Revista del Instituto Español de Estudios Estratégicos
ISSN-e: 2255-3479

Antonio Legaz
Analista de ciberdefensa

Correo: alegazs@indra.es

¿El fin de la sorpresa? Un estudio sobre la mutación del elemento sorpresa en el siglo de la (des)información

The end of surprise? A study on the mutation of the element of surprise in the century of (dis)information

Resumen

La revolución en la recolección y análisis de información ha transformado el papel de la sorpresa en la guerra moderna. Las tecnologías de vigilancia, el análisis de *big data* y la inteligencia artificial han reducido drásticamente la incertidumbre estratégica, limitando la capacidad de los actores para ejecutar ataques sorpresa. Sin embargo, este aparente fin de la sorpresa se enfrenta a un desafío creciente: la desinformación. La proliferación de información falsa, la manipulación de datos y el envenenamiento informativo han generado un nuevo tipo de «niebla de guerra digital», en la que la sobrecarga de información y el ruido estratégico pueden generar falsas certezas. Este trabajo explora cómo la sorpresa se ha transformado en la era de la información y cómo la lucha entre la transparencia y el engaño sigue definiendo el campo de batalla moderno. Finalmente, se analiza el papel del análisis de inteligencia en la conversión de datos en conocimiento útil, subrayando la importancia de distinguir entre información veraz y manipulación estratégica para evitar vulnerabilidades críticas.

Palabras clave

Sorpresa, Desinformación, Incertidumbre, Sesgos cognitivos.

Abstract

The revolution in intelligence gathering and analysis has transformed the role of surprise in modern warfare. Surveillance technologies, big data analytics and artificial intelligence have drastically reduced strategic uncertainty, limiting the ability of actors to execute surprise attacks. However, this apparent end of surprise faces a growing challenge: disinformation. The proliferation of false information, data manipulation and information poisoning has generated a new kind of digital fog of war, in which information overload and strategic noise can generate false certainties. This paper explores how surprise has been transformed in the information age and how the struggle between transparency and deception continues to define the modern battlefield. Finally, it discusses the role of intelligence analysis in turning data into useful knowledge, highlighting the importance of distinguishing between truthful information and strategic manipulation in order to avoid critical vulnerabilities.

Keywords

Surprise, Disinformation, Uncertainty, Cognitive biases.

Citar este artículo:

Legaz, Antonio (2025). «¿El fin de la sorpresa? Un estudio sobre la mutación del elemento sorpresa en el siglo de la (des)información». Revista del Instituto Español de Estudios Estratégicos, n.º 25, pp. 43-64.

1 El elemento sorpresa y su importancia histórica

1.1 Introducción a la sorpresa

¿Qué tienen en común el ataque japonés a Pearl Harbor en 1941, la invasión alemana de la Unión Soviética en 1941 (operación Barbarroja), la invasión de Noruega en 1940 y el ataque egipcio y sirio a Israel en 1973 (Guerra de Yom Kippur)? Todas estas operaciones clave del siglo xx fueron posibles gracias a un factor determinante: la sorpresa.

En el intrincado tapiz de la estrategia militar, la sorpresa ha sido un principio esencial en la estrategia militar, un recurso que puede alterar drásticamente el equilibrio de poder en un conflicto. La sorpresa no solo afecta a la táctica y la estrategia, sino que también influye en la psicología del adversario, generando desorientación y caos (Betts, 1982: 87-105). Su efectividad radica en la capacidad de desarticular los planes del enemigo, sembrar la incertidumbre y explotar la ventaja táctica con una fuerza que, en otras circunstancias, podría parecer insuficiente. No se trata únicamente de atacar sin previo aviso, sino de manipular la percepción del adversario para reducir su capacidad de respuesta.

La sorpresa, en su esencia más pura, busca generar una asimetría en la posición del oponente, desarticulando sus planes y sembrando la confusión y el desaliento en sus filas. Este efecto desestabilizador no solo se traduce en una ventaja táctica, sino que también amplifica el impacto de las acciones militares, permitiendo a una fuerza menos numerosa superar a otra de mayor envergadura. Por esta razón, la sorpresa ha sido considerada el medio idóneo para alcanzar una superioridad numérica relativa en el punto de decisión, incluso en ausencia de una superioridad absoluta.

A lo largo de la historia, comandantes y estrategas han recurrido a la sorpresa para compensar inferioridades numéricas o tecnológicas. La sorpresa no se limita a la mera ocultación de intenciones, sino que también se puede lograr mediante la velocidad, la flexibilidad y la audacia en la ejecución (Handel, 1984: 220-281). Federico el Grande, por ejemplo, basó su campaña de 1760 en maniobras inesperadas que desestabilizaron al ejército austriaco, demostrando que la sorpresa no solo es un acto de sigilo, sino también de innovación estratégica.

La consecución de la sorpresa, lejos de ser un acto fortuito, exige una conjunción de factores que incluyen el secreto en la preparación, la celeridad en la ejecución y la determinación tanto del Gobierno como del general al mando (Clausewitz, 1832: 198-204). Sin embargo, a pesar de su importancia, el éxito en la concreción de la sorpresa nunca está garantizado y, en múltiples ocasiones, la fricción inherente a la guerra obstaculiza su materialización. A pesar de los desafíos que plantea, el principio de la sorpresa se mantiene como un pilar fundamental de la estrategia, influyendo en la toma de decisiones y en la conducción de las operaciones militares a lo largo de la historia.

Es fundamental señalar que la sorpresa no se limita a las acciones ofensivas, sino que también es un recurso valioso en la defensa. La capacidad de anticipar los movimientos del enemigo y preparar las defensas de forma inesperada puede conferir una ventaja

significativa. Por ejemplo, la resistencia española contra Napoleón demostró que la sorpresa también podía surgir de la movilización y la determinación que, mediante la guerra de guerrillas, ataques imprevistos y una tenaz resistencia, logró desestabilizar al ejército invasor.

1.2 Taxonomía de la sorpresa

El estudio sistemático de la sorpresa estratégica exige trascender la tradicional dicotomía entre éxito y fracaso mediante una categorización funcional que permita un análisis estructurado del fenómeno. Siguiendo una aproximación taxonómica, es posible identificar cuatro modalidades principales: las «sorpresas de capacidad», manifestadas cuando el adversario despliega tecnologías o métodos desconocidos, como evidenciaron los submarinos clase Typhoon soviéticos, cuyas propiedades sigilosas comprometieron severamente los sistemas de detección occidentales (Paredes y Oliveira, 2023: 4-6). Las «sorpresas de intención», ejemplificadas paradigmáticamente por el ataque a Pearl Harbor, donde pese al conocimiento de las capacidades japonesas, se malinterpretaron sus objetivos estratégicos. Las «sorpresas de ejecución», ilustradas por la operación Barbarroja, donde el factor sorpresivo no residió en el qué sino en el cómo de la implementación táctica. Finalmente, existen las «sorpresas de temporalidad», caracterizadas por la materialización inesperada de amenazas anticipadas, como ocurrió con la ofensiva del Tet durante la guerra de Vietnam.

Esta taxonomía, lejos de constituir un mero ejercicio académico, posibilita el desarrollo de estrategias preventivas específicas de anticipación diferenciada (Zwitter, 2015: 9-11). Así, para contrarrestar las sorpresas de capacidad resulta imperativa la inversión sostenida en inteligencia tecnológica y contrainteligencia. Frente a las sorpresas de intención se requiere un riguroso análisis psicológico y contextual, implementando técnicas de perfilado a los actores hostiles como las propuestas por Borum[1] (2004: 22-25). Ante las sorpresas de ejecución deviene esencial la simulación y modelado de escenarios no convencionales. Finalmente, para las sorpresas de temporalidad se precisan sistemas de alerta temprana fundamentados en la detección e interpretación de indicadores y señales débiles.

