondo, darle estructura a la incertidumbre, ya sea a través de matemáticas, teoría de sistemas, simulaciones computacionales y algoritmos, ahí es donde se crean representaciones de economías, redes eléctricas, infraestructuras digitales, dinámicas sociales o equilibrios militares. Estos modelos no prometen un único resultado, generan trayectorias posibles, nos permiten explorar cómo un sistema podría evolucionar ante diferentes perturbaciones. No predicen “lo que ocurrirá”, exploran “lo que podría ocurrir”.

Modelos generativos y gemelos digitales

Una de las aplicaciones más potentes son los **gemelos digitales**, que son representaciones virtuales de sistemas reales que pueden ser manipuladas bajo variables hipotéticas. Esto permite:

- Evaluar cómo una infraestructura crítica respondería ante un ciberataque que aún no ha ocurrido.
- Probar la efectividad de políticas públicas antes de implementarlas.
- Simular movimientos estratégicos de adversarios en entornos geopolíticos inciertos.

Los gemelos digitales nos permiten observar consecuencias emergentes en un entorno controlado, antes de que el fenómeno exista en la realidad, lo que sería una hipótesis abstracta, se convierte en un escenario operativamente analizable, no elimina la incertidumbre, la convierte en algo explorado.

Inferencia sobre patrones débiles

La modelización formal también nos permite extraer conocimiento de señales que son apenas perceptibles. En lugar de esperar que la amenaza sea evidente, los modelos pueden integrar **patrones débiles** –comportamientos marginales, pequeñas anomalías en sistemas complejos, cambios iniciales en narrativas digitales– y proyectar cómo estas pequeñas perturbaciones podrían amplificarse. Este enfoque es crucial frente a **eventos de baja frecuencia y alto impacto**, donde los datos históricos son insuficientes para que se puedan extrapolar probabilidades. La modelización formal nos permite convertir la incertidumbre radical en escenarios estructurales plausibles.

Modelos contrafactuales y el pensamiento lateral

Predecir sin datos requiere, además, algo menos técnico, pero igual de importante: **pensamiento contrafactual**: es decir, explorar “lo que podría haber ocurrido” bajo condiciones alternativas. Esto nos permite:

- Identificar vulnerabilidades que no han sido explotadas aún.
- Entrenar sistemas de defensa frente a ciberataques, fallos tecnológicos o rupturas sociales que no tienen precedentes.
- Romper sesgos de confirmación derivados de experiencias pasadas.

El pensamiento lateral y contrafactual nos permite ampliar el horizonte estratégico, permitiendo que los analistas puedan **anticipar escenarios “imposibles pero plausibles”** antes de que produzcan evidencia empírica.

Construcción de datos sintéticos

Cuando los eventos aún no existen, los modelos pueden **generar datos sintéticos** que simulan comportamientos posibles. Por ejemplo, se pueden simular técnicas de un **ataque cibernético** que no se han ejecutado todavía, entrenar sistemas defensivos y protocolos preventivos frente a ellos. Esto permite que la IA y los sistemas de análisis anticipatorio trabajen sobre situaciones que, de otro modo, permanecerían invisibles hasta que la amenaza se materialice -es una manera de entrenarse para lo inédito-.

El verdadero valor estratégico

El verdadero poder de la modelización formal no reside en que podamos predecir el futuro con certeza, sino en **dar tiempo y margen de maniobra**. Permite que las decisiones estratégicas no estén condicionadas únicamente por lo que ya existe, sino que se basen en una comprensión estructural de lo que podría surgir. En contextos geopolíticos y de seguridad, esto se traduce en:

- Capacidad de diseñar defensas antes de que la amenaza aparezca.
- Anticipación de movimientos adversarios y preparación de contramedidas.
- Reducción del shock estratégico frente a rupturas sistémicas.

4.2 Señales débiles y escenarios sintéticos

Si la modelización es la estructura, las señales débiles son la materia prima más delicada que tenemos. El concepto de *weak signals*, introducido por **Igor Ansoff**, parte de una idea sencilla: explica que los cambios estructurales aparecen primero no como grandes cambios sino como **anomalías periféricas**. La anticipación requiere:

- Capacidad de detección periférica
- Tolerancia a ambigüedad
- Análisis multi-nivel

Las señales débiles no son pruebas concluyentes, son indicios. Pequeñas desviaciones, comportamientos marginales, variaciones incipientes... en la inteligencia anticipatoria, no debemos esperar a que se conviertan en datos

robustos, se deben interpretar como marcadores temprano de posible transformación.

