TECNOLOGÍAS DISRUPTIVAS COMO HERRAMIENTAS DE DISUASIÓN

Benigno González-Aller Gross
Vicealmirante

SÍNTESIS
En un mundo donde la fuerza militar tradicional ya no garantiza la seguridad, este artículo analiza cómo las tecnologías disruptivas —como la inteligencia artificial, la fotónica, la computación cuántica o la ciberdefensa— se han convertido en instrumentos clave de disuasión estratégica. Más allá del combate, su poder reside en proyectar incertidumbre, superioridad y resiliencia frente al adversario. A través de un enfoque accesible, el texto explora su impacto doctrinal, psicológico y político, y plantea los requisitos necesarios para que una nación, como España, transforme su potencial tecnológico en una verdadera ventaja estratégica.

PALABRAS CLAVE: TECNOLOGÍAS DISRUPTIVAS, FOTÓNICA, COMPUTACIÓN CÁNTICA, DISUASIÓN, RESILIENCIA, CIBERDEFENSA.

INTRODUCCIÓN

En el siglo XXI, la disuasión estratégica ha experimentado una transformación silenciosa pero profunda. Tradicionalmente entendida como la capacidad de prevenir una agresión mediante la amenaza creíble de represalias devastadoras —ya fueran nucleares o convencionales—, esta concepción ha quedado incompleta frente a la complejidad del entorno actual. Las dinámicas geopolíticas contemporáneas, caracterizadas por la competencia entre grandes potencias, la proliferación de actores no estatales y la acelerada evolución tecnológica, han desplazado el foco de la disuasión desde la cantidad de medios hacia la calidad de las capacidades.

El nuevo campo de juego es tecnológico. La ventaja ya no reside únicamente en la posesión de plataformas militares avanzadas, sino en la capacidad de innovar, integrar y proyectar tecnologías emergentes

de manera rápida y efectiva. En este sentido, la disuasión se redefine: no se trata tanto de amenazar con una respuesta aplastante tras una agresión, sino de generar en el adversario la convicción de que cualquier intento de ataque o interferencia resultará infructuoso, costoso o incluso contraproducente antes de materializarse.

La Brújula Estratégica de la Unión Europea (2022) lo expresa con claridad: «La superioridad tecnológica es un factor clave para preservar la autonomía estratégica y proteger nuestros valores en un entorno global cada vez más competitivo y contestado». Esta afirmación refleja un cambio de paradigma que también ha sido recogido en los documentos estratégicos de la OTAN y diversas potencias internacionales: el futuro de la disuasión está indisolublemente ligado al dominio de las tecnologías disruptivas.

Estas tecnologías —inteligencia artificial, computación cuántica, sistemas autónomos, capacidades cibernéticas, guerra electrónica o fotónica avanzada— actúan como multiplicadores de poder que amplían las opciones estratégicas sin necesidad de recurrir a la fuerza convencional. Su valor no radica únicamente en su uso táctico, sino en el efecto psicológico y estratégico que generan: aumentan la incertidumbre del adversario, complican su planificación, erosionan su percepción de ventaja y elevan el umbral del riesgo asumible.

En este nuevo escenario, la disuasión se ejerce también desde el plano cognitivo. La velocidad para detectar, decidir y actuar —impulsada por tecnologías como la inteligencia artificial y los sensores inteligentes— puede ser más determinante que el volumen de fuego disponible. El que actúa primero, con precisión y resiliencia, impone una narrativa operativa que desincentiva cualquier desafío. Disuadir, por tanto, es también proyectar una superioridad percibida en todos los dominios, visibles o invisibles.

Este artículo explora cómo las tecnologías disruptivas se están convirtiendo en herramientas clave de disuasión estratégica, más allá de su aplicación directa en combate. Analizaremos no solo sus características técnicas, sino su impacto doctrinal, psicológico y político, así como los requisitos que una nación debe reunir para integrar

dichas tecnologías en su arquitectura de defensa de forma creíble y sostenida.