La evolución histórica de la sorpresa estratégica, desde el clásico caballo de Troya hasta las amenazas híbridas contemporáneas, revela patrones reconocibles a través de la lente de esta categorización, permitiendo establecer paralelismos y extraer lecciones aplicables al entorno actual. No obstante, la naturaleza cambiante del conflicto exige una continua revisión y actualización de esta taxonomía, evitando el riesgo de prepararse exclusivamente para modalidades de sorpresa ya experimentadas. El reconocimiento de estas categorías

1 Borum propone un marco de análisis multifactorial para la comprensión de las motivaciones de actores hostiles que integra cuatro dimensiones: la evaluación del contexto ideológico-doctrinal, el análisis de procesos de radicalización, el estudio de factores situacionales precipitantes y la identificación de indicadores conductuales predictivos. Su metodología «Cuatro Vías hacia la Radicalización» (*Four-Stage Pathway to Terrorism*) permite descomponer secuencialmente el proceso decisional que conduce a la acción hostil.

no solo facilita el análisis retrospectivo, sino que, crucialmente, orienta el desarrollo de capacidades defensivas adaptativas frente a un fenómeno que, a pesar de su longevidad, continúa representando uno de los más formidables desafíos para la seguridad estratégica contemporánea.

Esta aproximación multidimensional a la sorpresa estratégica constituye un avance significativo respecto a los modelos explicativos tradicionales, excesivamente centrados en fallos de inteligencia o sesgos cognitivos individuales. La taxonomía propuesta integra factores tecnológicos, psicológicos, operacionales y temporales, ofreciendo un marco analítico comprensivo que trasciende las limitaciones de los enfoques monolíticos previos.

1.3 La sorpresa en el siglo XXI

Desde Clausewitz (1832) hasta Van Creveld (1991), la guerra ha sido descrita como un fenómeno dominado por la incertidumbre. El concepto de la «niebla de la guerra», término acuñado por Clausewitz, alude a la dificultad de obtener información clara y precisa en el campo de batalla. A lo largo de la historia, esta niebla ha sido un aliado de la sorpresa: el caos, la desinformación y la fricción han permitido a los estrategas explotar lagunas en la percepción del enemigo. Sin embargo, en el siglo XXI, la proliferación de tecnologías de vigilancia parece estar disipando esa niebla, reduciendo el margen para la sorpresa.

La revolución en inteligencia militar ha estado marcada por el desarrollo de tecnologías como los satélites de observación, el análisis masivo de datos y la inteligencia artificial aplicada a la detección de patrones (Allen y Chan, 2017: 45-62). En la Guerra Fría, el lanzamiento del CORONA, el primer programa de satélites de vigilancia de Estados Unidos ya permitía monitorear con precisión la actividad militar soviética, dificultando la posibilidad de ataques sorpresa a gran escala (Perry y Carter, 1999: 114-120). Hoy, la capacidad de vigilancia es exponencialmente mayor: en 2022, más de 10 000 satélites orbitaban la Tierra, muchos de ellos equipados con sensores de alta resolución, tecnología SAR (*Synthetic Aperture Radar*) e inteligencia artificial para el análisis en tiempo real de imágenes geoespaciales (Weeden y Samson, 2022: 32-47).

Este acceso sin precedentes a información detallada afecta directamente la dinámica del conflicto moderno. Por ejemplo, durante la guerra en Ucrania, la inteligencia occidental detectó con meses de antelación los preparativos rusos para la invasión de 2022. Informes de inteligencia basados en imágenes satelitales y datos de tráfico de telecomunicaciones permitieron anticipar los movimientos del ejército ruso, lo que llevó a Ucrania y sus aliados a prepararse mejor para la ofensiva (Freedman, 2022: 178-196).

A esta vigilancia satelital se suma el impacto del Big Data en la predicción de escenarios bélicos. Los algoritmos de aprendizaje automático analizan patrones en redes sociales, transacciones económicas y movimientos logísticos para prever acciones militares antes de que ocurran (Taddeo y Floridi, 2018: 723-735). Este tipo de inteligencia predictiva se utilizó, por ejemplo, en la lucha contra el Estado Islámico en Siria e Irak, donde los ataques de drones estadounidenses fueron guiados por análisis de datos que revelaban patrones de comportamiento de los combatientes (Schmidt, 2020: 56-73).

La cuestión clave es: ¿sigue siendo posible la sorpresa en la era de la vigilancia total y el análisis masivo de datos? La historia nos demuestra que, aunque las herramientas de inteligencia evolucionan, la sorpresa sigue siendo un factor de peso. La pregunta, por tanto, no es si la sorpresa ha desaparecido, sino cómo se ha transformado para adaptarse a un nuevo campo de batalla.

1.4 Objetivos

El presente trabajo se propone analizar, desde una perspectiva multidisciplinar que integra estudios de seguridad, comunicación estratégica y psicología cognitiva, la transformación del elemento sorpresa como factor decisivo en los enfrentamientos contemporáneos. Para ello, se plantean cinco interrogantes fundamentales cuyas respuestas permitirán comprender la evolución, estado actual y proyección futura de este fenómeno:

1. ¿Cómo ha mutado el elemento sorpresa en los conflictos modernos frente a la proliferación de tecnologías de vigilancia y recolección masiva de datos?
2. ¿En qué medida las herramientas tecnológicas como los satélites, el *big data* y el perfilado psicológico han modificado la capacidad de los actores estatales para ejecutar o prevenir ataques sorpresa?
3. ¿Qué papel juega la desinformación como contrapeso a la transparencia informativa y como nuevo vector para generar sorpresa estratégica?
4. ¿Por qué siguen produciéndose fallos de anticipación a pesar de contar con sistemas avanzados de vigilancia y análisis de información?
5. ¿Cuál es el futuro del elemento sorpresa en un mundo donde la abundancia de información puede paradójicamente incrementar la incertidumbre estratégica?

Estas interrogantes, abordadas desde una perspectiva tanto histórica como contemporánea, configuran el marco analítico mediante el cual este trabajo pretende ofrecer una visión de cómo el elemento sorpresa ha evolucionado sin desaparecer, adaptándose y transformándose para seguir siendo un factor decisivo en los conflictos del siglo XXI.

2 Herramientas de recolección masiva de información

2.1 Satélites: el fin de la niebla de la guerra

El siglo XXI ha sido testigo de una explosión en el uso militar del espacio. Los satélites de observación han transformado la manera en que los estados acceden a la información estratégica, erosionando significativamente la capacidad de sorpresa en la guerra (Weeden y Samson, 2022: 18-40).

En 2022, se registraron más de 2000 lanzamientos de satélites, y en 2023 la cifra total de objetos en órbita superó los 10 900 (Union of Concerned Scientists, 2023: 3-7). Este crecimiento no es meramente tecnológico, sino que refleja la creciente militarización del espacio. Satélites que antes se limitaban a tareas de observación meteorológica y comunicaciones ahora desempeñan un papel clave en la inteligencia militar, la vigilancia y el reconocimiento (ISR, por sus siglas en inglés).

La eficacia de estos sistemas es evidente en conflictos recientes. Durante la invasión rusa de Ucrania en 2022, imágenes satelitales de Maxar Technologies y análisis de inteligencia de Starlink X permitieron a Ucrania detectar y anticipar movimientos de tropas rusas (Freedman, 2022: 215-233). Por primera vez en la historia, el acceso a imágenes de satélite no estuvo restringido a las grandes potencias, sino que se convirtió en una herramienta disponible para Gobiernos más pequeños e incluso para actores privados y ONGs.