La inferencia como núcleo del análisis

Inferir significa que debemos **extraer conocimiento a partir de lo aparentemente insignificante**, es decir, trabajar con señales débiles, para la seguridad y la geopolítica, esto implica que debemos:

- Detectar movimientos sutiles en redes sociales que podrían preceder campañas de radicalización o desinformación.
- Observar pequeñas alteraciones en flujos financieros o tecnológicos que anticipan cambios estratégicos.
- Identificar ajustes doctrinales o procedimentales que podrían transformar capacidades militares o cibernéticas.

En todos estos casos, la señal es débil, y no prueban nada, pero su integración en un marco analítico formal permite construir hipótesis robustas.

Escenarios sintéticos: probando lo imposible

El siguiente paso es **generar escenarios sintéticos** a partir de estas señales anteriores que tenemos, simulaciones de eventos que aún no han ocurrido, construidas combinando modelos formales e inferencias preliminares. Esto no puede permitir:

- Entrenar sistemas defensivos y protocolos de respuesta frente a amenazas inéditas.
- Evaluar cómo interacciones complejas entre actores podrían generar cascadas de consecuencias no lineales.
- Explorar lo improbable: ataques combinados, rupturas institucionales, fallos tecnológicos críticos.

Al unir las señales débiles con escenarios sintéticos, la inteligencia anticipatoria convierte la incertidumbre en **información procesable**, aunque el fenómeno aún no exista en el mundo real.

La integración dinámica

Lo esencial no es producir un informe aislado, sino mantener un **ciclo dinámico**:

1. Las señales débiles detectadas alimentan los modelos formales.
2. Los modelos generan escenarios sintéticos y predicciones de posibles impactos.
3. Las observaciones refinan las hipótesis, mejorando la precisión de futuros modelos.

Este proceso nos permite que la anticipación sea **adaptativa y evolutiva**, reduciendo la sorpresa estratégica frente a eventos de baja frecuencia y alto impacto.

Aplicaciones en seguridad y geopolítica

En entornos de competencia estratégica, la combinación de señales débiles y escenarios sintéticos ofrece ventajas claras y decisivas:

- **Ciberseguridad:** nos permite detectar patrones incipientes de ataques y entrenar defensas antes de que se materialicen.
- **Conflicto híbrido:** podemos anticipar campañas de desinformación o movimientos encubiertos de actores estatales y no estatales.
- **Gestión de crisis:** tenemos la capacidad de evaluar impactos potenciales de rupturas económicas o políticas antes de que se conviertan en crisis abiertas.

La capacidad de actuar sobre información **que aún no es observable** nos transforma la anticipación en un activo estratégico tangible.

Riesgos y precauciones

Pero este terreno es delicado, trabajar con señales débiles y escenarios sintéticos no está exento de peligros e implica riesgos:

- Existe riesgo de **sobreinterpretación**, donde los patrones marginales se toman como amenazas reales.

- La dependencia excesiva de modelos automatizados nos puede generar **profecías autocumplidas**, si la acción basada en predicciones provoca que el evento ocurra.
- Se requiere siempre una supervisión humana rigurosa y validación constante de supuestos para que podamos evitar decisiones estratégicas erróneas.

El **equilibrio entre sensibilidad y prudencia es esencial**, anticipar no es ver fantasmas, ni tampoco es ignorar lo incipiente. El problema central sigue siendo el mismo: cómo podemos pensar con rigor sobre lo que aún no existe. La inteligencia anticipatoria no nos resuelve completamente esta tensión, pero nos ofrece herramientas para habilitarla sin paralizarse, y en un entorno donde las rupturas pueden surgir sin precedentes claros, esta capacidad, -imperfecta, pero estructurada- puede marcarnos la diferencia entre sorpresa traumática y adaptación estratégica.

V. EL LADO OSCURO: RIESGOS ESTRATÉGICOS DE LA ANTICIPACIÓN

Si anticipar es poder, también es responsabilidad, y cuanto mayor es la capacidad que tenemos de prever, mayor es el riesgo de equivocarnos... o de provocar aquello que se quería evitar.

La inteligencia anticipatoria nos amplía el margen de maniobra estratégica, si, pero también abre un terreno delicado donde la velocidad, la automatización y la confianza excesiva en modelos pueden convertirse en vulnerabilidades, el problema no es entonces anticipar, el problema es qué hacemos con esta anticipación.