LA TRANSFORMACIÓN DEL PARADIGMA DISUASORIO

Durante gran parte del siglo XX, la disuasión se basó en un principio simple: quien poseía la capacidad de infligir un daño inaceptable evitaba ser atacado. Este concepto, especialmente vinculado a la lógica nuclear de la Guerra Fría, se expresó mediante fórmulas como la Destrucción Mutua Asegurada (MAD) y el equilibrio del terror. Los arsenales estratégicos garantizaban que ningún actor racional iniciara un conflicto que no pudiera controlar: una disuasión basada en la masa, la escala y la visibilidad.

Sin embargo, el escenario actual ha mutado. Los conflictos interestatales tradicionales han dado paso a amenazas híbridas, cibernéticas e informacionales, difíciles de atribuir y diseñadas para operar por debajo del umbral del conflicto armado. En este contexto, la disuasión clásica pierde eficacia. Ya no se busca tanto la confrontación directa como la erosión gradual del adversario mediante acciones encubiertas, asimétricas o tecnológicamente sofisticadas.

La disuasión moderna se apoya menos en la capacidad destructiva y más en la superioridad tecnológica y cognitiva. Es una disuasión basada en imposibilitar, anticipar y paralizar, generando entornos operativos donde cualquier acción hostil resulte incierta, costosa o ineficaz incluso antes de ejecutarse.

Un cambio clave es el paso de una lógica monodominio (mar, tierra, aire) a una lógica multidominio, donde el ciberespacio, el espectro electromagnético y el espacio ultraterrestre adquieren un peso operativo comparable a los entornos físicos. Dominar el flujo de información, las comunicaciones seguras y el procesamiento acelerado de datos impone una asimetría disuasoria de gran alcance.

Conceptos como el *information advantage*, la velocidad de decisión o la resiliencia sistémica sustituyen a las viejas métricas de tanques o fragatas. Anticipar y responder antes que el adversario, apoyándose en

herramientas como la inteligencia artificial o la computación en el borde, se convierte en una ventaja decisiva.

Joseph Nye, en su teoría del *smart power*, ya anticipaba este tránsito hacia formas más sofisticadas de influencia estratégica: la combinación de capacidades duras (militares) con blandas (tecnológicas e informacionales) crea una disuasión difusa pero más robusta. Muchas de las acciones más efectivas hoy se producen en laboratorios de I+D, centros de mando cibernético o ejercicios de interoperabilidad avanzada, lejos del campo de batalla visible.

La transformación alcanza también al perfil del actor disuasor. Ya no son solo los Estados los que poseen capacidad estratégica: empresas tecnológicas, redes de innovación, consorcios industriales e incluso plataformas digitales modifican el equilibrio de poder. Esto obliga a repensar la disuasión como un fenómeno de ecosistema, donde la base industrial, la ciencia, la protección de datos y la soberanía digital son tan relevantes como el despliegue militar.

En este nuevo contexto, se consolida una disuasión ambigua y anticipatoria, centrada en proyectar incertidumbre sobre el coste de atacar más que en amenazar con un castigo explícito. Demostraciones tecnológicas limitadas —pruebas de comunicaciones cuánticas, ejercicios con enjambres autónomos, operaciones cibernéticas reversibles— pueden tener un efecto disuasorio más potente que la exhibición clásica de fuerza.

Asimismo, la reciente interrupción del suministro eléctrico en España ha puesto de relieve otra dimensión crítica: la necesidad de garantizar la resiliencia de las infraestructuras de mando y control frente a fallos sistémicos. En la era tecnológica, disuadir no es solo disponer de medios avanzados, sino asegurar su operatividad continua incluso en escenarios degradados. La resiliencia tecnológica, entendida como la capacidad para mantener funciones esenciales frente a contingencias naturales o provocadas, se convierte así en un factor de disuasión clave: proyecta la imagen de un sistema robusto e inalterable, capaz de resistir ataques indirectos o disrupciones críticas.

DISUASIÓN COGNITIVA Y VENTAJA DECISIONAL

Una de las transformaciones más significativas en la disuasión moderna es el salto del dominio físico al cognitivo. Ya no se trata solo de tener más medios, sino de pensar, decidir y actuar más rápido que el adversario, imponiéndole un ritmo que no puede seguir. La ventaja está en la velocidad y precisión con la que se transforma la información en acción.