La importancia de los satélites para disipar la niebla de la guerra radica en su capacidad para obtener información detallada y precisa, que se logra mediante diferentes tecnologías de observación.

Los satélites emplean la teledetección activa, basada en radares de apertura sintética (SAR) que emiten ondas de radio y analizan el tiempo que tardan en regresar. Esta tecnología permite detectar objetos y medir distancias con alta precisión, incluso en condiciones adversas como la presencia de nubes o la oscuridad. Los sistemas SAR son capaces de medir el tiempo de vuelo del pulso desde que sale del satélite hasta que llega a la Tierra y retorna, permitiendo saber a qué distancia está un elemento, además, analizan el grado de absorción y penetración de la onda en la superficie, lo que permite obtener información no solo geométrica, sino también sobre la composición de la superficie.

La teledetección pasiva capta la luz solar reflejada por la Tierra, de manera similar a una cámara fotográfica. Esta tecnología proporciona imágenes de alta resolución espacial, pero su calidad se ve afectada por la nubosidad y la hora del día. Los satélites de teledetección pasiva, como el Sentinel-2, ofrecen una resolución espacial de diez metros. Los satélites militares también utilizan sensores infrarrojos que posibilitan la detección de calor, lo que es útil para identificar actividades en la oscuridad, así como para rastrear cambios en la temperatura de ciertas áreas y grupos de personas. Durante la guerra en Siria, estos sensores fueron usados para identificar el transporte de armas químicas en zonas controladas por el régimen de Assad (Futter, 2018: 135-140). Además, emplean carga multiespectral e hiperespectral, capaces de detectar la luz en múltiples bandas del espectro electromagnético. Esto ha sido clave en la detección de instalaciones nucleares clandestinas, como ocurrió con el programa iraní en Natanz (Kemp, 2014: 39-78).

Una tendencia reciente es el uso de enjambres de nanosatélites. A diferencia de los satélites tradicionales, estos dispositivos de bajo costo pueden trabajar en red, proporcionando imágenes en tiempo real y reduciendo el riesgo de que una sola unidad sea destruida o inutilizada (Pelton, 2020: 1-20). Por ejemplo, el programa PlanetScope opera con cientos de pequeños satélites en órbita baja, permitiendo un monitoreo continuo del planeta con actualizaciones diarias.

En España contamos el satélite español PAZ que materializa algunos de estos avances tecnológicos. Este es una plataforma de teledetección activa que envía 33 imágenes

diarias, con la capacidad de detectar cambios en la superficie de hasta 2-3 mm mediante la interferometría, lo que permite identificar zonas donde se ha removido tierra o donde se han enterrado minas, monitorizar la posición y el rumbo de 170 000-200 000 embarcaciones en todo momento gracias a su tecnología AIS (sistema de identificación automática), realizar un seguimiento de objetivos en movimiento, como vehículos y convoyes militares según datos de la Organización Marítima Internacional (2022).

El nivel de vigilancia actual impone desafíos a cualquier ejército que busque realizar una operación sorpresa. La acumulación de datos en tiempo real, combinada con algoritmos de inteligencia artificial, permite identificar patrones y prever movimientos antes de que se ejecuten. Un ejemplo claro es el sistema Project Maven del Pentágono, establecido como un equipo multifuncional de guerra algorítmica, que usa IA para analizar imágenes de vigilancia táctica y detectar hasta 38 clases de objetos críticos, incluyendo preparativos de ataques o movimientos de insurgentes en zonas de conflicto (Work, 2017: 1-2; Pellerin, 2017: 2-3). El sistema emplea redes neuronales inspiradas en la biología y técnicas de aprendizaje profundo para procesar automáticamente imágenes y videos de drones, identificando con precisión vehículos militares, armamento, fortificaciones y movimientos de tropas sin intervención humana directa. Esto permite que un solo analista procese hasta tres veces más información que antes, trabajando simbióticamente con los algoritmos para transformar el volumen masivo de datos de vigilancia en inteligencia accionable (Pellerin, 2017: 3-4).

La tecnología satelital no solo es capaz de detectar actividades físicas, sino también operaciones en el espectro electromagnético. Los satélites equipados con radar de apertura sintética (SAR) como Sentinel-1 han demostrado capacidad para detectar interferencias electrónicas (jamming) dirigidas contra sistemas GPS. En un estudio documentado por la Agencia Espacial Europea (2020: 34-42), se analizaron patrones de interferencia detectados sobre zonas de conflicto en Siria y el este de Ucrania, donde los sistemas SAR captaron anomalías consistentes con actividades de guerra electrónica. Estas firmas electromagnéticas permiten identificar posiciones desde las que se realizan operaciones de interferencia, incluso cuando los equipos físicos están ocultos o camuflados. Estas capacidades representan un cambio significativo en la transparencia del campo de batalla electromagnético, tradicionalmente invisible a la observación directa (Papathanasiou, 2019: 125-137). Este tipo de vigilancia reduce drásticamente la posibilidad de sorpresa táctica en el dominio cibernético y electromagnético, proporcionando alertas tempranas sobre actividades hostiles antes de que puedan materializarse en ataques convencionales.

2.2 La mente y lo digital: el big data *y el perfilado*

Si la vigilancia satelital ha reducido el margen para la sorpresa física, el desarrollo de herramientas avanzadas de perfilado psicológico combinado con el análisis del *big data* ha llevado la anticipación militar a un nuevo nivel. A través del análisis masivo de datos, patrones de comportamiento y predicciones psicológicas, los estados pueden prever decisiones estratégicas de sus adversarios con una precisión sin precedentes (Taddeo y Floridi, 2018: 723-735).

El concepto de perfilado psicológico aplicado a la guerra no es nuevo. Sun Tzu ya advertía que conocer al enemigo era tan importante como conocer el propio ejército. Sin embargo, en el siglo XXI, esta idea se ha materializado en sistemas de inteligencia artificial que analizan el comportamiento de líderes políticos, militares y organizaciones hostiles para prever sus acciones (Kahneman y Renshon, 2007: 34-48).

Un ejemplo claro de esta tendencia fue la operación de inteligencia previa a la invasión de Irak en 2003. Agencias de inteligencia estadounidenses utilizaron análisis de personalidad para evaluar las posibles respuestas de Saddam Hussein ante distintas presiones militares y diplomáticas (Post, 2003: 175-190). Hoy, herramientas como el perfilado de liderazgo computacional permiten predecir con alto grado de certeza la probabilidad de que un líder opte por la guerra, el compromiso diplomático o la disuasión nuclear (Renshon, 2021: 53-71).

El perfilado psicológico moderno se basa en el análisis de diversas variables que permiten predecir comportamientos y reducir la sorpresa ante decisiones estratégicas. Uno de los aspectos clave es el estudio de la historia personal y las creencias ideológicas de un individuo. Un ejemplo reciente es el análisis del comportamiento de Vladimir Putin, cuyo pasado como agente de la KGB y su visión del nacionalismo ruso han sido fundamentales para anticipar sus movimientos estratégicos (Hill y Gaddy, 2015: 98-112). Además, los patrones de toma de decisiones son otro factor importante, ya que se han identificado sesgos cognitivos recurrentes en líderes políticos y militares. Por ejemplo, el sesgo de exceso de confianza se observó tanto en Hitler en 1941 como en Israel antes de la Guerra de Yom Kipur en 1973, y se ha incorporado en modelos para predecir decisiones estratégicas (Levy, 1994: 279-312).

En la construcción del perfilado psicológico el análisis del lenguaje y el comportamiento no verbal también juega un papel crucial. Los algoritmos de inteligencia artificial han sido entrenados para detectar señales de agresión o conciliación en los discursos públicos. Las agencias de inteligencia emplean regularmente técnicas de análisis de comportamiento para evaluar líderes extranjeros (Fingar, 2011: 112-129).