5.1 Automatización decisional

En '*Superinteligencia*', **Nick Bostrom** advierte sobre los riesgos de delegar decisiones críticas en sistemas cuya lógica interna no comprendemos del todo. Esa advertencia, que en apariencia puede sonarnos futurista, es ya profundamente actual. La automatización decisional representa la frontera más delicada de la inteligencia anticipatoria. Hasta ahora, hemos visto cómo los sistemas formales, la inferencia de señales débiles y los escenarios sintéticos permiten predecir lo que aún no existe, pero convertir estas predicciones en acción inmediata nos plantea un riesgo crítico: **delegar decisiones estratégicas a algoritmos y sistemas autónomos**.

En esencia, automatizar decisiones significa transferir parte del juicio humano a máquinas que procesan información, identifican patrones y, en algunos casos,

recomiendan o ejecutan acciones sin una supervisión directa. En entornos de seguridad y geopolítica, esto tiene implicaciones profundas.

Ventajas aparentes

Los sistemas automatizados ofrecen beneficios claros:

- **Velocidad de reacción:** los algoritmos pueden procesar señales y activar protocolos de defensa o contingencia mucho más rápido que cualquier cadena de comando humana.
- **Manejo de complejidad masiva:** la IA nos puede integrar cientos de variables simultáneamente, evaluando escenarios que serían imposibles de considerar manualmente.
- **Reducción de errores humanos en la interpretación de datos:** los sesgos cognitivos y la fatiga afectan menos a los sistemas computacionales bien entrenados.

Desde el punto de vista operacional, parece una ventaja indiscutible, en entornos donde los ciberataques, las campañas híbridas o los movimientos financieros estratégicos ocurren a gran velocidad, reaccionar tarde puede equivaler a perder, pero esa misma velocidad es el origen del riesgo.

Riesgos estratégicos

Sin embargo, el lado oscuro es inmediato y nos introduce vulnerabilidades que no son teóricas, sino estructurales:

1. Caja negra algorítmica:

Los modelos predictivos nos pueden producir recomendaciones difíciles de interpretar o explicar. Los decisores humanos podríamos ejecutar acciones críticas sin comprender completamente las premisas del algoritmo, es aquí donde el margen de error se vuelve inquietante.

2. Profecías autocumplidas:

Si una IA predice una amenaza y actúa en consecuencia, la acción misma puede provocar la materialización del escenario anticipado. Por ejemplo, un despliegue militar preventivo basado en predicciones podría escalar una tensión que inicialmente era solo un riesgo potencial.

3. Errores en escenarios de baja frecuencia:

Precisamente donde más queremos anticipar -eventos de baja frecuencia y alto impacto- es donde los modelos son más inciertos, automatizar respuestas en este terreno puede amplificar un error en lugar de contenerlo.

4. Dependencia tecnológica:

La confianza excesiva en sistemas automatizados puede erosionar nuestra capacidad humana de juicio, reduciendo la resiliencia ante fallos inesperados o adversarios que manipulen la información de entrada.

En otras palabras, la paradoja es clara: lo que ofrece ventaja operativa puede convertirse en fragilidad estructural si no se gestiona con cuidado.

Rapidez versus prudencia

Aquí aparece la tensión difícil de resolver. Para que la **anticipación automatizada** sea eficaz, necesita rapidez y cierto grado de autonomía, pero para que sea segura, necesita la supervisión humana, validación constante y capacidad de intervención. En decisiones militares, de ciberdefensa o de intervención geopolítica preventiva, un error puede ser irreversible, el equilibrio entre velocidad y prudencia no es técnico, es profundamente estratégico.

Estrategias de mitigación

No se trata de rechazar la automatización, sino de encuadrarla. Para reducir riesgos sin renunciar a la anticipación automatizada, se proponen varias prácticas:

- **Human-in-the-loop:** que todas las decisiones críticas siempre sean revisadas por expertos antes de ejecución.
- **Redundancia de modelos:** que se comparen salidas de diferentes algoritmos antes de actuar.
- **Simulación previa de escenarios de fallo:** evaluar cómo el sistema reaccionaría ante predicciones erróneas.
- **Transparencia y trazabilidad:** asegurarnos de que cada recomendación automatizada pueda ser auditada y explicada.

Estas medidas no eliminan el riesgo, pero lo hacen gestionable, preservando y evitando que la anticipación se convierta en un automatismo ciego.

5.2 Profecías autocumplidas

El fenómeno descrito por el sociólogo **Robert K. Merton** tiene aplicación directa en **seguridad internacional**, describió hace décadas el fenómeno de la profecía autocumplida: una creencia que, al ser asumida como verdadera, provoca comportamientos que terminan haciéndola realidad. Es decir, si una simulación anticipa un ataque y se responde preventivamente, puede activarse la escalada que el modelo solo estimaba como posibilidad. La anticipación mal calibrada puede generar justo el conflicto que se intentaba prevenir.