En este contexto, la inteligencia artificial (IA) se ha convertido en un multiplicador estratégico clave. Aplicada a la defensa, permite extraer conocimiento útil a partir de enormes volúmenes de datos —provenientes de sensores, satélites, redes sociales o inteligencia humana y abierta (HUMINT/OSINT)— y traducirlo en decisiones operativas con una rapidez imposible para un ser humano.

El ciclo OODA (Observar–Orientar–Decidir–Actuar), formulado por John Boyd, resume bien esta lógica. Con IA, ese ciclo se acorta drásticamente: sistemas autónomos pueden observar su entorno, reinterpretarlo sobre la marcha, tomar decisiones y actuar en tiempo real. Esa velocidad crea una asimetría que desincentiva al adversario: si sabe que irá siempre un paso por detrás, pensará dos veces antes de actuar.

Un buen ejemplo es el uso de IA en sistemas de alerta temprana. Al combinar imágenes de satélite, señales electrónicas, patrones meteorológicos o movimientos logísticos, se puede anticipar una amenaza antes de que se materialice. No solo se gana capacidad de respuesta: se influye en el comportamiento enemigo antes de que tome la iniciativa.

La IA también mejora la planificación táctica, la logística, la gestión de recursos y la selección de objetivos, dando lugar a lo que llamamos inteligencia aumentada: decisiones humanas reforzadas por análisis precisos. Desde la perspectiva disuasoria, esto significa dejar claro que cualquier acción enemiga será detectada, comprendida y neutralizada a tiempo.

Esta ventaja se amplifica aún más con el procesamiento en el borde (edge computing), que permite a sensores y plataformas procesar

datos directamente sobre el terreno, sin depender de redes centrales. Esto mejora la autonomía táctica, la resiliencia frente a ciberataques y la capacidad de respuesta. Un enjambre de drones con inteligencia distribuida no solo actúa con eficacia: desconcierta por su imprevisibilidad.

Además, la disuasión cognitiva no se limita al campo operativo. El control del espacio informativo —gestionar percepciones, contrarrestar narrativas, detectar desinformación o incluso generar mensajes automáticos estratégicos— forma parte del nuevo campo de batalla. Y ahí, la IA vuelve a ser decisiva.

Todo ello tiene un fuerte impacto psicológico. Si el enemigo percibe que te anticipas a sus movimientos, que ves lo que él no ve y actúas antes de que decida, pierde la iniciativa. Esa parálisis es en sí misma un efecto disuasorio.

Pero esta forma de superioridad no se improvisa. Exige acceso soberano a datos, talento especializado, capacidad de entrenar modelos propios, infraestructuras digitales seguras y un marco normativo que permita avanzar con agilidad. No basta con comprar tecnología: hay que construir un ecosistema tecnológico nacional, resiliente y actualizado.

En definitiva, la IA no solo cambia la forma de combatir: cambia la forma de disuadir. En un entorno donde quien decide antes domina el juego, disuadir es demostrar que siempre llegarás primero.

CAPACIDADES TECNOLÓGICAS CLAVE PARA LA DISUASIÓN

Comunicaciones cuánticas: la inviolabilidad como arma estratégica

En un entorno donde la información es tan crítica como el combustible o las municiones, proteger su integridad se convierte en una prioridad estratégica. La comunicación cuántica, y en particular la criptografía cuántica, ofrece una solución inédita: establecer canales absolutamente seguros, no por la complejidad del cifrado, sino por las propias leyes de la física.

Esta tecnología se basa en un principio esencial de la mecánica cuántica: no se puede observar un sistema cuántico sin alterarlo. En telecomunicaciones, esto implica que cualquier intento de interceptar el canal modifica automáticamente el estado de las partículas (normalmente fotones), alertando a los interlocutores legítimos. Este fenómeno es la base de la distribución cuántica de claves (QKD), que permite compartir claves criptográficas de forma inviolable.

La disuasión que ofrecen estas comunicaciones nace de su seguridad inherente. Un adversario que sabe que no puede interceptar, descifrar ni manipular sin ser detectado, se enfrenta a un cerrojo invisible que reduce su margen de maniobra. Es especialmente útil en escenarios donde las redes tradicionales pueden quedar expuestas a ciberataques, interferencias electromagnéticas o sabotajes.

Además, su despliegue tiene un claro valor estratégico: un sistema de defensa que opera con tecnología cuántica transmite un mensaje inequívoco —«no penetrarás sin consecuencias»— con el mismo efecto disuasorio que el despliegue de una flota o un escudo antimisiles.