Por otra parte, el *big data* ha revolucionado la inteligencia militar al permitir el análisis de cantidades masivas de información en tiempo real. Mientras que en el pasado los analistas militares dependían de informes fragmentados y fuentes humanas, hoy los algoritmos pueden detectar patrones ocultos en datos que van desde transacciones bancarias hasta interacciones en redes sociales (Allen y Chan, 2017: 63-85).

Un ejemplo de su impacto es la lucha contra el terrorismo. Los sistemas avanzados de análisis de datos desarrollados por agencias de seguridad permiten monitorizar comunicaciones digitales y detectar patrones de radicalización. El estudio de casos reales demuestra que estos sistemas pueden identificar indicadores específicos de radicalización en entornos online, como cambios en patrones lingüísticos, consumo de material extremista y participación creciente en foros radicales (Behr *et al.*, 2013: 42-47). Esta vigilancia digital se complementa con métodos de análisis de redes sociales que permiten identificar patrones de reclutamiento utilizados por organizaciones como el Estado Islámico, facilitando la neutralización de células terroristas antes de que ejecuten atentados (Berger y Morgan, 2015: 4-20).

En el ámbito de la guerra convencional, el análisis predictivo basado en *big data* ha sido clave en conflictos recientes. Durante la guerra en Ucrania, la inteligencia occidental utilizó modelos de predicción basados en análisis de datos económicos, logísticos y de movimientos militares para anticipar la invasión rusa semanas antes de que ocurriera (Freedman, 2022: 250-267).

A pesar de sus ventajas, estas herramientas no son infalibles. La sobrecarga de información y la proliferación de datos falsos pueden generar parálisis analítica, un fenómeno en el que los tomadores de decisiones se ven abrumados por un exceso de datos sin poder extraer conclusiones claras (Tetlock y Gardner, 2015: 25-40).

Además, el engaño estratégico sigue siendo un factor clave en la guerra. Actores como Rusia y China han perfeccionado el uso de desinformación para manipular la percepción de sus adversarios. Durante la anexión de Crimea en 2014, Rusia utilizó una combinación de desinformación y operaciones encubiertas para ocultar sus intenciones hasta que la ocupación fue un hecho consumado (Galeotti, 2017: 85-103).

Los avances tecnológicos han reducido el margen para la incertidumbre, pero la sorpresa no ha desaparecido. La información, por abundante que sea, solo es útil si se analiza con precisión y sin caer en falsas certezas. La historia ha demostrado que no es la falta de datos lo que genera vulnerabilidad, sino la manera en que se interpretan y se integran en la toma de decisiones (Fingar, 2011: 112-129).

3 Desinformación: el gran obstáculo en la era de la información

3.1 De la desinformación analógica a la digital

Si bien el acceso masivo a la información y las nuevas tecnologías han permitido una recopilación de datos sin precedentes, estos avances no garantizan una mejor toma de decisiones si la información recopilada es errónea o manipulada. La inteligencia predictiva y el análisis estratégico dependen no solo de la cantidad de datos disponibles, sino también de su veracidad y de la capacidad para interpretar correctamente los patrones que surgen de ellos. Sin embargo, en un entorno saturado de información, donde la desinformación y la manipulación informativa se han convertido en herramientas estratégicas clave, diferenciar entre datos fiables y engaños intencionados es un desafío cada vez mayor.

La manipulación de la información con fines estratégicos es una práctica tan antigua como la guerra misma. Desde tiempos inmemoriales, los ejércitos y los Gobiernos han utilizado la desinformación para confundir al enemigo, debilitar su moral o influir en la percepción de la población. Sun Tzu ya advertía que toda guerra se basa en el engaño, destacando la importancia de hacer creer al adversario que se es débil cuando se es fuerte, o que se atacará por un flanco cuando se hará por otro. A lo largo de la historia, el engaño ha jugado un papel crucial en numerosos conflictos, demostrando que la percepción de la realidad puede ser tan decisiva como la realidad misma.

Un ejemplo clásico de esto es la operación Fortitude durante la Segunda Guerra Mundial, en la que los Aliados llevaron a cabo una elaborada farsa para hacer creer a los

nazis que el desembarco en Francia se produciría en Pas-de-Calais en lugar de Normandía (Holt, 1978: 53-68). Se utilizaron falsos movimientos de tropas, transmisiones de radio engañosas y hasta la creación de un ejército ficticio con inflables y decorados para reforzar la ilusión de una inminente invasión en el punto equivocado. Este engaño fue tan efectivo que incluso después del 6 de junio de 1944, cuando las tropas aliadas ya habían desembarcado en Normandía, los nazis continuaron creyendo que era una distracción y que la verdadera ofensiva se daría en Pas-de-Calais, retrasando su respuesta.

Hoy en día, la desinformación se ha convertido en un fenómeno global, potenciado por el acceso masivo a las redes sociales y el crecimiento de plataformas digitales que permiten la difusión instantánea de contenido sin verificación rigurosa. La anexión de Crimea en 2014 es un claro ejemplo del uso contemporáneo de estas estrategias. Rusia empleó una combinación de acción militar encubierta y una intensa campaña de desinformación para justificar la intervención ante la opinión pública interna y externa (Galeotti, 2017: 42-58). Se crearon narrativas falsas que representaban a las fuerzas rusas como «grupos de autodefensa» locales, mientras que los medios estatales propagaban la idea de que el Gobierno ucraniano estaba controlado por extremistas, dificultando la respuesta occidental y generando incertidumbre.

En el siglo XXI, la proliferación de información digital ha cambiado las reglas del juego. La información falsa ya no se difunde exclusivamente a través de panfletos o radio, sino que se viraliza en cuestión de minutos mediante redes sociales. Durante las elecciones presidenciales de EE. UU. en 2016, investigaciones revelaron que miles de cuentas automatizadas, muchas vinculadas a Rusia, participaron en la difusión de información engañosa con el objetivo de polarizar la opinión pública y erosionar la confianza en las instituciones democráticas (Benkler *et al.*, 2018: 225-260). A través de bots se promovieron teorías conspirativas y noticias falsas diseñadas para influir en el electorado, exacerbando divisiones preexistentes en la sociedad estadounidense.

Desde un punto de vista estratégico, la desinformación ya no es simplemente una herramienta de propaganda; se ha convertido en un arma política y militar con el potencial de desestabilizar Gobiernos y manipular la percepción de la realidad. La rapidez con la que se propagan estas narrativas falsas, combinada con la dificultad para desmentirlas de manera efectiva, hace que las operaciones de desinformación sean más peligrosas que nunca. A diferencia de las guerras tradicionales, donde los ejércitos se enfrentan en el campo de batalla, la guerra de la información se libra en la mente de la población, donde la verdad y la mentira compiten por imponerse.

La historia ha demostrado que el control de la información es tan importante como el control del territorio. En un mundo donde la información fluye sin restricciones, la capacidad de distinguir entre la verdad y la manipulación es un desafío cada vez más complejo, tanto para los Gobiernos como para los ciudadanos.

3.2 Los nuevos métodos de desinformación

El impacto de la desinformación en el análisis de inteligencia es particularmente grave, ya que socava la credibilidad de las fuentes y dificulta la toma de decisiones basada en

hechos verificables. Los analistas ya deben enfrentarse a sus propios sesgos cognitivos en la interpretación de datos, pero cuando la información es deliberadamente manipulada, el riesgo de conclusiones erróneas aumenta exponencialmente (Heuer, 1999: 111-126). Esta situación es impulsada por la proliferación de herramientas tecnológicas diseñadas para amplificar la manipulación informativa.