Cómo se generan las profecías autocumplidas

El proceso suele ser sutil y desarrollarse de forma gradual:

1. Un sistema anticipatorio detecta señales débiles o proyecta un escenario de riesgo.
2. Los decisores basándose en esa predicción, adoptan medidas preventivas: despliegues militares, sanciones económicas, operaciones cibernéticas o políticas defensivas agresivas.
3. Las acciones tomadas son percibidas por el adversario como amenaza real.
4. El adversario responde.
5. El escenario inicialmente hipotético empieza a materializarse.

El resultado: **la predicción no sólo anticipa el futuro, sino que lo produce**, y lo más peligroso es que, cuando el escenario se cumple, refuerza la confianza en el modelo que lo proyectó, cerrando un círculo difícil de cuestionar. Lo que inicialmente era un riesgo teórico se convierte en amenaza real, reforzando la percepción de la inteligencia y cerrando un bucle de retroalimentación que puede ser difícil de detener.

Ejemplos estratégicos

- En conflictos internacionales, un movimiento preventivo basado en inteligencia anticipatoria puede ser percibido como amenaza, provocando que el adversario responda agresivamente.
- En ciberseguridad, la preparación frente a un ataque simulado puede provocar escaladas de tensión en redes compartidas, creando vulnerabilidades que antes no existían.
- En operaciones preventivas contra actores no estatales, la intervención anticipada puede consolidar la resistencia o radicalización, transformando una amenaza potencial en una crisis abierta.

Estos ejemplos nos muestran cómo la anticipación puede **crear la realidad que se intenta evitar** si no se gestiona con cuidado.

Riesgo de escalada sistémica

La combinación de inteligencia anticipatoria con automatización decisional intensifica la probabilidad de escaladas inesperadas. Cuando las decisiones preventivas se toman rápidamente, basadas en modelos que nadie comprende completamente, el margen de error aumenta:

- **Errores de interpretación:** señales débiles pueden ser sobrevaloradas.
- **Reacciones adversarias no previstas:** la acción defensiva puede desencadenar respuestas desproporcionadas.
- **Efecto cascada:** en sistemas interconectados, una reacción local puede propagarse y generar crisis regionales o globales.

En entornos híbridos y altamente tecnológicos, incluso pequeñas decisiones pueden desencadenar conflictos mayores, convirtiendo la anticipación en un arma de doble filo.

Estrategias para mitigar el riesgo

Para evitar que la predicción se convierta en una causa de crisis, es necesario que:

- **Integremos el juicio humano en todas las decisiones críticas,** evaluando impactos colaterales antes de actuar.

- **Simulemos efectos de retroalimentación:** evaluemos cómo las acciones preventivas podrían modificar el comportamiento del adversario.
- **Establezcamos protocolos de escalada controlada,** limitando la magnitud de las intervenciones automáticas.
- **Revisemos y actualicemos continuamente modelos predictivos,** reconociendo que todo modelo es simplificación y puede inducir sesgos.

La anticipación no debe eliminar la incertidumbre, sino **gestionarla con prudencia y responsabilidad.**

CONCLUSIÓN

Al terminar de explorar la inteligencia anticipatoria, podemos darnos cuenta de que lo fascinante no es solo la tecnología ni los algoritmos, sino **lo que nos dice sobre nosotros mismos.** Porque anticipar el futuro antes de que existan los datos no es un juego de números: es un acto profundamente humano. Es un ejercicio de curiosidad, de humildad y, al mismo tiempo, de coraje. Humildad, porque por muy sofisticados que sean los modelos o complejas las simulaciones, **nunca podremos controlar todo,** siempre habrá sorpresas, errores, señales que pasamos por alto. La anticipación nos obliga a aceptar que la certeza absoluta no existe, que incluso la mejor preparación puede fallar. Aprender a vivir con eso y, aun así, tomar decisiones, es un desafío que pone a prueba nuestro juicio y nuestra responsabilidad.