Estas tecnologías ya se están adaptando a plataformas móviles como buques, satélites o vehículos blindados, gracias a los avances en miniaturización de sensores, fuentes de fotones y sistemas ópticos. Su integración permitirá comunicaciones seguras incluso en movimiento.

Desde la perspectiva disuasoria, no se trata solo de proteger datos, sino de imponer una asimetría tecnológica que frustre la planificación enemiga. Cuando el flujo de información se vuelve inaccesible, el adversario pierde iniciativa. Esa incertidumbre es, en sí misma, disuasión.

Por tanto, invertir en comunicaciones cuánticas no es solo reforzar la ciberseguridad: es construir un pilar estructural de la estrategia nacional de disuasión tecnológica. Como lo fueron en su día el radar o el GPS, la criptografía cuántica está llamada a ser una infraestructura crítica para operar con ventaja en el nuevo dominio informacional.

Sistemas autónomos y enjambres inteligentes: disuasión asimétrica por saturación

Una de las transformaciones más significativas del panorama militar contemporáneo es la irrupción de sistemas autónomos y, especialmente, de su empleo coordinado en enjambres inteligentes. Estas capacidades suponen una alteración profunda del equilibrio coste-eficacia y ofrecen nuevas formas de disuasión, especialmente útiles en escenarios de competencia entre actores asimétricos o frente a adversarios convencionales más rígidos.

Los sistemas autónomos abarcan desde drones aéreos y submarinos hasta vehículos terrestres, sensores móviles o plataformas cibernéticas, diseñados para operar con distintos grados de independencia. Su inteligencia reside en algoritmos que interpretan el entorno, toman decisiones y ejecutan misiones sin intervención constante. Esta autonomía, combinada con la coordinación entre plataformas, da lugar al enjambre.

Un enjambre no es solo un grupo de drones. Es un sistema que comparte información, ajusta su comportamiento colectivo y adapta su táctica en tiempo real, guiado por una inteligencia distribuida. Este despliegue genera una amenaza no lineal: con recursos limitados, puede saturar defensas, desorganizar al adversario y ejecutar maniobras difíciles de prever o neutralizar.

Desde el punto de vista disuasorio, los enjambres alteran dos factores clave:

- **Desproporcionalidad de coste**: destruirlos puede requerir recursos mucho más caros que su despliegue, lo que genera una disuasión por desgaste anticipado.
- **Imprevisibilidad táctica**: su comportamiento variable impone una carga cognitiva al enemigo, que no puede anticipar sus movimientos ni desarrollar doctrinas defensivas fijas, generando parálisis operativa.

Además del impacto ofensivo, refuerzan la disuasión defensiva. Pueden actuar como guardias perimetrales inteligentes, detectando y reaccionando ante amenazas en segundos. En un mundo donde la velocidad es ventaja, esta capacidad genera respeto en el agresor.

También permiten respuestas escalables y reversibles. Un enjambre puede reprogramarse o retirarse sin causar daños irreversibles, lo que refuerza su utilidad como herramienta de disuasión ambigua: muestra capacidades sin comprometerse a usarlas, sembrando dudas en el cálculo enemigo.

Aun con sus retos éticos, legales y doctrinales —como el control humano sobre la fuerza o la trazabilidad de decisiones—, su potencial estratégico sigue siendo alto. Enfrentar sistemas autónomos ofensivos conlleva incertidumbre y riesgo.

Finalmente, los enjambres no exigen grandes inversiones, sino ecosistemas de innovación con acceso a talento en inteligencia artificial, electrónica, sensores y comunicaciones. Esto los convierte en una opción especialmente valiosa para potencias medias que desean proyectar influencia sin depender de grandes plataformas.

Ciberdefensa ofensiva y guerra electrónica: disuasión por negación e incertidumbre

La superioridad en el espectro electromagnético y el ciberespacio es hoy uno de los pilares clave de la disuasión tecnológica. A diferencia de los dominios clásicos —mar, tierra, aire—, donde el despliegue de medios es visible y medible, el dominio cibernético y electromagnético opera en la sombra, con acciones difíciles de atribuir y anticipar. Por eso su impacto disuasorio puede ser devastador: basta con sembrar dudas sobre la fiabilidad de los sistemas del adversario para alterar su planificación y percepción de control.