Los *bots* y trols operan como ejércitos digitales diseñados para inundar el espacio informativo con narrativas específicas, dificultando la identificación de fuentes legítimas y generando confusión en la opinión pública. En conflictos recientes, como la guerra en Ucrania, estos métodos han sido utilizados para fabricar una percepción distorsionada del enfrentamiento, desestabilizando a la sociedad y reduciendo la capacidad de los analistas de inteligencia para obtener una visión clara del desarrollo de los eventos. También, los *deepfakes*, por su parte, representan un avance en la manipulación audiovisual, permitiendo la creación de vídeos falsos que pueden atribuir declaraciones o acciones a actores políticos y militares sin que estos las hayan realizado. Esta tecnología tiene un enorme potencial disruptivo en el campo militar, donde la confianza en la autenticidad de la información es clave. La posibilidad de difundir vídeos falsificados con discursos de líderes militares o políticos puede generar caos, confusión y decisiones erróneas basadas en información manipulada.

A su vez, la falsificación de documentos sigue siendo una de las estrategias más utilizadas en la desinformación militar. Documentos filtrados y modificados pueden influir en negociaciones diplomáticas, desmoralizar tropas o provocar crisis entre aliados. La manipulación de registros de inteligencia, informes estratégicos y órdenes militares ha sido utilizada a lo largo de la historia para inducir errores en la planificación operativa de los adversarios.

Un factor agravante en la problemática de la desinformación es la velocidad con la que se propaga. En décadas anteriores, las operaciones de manipulación informativa requerían meses o incluso años para surtir efecto, mientras que, en la actualidad, con la presencia de redes sociales y plataformas digitales, una noticia falsa puede alcanzar a millones de personas en cuestión de horas. Este fenómeno se vio reflejado en la crisis de desinformación durante la pandemia de COVID-19, donde teorías de conspiración y datos manipulados se viralizaron, generando desconfianza en la ciencia y en las medidas de salud pública (Lewandowsky *et al.*, 2021: 80-127). La falta de regulación efectiva sobre la propagación de contenido falso ha permitido que ciertos actores exploten esta situación para fines políticos o económicos, erosionando la confianza en las instituciones y polarizando sociedades enteras.

Combatir la desinformación requiere un enfoque multidimensional que combine tecnología, educación y regulación. La implementación de algoritmos de detección de patrones es una estrategia prometedora para identificar redes de desinformación en tiempo real (Ferrara *et al.*, 2016: 96-104). Sin embargo, también existe el riesgo de que estos algoritmos puedan sesgarse y terminar censurando información válida. Por ello, es crucial que el desarrollo de estas tecnologías se complemente con la supervisión humana y la transparencia en sus mecanismos de aplicación.

Otro elemento esencial en la lucha contra la desinformación es la educación mediática. Estudios han demostrado que el pensamiento crítico y la capacidad de evaluar fuentes

de información pueden reducir significativamente la propagación de noticias falsas (McGrew *et al.*, 2018: 165-193). En este sentido, algunos países han implementado programas educativos enfocados en enseñar a los ciudadanos cómo identificar contenido manipulado y cómo verificar la credibilidad de una fuente antes de compartirla. Aunque estos programas son un paso en la dirección correcta, su impacto a gran escala aún está por demostrarse.

A nivel gubernamental, organismos internacionales como la Unión Europea han desarrollado estrategias conjuntas para rastrear y eliminar contenido falso de plataformas digitales (European Commission, 2020: 8-15). No obstante, este tipo de medidas plantea un dilema sobre la libertad de expresión, ya que la regulación del contenido en internet podría ser utilizada por ciertos Gobiernos para censurar críticas legítimas o silenciar la disidencia. La solución radica en encontrar un equilibrio entre la protección de la información veraz y el respeto a los derechos fundamentales.

En el ámbito militar y de seguridad, las agencias de inteligencia han comenzado a adoptar estrategias de «verificación cruzada intensiva» para garantizar la fiabilidad de la información antes de incorporarla en sus análisis (Rid, 2020: 412-435). Esto implica contrastar fuentes de distinta procedencia, analizar patrones de desinformación y rastrear el origen de determinadas narrativas falsas. Sin embargo, el desafío sigue siendo monumental debido a la cantidad abrumadora de información que circula a diario en entornos digitales.

El combate a la desinformación también depende en gran medida de la responsabilidad de los medios de comunicación tradicionales. Si bien la proliferación de redes sociales ha descentralizado la producción y distribución de noticias, los medios siguen jugando un papel crucial en la verificación de hechos y en la educación del público sobre la importancia de contrastar información. Sin embargo, también han sido responsables en ocasiones de propagar información errónea en su afán de ser los primeros en reportar una noticia. Esto resalta la importancia de la ética periodística y la necesidad de mecanismos de autocontrol en las prácticas informativas.

Así, el fenómeno de la desinformación no solo afecta a la percepción de la realidad, sino que representa una amenaza tangible para la seguridad global, el análisis de inteligencia y la estabilidad de las democracias. Afrontarlo exige un compromiso conjunto entre Gobiernos, empresas tecnológicas, medios de comunicación y ciudadanos, para construir una sociedad más resiliente y crítica frente a la manipulación informativa.

4 La importancia del análisis

Retomamos la pregunta inicial, más allá de la sorpresa en su ejecución ¿qué tienen en común el ataque japonés a Pearl Harbor en 1941, la invasión alemana de la Unión Soviética también en 1941 (operación Barbarroja), la invasión alemana de Noruega en 1940 y el ataque egipcio y sirio a Israel en 1973 (guerra de Yom Kippur)?

En todos estos casos, las víctimas hicieron suposiciones erróneas sobre las intenciones y capacidades del atacante (Betts, 1982: 32-54). Por ejemplo, Estados Unidos subestimó la capacidad de Japón para llevar a cabo un ataque en Pearl Harbor, mientras que la Unión

Soviética no creyó que Alemania atacaría, a pesar de las señales de movilización. En el caso de la guerra de Yom Kippur, Israel no consideró la posibilidad de un ataque conjunto por parte de Egipto y Siria, a pesar de las señales de que se estaban preparando. La invasión de Noruega por parte de Alemania fue una sorpresa porque Noruega no se consideraba un objetivo prioritario y creía en su neutralidad.

A pesar de que en todos estos casos existían señales de que un ataque era inminente, estas señales no fueron interpretadas correctamente o fueron ignoradas. El estudio de la sorpresa militar ha demostrado que los sesgos cognitivos desempeñan un papel crucial en estos fracasos. Los líderes tienden a aferrarse a sus percepciones previas incluso cuando la evidencia sugiere lo contrario, un fenómeno que se acentúa en entornos de alta incertidumbre (Jervis, 1976: 58-84). En el caso de Pearl Harbor, hubo información de inteligencia que indicaba la posibilidad de un ataque, pero no se le dio la importancia necesaria (Wohlstetter, 1962: 382-401). De igual manera, Stalin recibió advertencias sobre la inminente invasión alemana, pero optó por ignorarlas bajo la creencia de que Hitler no abriría un segundo frente en 1941 (Gorodetsky, 1999: 238-265). Similarmente, en la guerra de Yom Kippur, Israel no consideró la posibilidad de un ataque egipcio-sirio a gran escala, a pesar de múltiples advertencias. La creencia de que Egipto no se arriesgaría a una guerra sin superioridad aérea llevó a ignorar los movimientos de tropas en la frontera (Bar-Joseph, 2013: 145-162).