Coraje, porque actuar sobre lo que todavía no ha sucedido significa **arriesgarse a equivocarse.** Significa pensar en escenarios improbables, en amenazas que otros ni siquiera imaginan, y tener la fuerza para proponer acciones antes de que alguien más vea el peligro. No es cómodo, no es fácil, y muchas veces el mundo no reconocerá el valor de haber prevenido una crisis que nunca llegó a suceder. La inteligencia anticipatoria nos da **tiempo,** un recurso que suele ser el más escaso en cualquier decisión estratégica. Nos permite preparar, reflexionar y actuar con visión, en lugar de simplemente reaccionar cuando ya es demasiado tarde. Nos recuerda que la ventaja no está solo en la información que tenemos, sino en nuestra capacidad de pensar, de imaginar y de organizar nuestro conocimiento para navegar la incertidumbre. Al final, debemos pensar que lo más importante no son los modelos ni los algoritmos: **somos nosotros,** las personas detrás de la decisión. La inteligencia anticipatoria solo tiene valor si se combina con juicio, ética y conciencia de las consecuencias, no basta con ver lo que puede ocurrir; hay que preguntarse **qué queremos que ocurra y cómo nuestras acciones pueden cambiar el futuro.**

En definitiva, la anticipación estratégica es un acto de responsabilidad y de humanidad. Nos invita a ser arquitectos del mañana, a tomar decisiones difíciles con cuidado, y a entender que la verdadera ventaja no es predecir, sino **preparar con sensatez, actuar con claridad y asumir con humildad nuestra capacidad de influir en el mundo que aún no existe.**

Bibliografía

Allison, G. (2017). *Destined for war: Can America and China escape Thucydides's trap?* Houghton Mifflin Harcourt.

<https://books.apple.com/es/book/destined-for-war/id1246064150>

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.

European Commission. (2020). *Strategic foresight report 2020: Charting the course towards a more resilient Europe*. Publications Office of the European Union.

https://commission.europa.eu/system/files/2020-09/comm-rtd-corporate-2020-strategic-foresight-report_en.pdf

European Commission. (2021). *Strategic foresight report 2021: The EU's capacity and freedom to act*. Publications Office of the European Union.

https://commission.europa.eu/system/files/2021-11/strategic-foresight-report-2021_en.pdf

Fuerth, L. S., & Faber, E. M. H. (2012). *Anticipatory governance: Practical upgrades: Equipping the executive branch to cope with increasing speed and complexity of major challenges*. George Washington University.

<https://gwpapers.unc.edu/gwp119/>

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge University Press.

Kent, S. (1966). *Strategic intelligence for American world policy* (Rev. ed.). Princeton University Press.

Knight, F. H. (1921). *Risk, uncertainty, and profit*. Houghton Mifflin.

LISA Institute. (2023–2026). *Artículos de análisis sobre inteligencia estratégica y prospectiva*. LISA News.

https://www.lisanews.org/etiqueta/inteligencia-estrategica/?utm_source

LISA Institute. (2025, April 16). *Masterclass: Inteligencia estratégica al servicio de la prospectiva y la anticipación* [Video]. YouTube.

<https://www.youtube.com/watch?v=H5OEapw4cul>

LISA Institute. *De las crisis complejas a las soluciones estratégicas: Cómo aplicar la prospectiva en entornos de incertidumbre*. YouTube.
<https://www.youtube.com/watch?v=AK5AI16slgA>

LISA Institute. *Congreso LISA 2025: Innovación en inteligencia, ciberseguridad y prospectiva estratégica*. LISA News.
<https://www.lisanews.org/lisa-institute/congreso-lisa-institute-2025-innovacion-en-inteligencia-ciberseguridad-y-prospectiva-estrategica/?utm>

Lowenthal, M. M. (2017). *Intelligence: From secrets to policy*

National Intelligence Council. *Global Trends 2040: A more contested world*. Office of the Director of National Intelligence.
https://www.dni.gov/files/documents/GlobalTrends_2040.pdf

NATO Allied Command Transformation. (2023). *Strategic foresight analysis 2023*. NATO.
https://www.act.nato.int/images/stories/media/doclibrary/ACT_Strategic_Foresight_Analysis_2023.pdf

Perez-Ortiz, M. (2025). *From prediction to foresight: The role of AI in designing responsible futures*
<https://arxiv.org/abs/2511.21570>

Rosen, R. (1985). *Anticipatory systems: Philosophical, mathematical, and methodological foundations*.

Sardar, Z. (2010). Welcome to postnormal times.
<https://doi.org/10.1016/j.futures.2009.11.028>

Serra del Pino, J. (2019). *Manual de prospectiva y decisión estratégica*. Ariel.

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*.

Taleb, N. N. (2012). *Antifragile: Things that gain from disorder*.

Tetlock, P. E., & Gardner, D. (2015). *Superforecasting: The art and science of prediction*.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases.
<https://doi.org/10.1126/science.185.4157.1124>

United Nations Office for Disarmament Affairs. (2019). *The impact of autonomous weapons systems on international peace and security*. United Nations.

https://documents.unoda.org/wp-content/uploads/2019/06/AWS_report.pdf