La **ciberdefensa ofensiva** no solo protege infraestructuras digitales. También permite penetrar, degradar o inutilizar sistemas enemigos sin contacto físico. Incluye sabotajes logísticos, colapso de redes de

mando y control, alteración de sensores, desvío de sistemas de navegación o manipulación informativa con fines psicológicos.

Aquí, la disuasión opera por negación: si el enemigo cree que sus sistemas pueden quedar fuera de servicio —incluso sin saber cómo ni cuándo—, su agresión pierde sentido. A veces, basta la sospecha de una red comprometida para generar parálisis.

La **guerra electrónica** ha cobrado también un nuevo protagonismo. Su propósito: interferir, degradar o explotar los sistemas del enemigo. Desde supresión de radares hasta manipulación de señales GPS, su impacto en las operaciones es directo y creciente.

Desde una óptica disuasoria, dominar el espectro impone incertidumbre al adversario: si no puede confiar en sus sensores o comunicaciones, pierde capacidad operativa. La supervivencia táctica depende tanto del control electromagnético como de la protección física.

La sinergia entre ciberdefensa y guerra electrónica refuerza este efecto. Atacar cibernéticamente y luego cegar el sistema por vía electrónica —o viceversa— genera amenazas multidominio que fuerzan al enemigo a invertir en protección, elevando así el umbral disuasorio.

Desde el punto de vista doctrinal, el enfoque más eficaz en ciberdefensa y guerra electrónica combina tres pilares fundamentales:

- **Resiliencia preventiva**: implica diseñar sistemas que puedan seguir funcionando incluso cuando están siendo atacados o parcialmente dañados. Esto se logra mediante redes distribuidas —que no dependen de un único punto de fallo—, el uso de sistemas autónomos capaces de adaptarse por sí mismos y la capacidad de operar en modo degradado, es decir, manteniendo funciones críticas, aunque parte del sistema esté comprometido. Esta resiliencia no solo mejora la defensa, sino que transmite al adversario que cualquier ataque tendrá un efecto limitado, reduciendo así su incentivo para actuar.
- **Capacidad ofensiva creíble**: significa no solo tener medios para atacar, sino demostrar que se está dispuesto y preparado para usarlos si es necesario. La disuasión no se basa únicamente en

castigos futuros, sino también en la amenaza de una respuesta inmediata y efectiva que neutralice al agresor antes de que cumpla su objetivo. Esta capacidad ofensiva sirve para sembrar dudas en la mente del enemigo: cualquier intento puede volverse en su contra rápidamente.

• **Ambigüedad estratégica**: consiste en no revelar completamente las propias capacidades. Mantener un grado de opacidad tecnológica genera incertidumbre en el adversario, que no puede evaluar con precisión ni las capacidades reales ni las líneas rojas del oponente. Esta ambigüedad, bien gestionada, actúa como una forma sutil pero potente de disuasión: el enemigo no se atreve a actuar si no sabe con qué se enfrentará.

En conjunto, la ciberdefensa ofensiva y la guerra electrónica permiten ejercer disuasión sin necesidad de hacer ruido ni mostrar fuerza de manera visible. Son instrumentos silenciosos, invisibles, pero efectivos: basta con generar sospechas, crear precedentes o realizar una demostración puntual para condicionar el comportamiento del adversario, sin necesidad de desplegar tropas ni disparar un solo proyectil.

Tecnología fotónica: velocidad, inmunidad y disuasión invisible

La fotónica es hoy una de las tecnologías emergentes más prometedoras en el ámbito de la defensa. Basada en el uso de la luz en lugar de electrones para transmitir, procesar y detectar información, no es simplemente una mejora de lo existente: es un salto cualitativo. Permite sistemas mucho más rápidos, compactos, resistentes y difíciles de interceptar, algo que cambia las reglas del juego cuando hablamos de disuasión tecnológica.