En la mayoría de los casos hubo operaciones de engaño por parte de los atacantes para ocultar sus verdaderas intenciones. Alemania llevó a cabo operaciones de desinformación para ocultar sus planes de ataque a la Unión Soviética, y también en el caso de Noruega. Japón tomó medidas para hacer creer que negociaba con Estados Unidos cuando realmente se preparaba para el ataque.

Estos ejemplos ilustran cómo una combinación de suposiciones erróneas, falta de atención a las advertencias y un estado de preparación inadecuado hacen que los ataques sorpresa sean un fenómeno que palie, no con mejor información sino con la alerta constante y la correcta atención al análisis de la obtención.

Una falla en la prevención de ataques sorpresa a menudo radica en la incapacidad de una organización para manejar la información de manera adecuada, no logrando distinguir entre señales importantes y ruido (Barnea y Meshulach, 2021: 43-59). La sobrecarga de datos puede ser tan peligrosa como su escasez, ya que puede llevar a la parálisis analítica o a la priorización incorrecta de amenazas (Fingar, 2011: 75-91). Durante la invasión de Noruega, las autoridades aliadas recibieron informes sobre movimientos inusuales en la Kriegsmarine, pero estos fueron interpretados como maniobras rutinarias (Gannon, 2021: 35-48). Un problema recurrente en la inteligencia militar es que las señales de advertencia suelen ser ambiguas y requieren no solo información objetiva, sino también intuición estratégica para ser correctamente interpretadas (Heuer y Pherson, 2010: 132-148).

Un análisis eficaz no solo depende de la información disponible, sino también de la estructura organizativa y la capacidad de cuestionar suposiciones. Como menciona Handel (1984), la inteligencia no solo debe identificar amenazas, sino también desafiar narrativas preexistentes dentro de la toma de decisiones estratégicas. Esto implica fomentar un pensamiento crítico dentro de las agencias de inteligencia y evitar la tendencia al

conformismo analítico. Un claro ejemplo de este problema fue la confianza excesiva en la disuasión nuclear durante la Guerra Fría, lo que llevó a descartar la posibilidad de conflictos convencionales a gran escala (Luttwak, 1987: 189-205).

Así, la misión principal del análisis de inteligencia es proporcionar información y conocimientos oportunos que ayuden a los tomadores de decisiones a comprender los acontecimientos con implicaciones trascendentales para los intereses nacionales (Fingar, 2011: 117-132). No se trata solo de presentar «hechos», sino de ofrecer perspectivas sobre tendencias, la lógica política de líderes extranjeros o la forma en que se perciben los problemas fuera del país. En otras palabras, el análisis es lo que transforma los datos brutos en inteligencia útil.

La importancia del análisis se manifiesta en la evaluación de las capacidades y las intenciones del enemigo. Las capacidades de tiempo de guerra de los sistemas de armas no pueden deducirse automáticamente de sus características técnicas, sino que dependen de los conceptos operativos, la estrategia y las tácticas que dirigirían su uso (Kam, 2004: 163-178). Esto implica que el análisis no se limita a la recopilación de información técnica, sino que también requiere una comprensión del contexto en el que se emplea dicha tecnología.

El análisis también es fundamental para la identificación de «señales débiles» que podrían indicar un ataque sorpresa. Un ataque sorpresa es un juego de ingenio entre un «atacante» que busca lanzar un ataque por sorpresa y una «víctima» que intenta recopilar información sobre las intenciones del atacante (Barnea y Meshulach, 2021: 60-75). En este juego, la capacidad de discernir «señales débiles», a menudo fragmentadas y ambiguas, es crucial para anticipar los movimientos del enemigo. Esta habilidad analítica requiere creatividad, pensamiento original e iniciativa para construir escenarios preventivos, y a menudo implica el estudio de entornos nuevos y desconocidos. Como menciona un estudio de la NRC[2], un buen analista puede ayudar a sus clientes a identificar las preguntas que deberían haber hecho, lo que implica un papel activo en la configuración de la agenda de inteligencia.

Los sesgos cognitivos y las limitaciones organizacionales pueden obstaculizar el análisis efectivo. Los analistas a menudo se enfrentan a información ambigua y deben lidiar con sus propios sesgos y suposiciones (Kam, 2004: 189-207). El análisis se ve afectado por la necesidad de una toma de decisiones rápida en grupos que pueden ser influenciados por líderes u otros miembros dominantes. Además, los decisores pueden simplificar las evaluaciones de inteligencia, lo que puede llevar a pasar por alto detalles importantes. La tendencia de los analistas a ser cautelosos en sus predicciones y a buscar consenso puede generar ambigüedades que diluyen la fuerza de sus conclusiones. La necesidad de dar una conclusión clara puede llevar a la pérdida de matices importantes y por la falta de voluntad de tomar riesgos en sus valoraciones.

La historia demuestra que la sorpresa militar no es solo un fenómeno táctico, sino también un fallo de percepción. La verdadera prevención del ataque sorpresa no radica

2 Véase: National Research Council (2011). Intelligence Analysis: Behavioral and Social Scientific Foundations. En: B. Fischhoff & C. Chauvin (Eds.). *Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security*. The National Academies Press.

en la acumulación infinita de datos, sino en la capacidad de analizarlos de manera flexible y crítica (Tetlock y Gardner, 2015: 75-89). La clave, por tanto, no es únicamente obtener información, sino comprenderla antes de que sea demasiado tarde.

Este «demasiado tarde» se materializa con trágica regularidad. Cincuenta años después del trauma del Yom Kippur, Israel ha vuelto a sufrir su propio fantasma estratégico: la incapacidad para convertir la información disponible en acción decisiva. Mientras los soldados israelíes observaban, paralizados, la infiltración masiva de milicianos de Hamás el 7 de octubre de 2023, no presenciábamos un fallo de recolección de inteligencia, sino la manifestación contemporánea de lo que Bar-Joseph denominó «la trampa de la observación sin actuación» (Bar-Joseph, 2005:142-144). La verdadera sorpresa no radicó en la ausencia de información, sino en la incomprensible desconexión entre sistemas de vigilancia ultramodernos y mecanismos decisorios anclados en burocracias del siglo pasado. Esta disociación entre conocimiento y acción demuestra que la sofisticación tecnológica, lejos de garantizar seguridad, puede generar una peligrosa complacencia cuando la cadena de mando carece de protocolos que conviertan el análisis en imperativo operacional inmediato.

El análisis debe transmutarse en mandato. La inteligencia que no cataliza acción es mera contemplación académica del desastre. Los sistemas de alerta avanzada que carecen de mecanismos de activación automática son vulnerables a la parálisis institucional (Wirtz, 2004:12-15), una lección que en 1973 no se consiguió imprimir en la conciencia estratégica israelí. Para romper esta inercia, es necesario revolucionar la arquitectura decisoria creando umbrales de acción predeterminados donde ciertos indicadores críticos desencadenen protocolos de respuesta inmediata, eludiendo las jerarquías tradicionales. La tragedia de octubre evidencia que la democratización de la capacidad decisoria en niveles tácticos, particularmente cuando la información está disponible en tiempo real, no es un lujo académico sino un imperativo estratégico. En última instancia, el análisis de inteligencia solo cumple su verdadero propósito cuando trasciende la esfera informativa para convertirse en un catalizador ineludible de la acción defensiva.

5 La verdadera tragedia: la pérdida de la capacidad de sorprenderse

En el laberinto de la guerra, donde la estrategia y la tecnología se entrelazan, la ilusión de controlar el futuro a través de la información puede convertirse en una trampa. La noción del «fin de la sorpresa» en el ámbito militar no debe interpretarse como la erradicación de lo inesperado, sino como la urgente necesidad de cultivar una mentalidad vigilante. Porque, a pesar de la aparente omnipresencia de la información y los avances tecnológicos, la historia nos enseña que la complacencia y la pérdida de la capacidad de sorprendernos son el caldo de cultivo perfecto para la vulnerabilidad.

La raíz de la sorpresa se nutre de nuestra propia falta de atención. A menudo, la abundancia de datos nos ciega, llevándonos a ignorar las señales que nos advierten del peligro inminente. Las víctimas de ataques sorpresa no carecían de información, sino de la capacidad de interpretarla correctamente (Kam, 2004: 215-230). La familiaridad con las rutinas, la complacencia y nuestra tendencia a rechazar lo que consideramos improbable

nos hacen vulnerables. En un mundo donde la información fluye constantemente, la verdadera amenaza reside en nuestra propia incapacidad de prestar atención a las señales de advertencia.

Esta incapacidad interpretativa revela una dimensión más profunda y problemática: la difuminación de responsabilidades en la cadena analítico-decisoria. Cuando todos observan la anomalía pero nadie actúa, no enfrentamos meramente un fallo técnico, sino un colapso moral del sistema de seguridad. «La ambigüedad en la atribución de responsabilidades constituye, por sí misma, una vulnerabilidad letal que los adversarios pueden explotar deliberadamente» (Bar-Joseph, 2005: 187-189). La toma de decisiones en entornos de alta incertidumbre requiere distinguir rigurosamente entre la responsabilidad del analista (alertar con contundencia proporcional a la gravedad de los indicios, aun siendo estos fragmentarios) y la del decisor (actuar resolutivamente con información incompleta cuando los riesgos de inacción superan los de una respuesta excesiva). El silencio cómplice ante esta confusión de roles ha permitido que organizaciones enteras se paralicen en momentos críticos, refugiándose cada actor en la zona de confort burocrática de su no responsabilidad.

La supuesta neutralidad de la inacción es, quizá, la falacia más peligrosa en el ámbito de la seguridad estratégica. La decisión de no decidir constituye, paradójicamente, la decisión más definitiva, pues entrega la iniciativa completamente al adversario (Fischhoff y Chauvin, 2011:118-120). Esta perspectiva exige revolucionar nuestros marcos institucionales, estableciendo protocolos donde la responsabilidad de actuar ante indicios críticos no sea meramente una opción. Sin este elemento catalizador que transforme el análisis en acción resolutiva, nuestros sofisticados sistemas de vigilancia no serán más que testigos pasivos, documentando con precisión técnica, pero sin consecuencia operativa, el próximo desastre que podría haber sido evitado.

Por el lado del atacante, en ocasiones, el secreto del enemigo persiste como un obstáculo difícil de superar. A pesar de la transparencia de la era de la información, existen zonas grises donde los adversarios pueden operar con sigilo. Un ejemplo moderno de ello es el diseño de las hélices de los submarinos, que han evolucionado para reducir su firma acústica y evitar su detección. En un mundo donde la información parece estar al alcance de todos, la realidad es que existen operaciones y capacidades que aún escapan a nuestro conocimiento.

La historia demuestra que la evolución tecnológica es cíclica: en ciertos momentos, los sistemas diseñados para evitar la sorpresa superan a aquellos que buscan generarla, pero más tarde, la situación se invierte (Kam, 2004: 231-246). El progreso militar no sigue una línea recta, sino un proceso de adaptación constante entre ofensiva y defensiva (Luttwak, 1987: 212-229). Así ocurrió con el desarrollo del radar en la Segunda Guerra Mundial. Inicialmente otorgó ventaja a los Aliados al detectar bombarderos enemigos, pero más tarde impulsó la creación de aeronaves furtivas para evadir esa detección. Así, innovación tecnológica, en su búsqueda de la ventaja, también puede generar nuevas fuentes de sorpresa.

En este contexto, la suposición de un «fin de la sorpresa» es, en el mejor de los casos, una falacia peligrosa. No se trata de la erradicación de la sorpresa, sino de la necesidad de

mantener una actitud de vigilancia continua. Por ello, es vital realizar un análisis crítico de la información disponible, prestar atención a las señales sutiles y ser conscientes de nuestras propias limitaciones cognitivas. La falsa sensación de seguridad, la capacidad del enemigo de ocultar sus planes y la evolución tecnológica que genera nuevas sorpresas son factores que aseguran que la sorpresa siga siendo un elemento inevitable en la guerra moderna. El verdadero desafío radica en nuestra capacidad de prepararnos para lo inesperado, manteniendo nuestra capacidad de asombro y la humildad ante lo desconocido.

6 Conclusión: ¿fin de la sorpresa o evolución de la incertidumbre?

La historia demuestra que la sorpresa nunca ha dependido exclusivamente de la falta de información, sino de la incapacidad humana para interpretar correctamente el entorno. A lo largo del tiempo, las innovaciones tecnológicas han reducido el margen para los ataques sorpresa tradicionales, pero no han eliminado el factor de incertidumbre en la guerra. La sorpresa no desaparece con la información, sino que se transforma, explotando fallos de percepción, exceso de confianza y errores en el análisis estratégico (Betts, 1982: 250-268).

En la actualidad, la vigilancia global y el análisis masivo de datos han cambiado las dinámicas de la sorpresa militar, pero no la han erradicado. La guerra sigue siendo un entorno de alta incertidumbre, donde el ingenio humano y la adaptabilidad continúan desempeñando un papel crucial (Freedman, 2022: 398-415). La sorpresa ya no se basa únicamente en el sigilo físico, sino en la manipulación de la percepción, el engaño estratégico y la explotación de vulnerabilidades cognitivas.

Cuando las fuentes de información están deliberadamente contaminadas con elementos falsos o manipulados, los analistas se enfrentan al reto de filtrar el ruido del entorno y distinguir lo veraz de lo engañoso. En este contexto, la recopilación masiva de información deja de ser una garantía de conocimiento y puede, en cambio, convertirse en un arma de desorientación masiva. La historia ha demostrado que una inteligencia mal interpretada o basada en premisas falsas puede llevar a decisiones catastróficas en el ámbito militar y geopolítico. Por ello, la clave para evitar la sorpresa en el mundo contemporáneo no radica únicamente en la cantidad de información disponible, sino en la capacidad de evaluarla de manera crítica y estructurada.

Como señala Tetlock y Gardner (2015), la sobrecarga de información sin un análisis riguroso puede ser tan peligrosa como la ausencia de datos. Sin una metodología analítica adecuada, la saturación informativa puede generar parálisis estratégica o, peor aún, decisiones basadas en premisas incorrectas. En este sentido, el análisis de inteligencia se convierte en el verdadero pilar sobre el cual debe construirse la seguridad estratégica, permitiendo convertir el caótico flujo de datos en información procesable y útil para la toma de decisiones.

Por tanto, no estamos ante el fin de la sorpresa, sino ante su transformación. La pregunta no es si la sorpresa desaparecerá, sino cómo seguirá adaptándose a un mundo donde la información es más accesible que nunca, pero la interpretación de esa información sigue siendo el eslabón más débil. Como afirmaba Liddell Hart (1954: 165), «la mejor sorpresa no es aquella que el enemigo no ve venir, sino aquella que ve venir demasiado tarde para reaccionar».

Bibliografía

Agencia Espacial Europea. (2020).*SAR Imaging of Electronic Warfare Activities in Conflict Zones*, Technical Report Series, ESA-TR-2020-03.

Allen, G. C. y Chan, T. (2017). *Artificial Intelligence and National Security*. Cambridge, MA: Belfer Center for Science and International Affairs.

Aznar Montesinos, F. (2021). El espacio exterior, una nueva dimensión de la Seguridad, *Documento de análisis, 10/2021*, Instituto Español de Estudios Estratégicos (IEEE).

Bar-Joseph, U. (2013). *The Watchman Fell Asleep: The Surprise of Yom Kippur and Its Sources*. Albany: State University of New York Press.

Barnea, A. (2005). Link Analysis as a Tool for Competitive Intelligence, *Competitive Intelligence Magazine*, 10(4).

—(2018). Challenging the "Lone Wolf" Phenomenon in an Era of Information Overload, *International Journal of Intelligence and CounterIntelligence*, 31(2).

Barnea, A. y Meshulach, A. (2021). Forecasting for Intelligence Analysis: Scenarios to Abort Strategic Surprise, *Intelligence and National Security*, 36(2).

Behr, I., Reding, A., Edwards, C. y Gribbon, L. (2013). *Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism*, RAND Europe.

Benkler, Y., Faris, R. y Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press.

Berger, J. M. y Morgan, J. (2015). The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter, *The Brookings Project on U.S. Relations with the Islamic World*, 3(20).

Betts, R. K. (1982). *Surprise Attack: Lessons for Defense Planning.* Washington, D.C.: Brookings Institution Press.

Boghardt, T. (2009). Operation INFEKTION: Soviet Bloc Intelligence and the AIDS Disinformation Campaign, *Studies in Intelligence*, 53(4).

Borum, R. (2004). *Psychology of terrorism*. University of South Florida.

Chesney, R. y Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, *California Law Review*, 107.

Clausewitz, K. von (1832). *On War*. Princeton: Princeton University Press.

DARPA (2017). *Deep Exploration and Filtering of Text (DEFT) Program,* DARPA.

European Commission. (2020). *Tackling Online Disinformation: A European Approach*. Luxembourg: Publications Office of the European Union.

Ferrara, E. *et al.* (2016). The Rise of Social Bots, *Communications of the ACM*, 59(7).

Fingar, T. (2011). *Reducing Uncertainty: Intelligence Analysis and National Security*. Stanford: Stanford University Press.

Freedman, L. (2022). *Command: The Politics of Military Operations from Korea to Ukraine*. London: Allen Lane.

Futter, A. (2018). *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Georgetown University Press.

Galeotti, M. (2017). *Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right*. Rome: NATO Defense College.

Gannon, K. (2021). *The Fall of Kabul: Intelligence Miscalculations and Strategic Errors*. Washington, D.C.: The Atlantic Council.

Gorodetsky, G. (1999). *Grand Delusion: Stalin and the German Invasion of Russia*. Yale University Press.

Handel, M. (1984). Intelligence and the Problem of Strategic Surprise, *Journal of Strategic Studies*, 7(3).

Heuer, R. J. (1999). *Psychology of Intelligence Analysis*. Washington, D.C.: CIA Center for the Study of Intelligence.

Heuer, R. J. y Pherson, R. H. (2010). *Structured Analytic Techniques for Intelligence Analysis*. Washington, D.C.: CQ Press.

Hill, F. y Gaddy, C. G. (2015). *Mr. Putin: Operative in the Kremlin*. Washington, D.C.: Brookings Institution Press.

Holt, T. (1978). *The Deceivers: Allied Military Deception in the Second World War*. New York: Scribner.

Jervis, R. (1976). *Perception and Misperception in International Politics*. Princeton University Press.

Kahneman, D. y Renshon, J. (2007). Why Hawks Win, *Foreign Policy*, 158.

Kam, E. (2004). *Surprise Attack: The Victim's Perspective, With a New Preface*. Cambridge, MA: Harvard University Press.

Kemp, R. S. (2014). The Nonproliferation Emperor Has No Clothes: The Gas Centrifuge, Supply-Side Controls, and the Future of Nuclear Proliferation, *International Security*, 38(4).

Levy, J. S. (1994). Learning and Foreign Policy: Sweeping a Conceptual Minefield, *International Organization*, 48(2).

Lewandowsky, S., Ecker, U. K. H. y Cook, J. (2021). Misinformation and Its Correction: Cognitive Mechanisms and Recommendations for Mass Communication, *Psychological Science in the Public Interest*, 22(3).

Liddell Hart, B. H. (1954). *Strategy*. New York: Praeger.

Lucas, E. y Pomerantsev, P. (2016). *Winning the Information War: Techniques and Counter-strategies to Combat Russian Propaganda in Europe*. Washington, D.C.: Center for European Policy Analysis.

Luttwak, E. (1987). *Strategy: The Logic of War and Peace*. Cambridge, MA: Harvard University Press.

McGrew, S. *et al.* (2018). Can Students Evaluate Online Sources? Learning From Assessments of Civic Online Reasoning, *Theory & Research in Social Education*, 46(2).

National Research Council. (2011). *Intelligence Analysis: Behavioral and Social Scientific Foundations.* B. Fischhoff & C. Chauvin (Eds.). The National Academies Press.

Organización Marítima Internacional. (2021). *Informe sobre el Transporte Marítimo 2021*. Londres: OMI.

Oreskes, N. y Conway, E. M. (2010). *Merchants of Doubt: How a Handful of Scientists Obscured the Truth on Issues from Tobacco Smoke to Global Warming*. New York: Bloomsbury Press.

Papathanasiou, K., Boutsi, A. y Filippidis, P. (2019). Detection and Classification of Electronic Warfare Signals Using Satellite Remote Sensing, *IEEE Transactions on Geoscience and Remote Sensing*, 57(3).

Paredes, M. y Oliveira, J. (2023). Tecnologías emergentes y amenazas asimétricas en el entorno marítimo.

Pellerin, C. (2017). Project Maven to Deploy Computer Algorithms to War Zone by Year's End, *DoD News*, 21 de julio de 2017.

Pelton, J. N. y Madry, S. (2020). Introduction to the Small Satellite Revolution and Its Many Implications, *Handbook of Small Satellites*.

Perry, W. J. y Carter, A. B. (1999). *Preventive Defense: A New Security Strategy for America*. Washington, D.C.: Brookings Institution Press.

Post, J. M. (2003). *The Psychological Assessment of Political Leaders*. Ann Arbor: University of Michigan Press.

Preston, P. (2012). *The Spanish Holocaust: Inquisition and Extermination in Twentieth-Century Spain*. London: HarperPress.

Renshon, J. (2021). Psychological Approaches to International Relations. En: *Oxford Research Encyclopedia of Politics*.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.

Schmidt, E. (2020). *The Age of AI: And Our Human Future*. Little, Brown and Company.

Sun Tzu (500 a. C.). *El arte de la guerra*. Barcelona: Ediciones Obelisco, 2019.

Taddeo, M. y Floridi, L. (2018). How AI can be a force for good, *Science*, 361(6404).

Tetlock, P. y Gardner, D. (2015). *Superforecasting: The Art and Science of Prediction*. New York: Crown.

Union of Concerned Scientists (2023). *UCS Satellite Database*, Cambridge, MA.

Van Creveld, M. (1991). *The Transformation of War*. New York: Free Press.

Weeden, B. y Samson, V. (2022). *Global Counterspace Capability: An Open Source Assessment*. Washington, D.C.: Secure World Foundation.

Wirtz, J. J. (2004). Miscalculation, Surprise and American Intelligence after the Cold War. *International Journal of Intelligence and CounterIntelligence*, 15(1), 1-19.

Wohlstetter, R. (1962). *Pearl Harbor: Warning and Decision*. Stanford University Press.

Work, R. (2017). *Establishment of the Algorithmic Warfare Cross-Functional Team (Project Maven)*, Memorando del Departamento de Defensa, 26 de abril de 2017.

Zwitter, A. (2015). Anticipatory intelligence and strategic surprise prevention.

Artículo recibido: 30 de enero de 2025
Artículo aceptado: 13 de mayo de 2025