Una de sus mayores bazas es la velocidad. La fotónica opera a escalas ópticas, con anchos de banda que la electrónica convencional ni se acerca a alcanzar. Esto significa comunicaciones ultra rápidas, sensores que detectan amenazas antes que nadie, y sistemas capaces de procesar datos en tiempo real. En un mundo donde quien actúa

primero impone las condiciones, acortar los ciclos de reacción puede ser la diferencia entre dominar o ser dominado. Tener redes ópticas, nodos de procesamiento fotónico o sistemas distribuidos en plataformas militares no solo proporciona eficacia: disuade a quien se plantee un ataque, sabiendo que su ventana de oportunidad será mínima.

Otra virtud clave de la fotónica es su inmunidad natural a las interferencias electromagnéticas. Mientras los sistemas electrónicos pueden ser cegados o manipulados mediante técnicas de guerra electrónica, los enlaces ópticos son resistentes al «jamming» y al «spoofing». Esto convierte a la arquitectura fotónica en una auténtica fortaleza invisible. Para el adversario, enfrentarse a una red militar fotónica significa asumir que sus herramientas habituales de ataque pueden no funcionar, lo que añade otra capa de disuasión tecnológica.

El abanico de aplicaciones de la fotónica es amplio. Por ejemplo, permite establecer comunicaciones ópticas en espacio libre entre buques, satélites o drones, difíciles de interceptar, lo que las hace ideales para entornos sensibles. También puede utilizarse en sensores integrados en las propias estructuras de aviones o barcos, capaces de detectar vibraciones, cambios de temperatura o deformaciones casi al instante. En navegación, los giróscopos basados en tecnología fotónica permiten una navegación inercial de gran precisión, sin depender del GPS, lo que resulta muy útil frente a intentos de bloqueo o suplantación de señal, o incluso en navegaciones submarinas. Incluso en guerra electrónica, la fotónica ofrece soluciones innovadoras, como el uso de láseres o filtros ópticos para manipular señales enemigas, todo ello con dispositivos pequeños, silenciosos y de bajo consumo.

Pero quizá el aspecto más interesante de la fotónica en clave disuasoria es su asimetría. Mientras la mayoría de capacidades electrónicas son conocidas o, al menos, previsibles, el grado de sofisticación que puede alcanzar un sistema fotónico —sobre todo si integra múltiples funcionalidades en un solo chip— resulta mucho más difícil de evaluar

desde fuera. Esa incertidumbre juega a favor del defensor: el adversario tenderá a sobrestimar nuestras capacidades, dudará, se frenará. En este sentido, la fotónica no solo disuade por lo que hace, sino también por lo que sugiere que podría hacer.

Además, los sistemas fotónicos permiten mantener un perfil extremadamente bajo: ni emisiones térmicas, ni señales electromagnéticas detectables. Esto refuerza la supervivencia de plataformas y sensores y desestabiliza psicológicamente al agresor, que ya no puede confiar en sus propios sistemas de detección.

En resumen, la fotónica no es solo una tecnología avanzada: es una herramienta estratégica que refuerza la disuasión desde la velocidad, la invisibilidad y la incertidumbre. Y lo mejor es que apenas estamos empezando a explorar todo su potencial.

Nuevas tecnologías que refuerzan la disuasión: lo que viene

Más allá de las capacidades ya desplegadas en inteligencia artificial, fotónica o ciberdefensa, existe un conjunto de tecnologías emergentes que, aunque todavía están en fase de desarrollo o implantación inicial, poseen un potencial transformador inmenso. Su sola mención en los entornos estratégicos genera ya efectos disuasorios: no porque estén listas para el combate, sino porque obligan al adversario a preguntarse qué capacidades reales tiene el otro bando, y si está preparado para afrontarlas.

Una de las más relevantes es la **computación cuántica**. A diferencia de los ordenadores actuales, que trabajan con bits (unos o ceros), los ordenadores cuánticos usan qubits, que pueden representar múltiples estados a la vez. Esto les permite realizar operaciones extremadamente complejas en tiempos muy reducidos. Aplicado a la defensa, significa que podrían romper los sistemas de cifrado tradicionales, optimizar rutas logísticas en segundos, simular escenarios de conflicto con enorme precisión o gestionar grandes volúmenes de datos operativos en tiempo real. Aunque todavía se trata de una tecnología incipiente, su mera perspectiva obliga a

repensar cómo proteger los sistemas actuales. Disuade, no por lo que puede hacer hoy, sino por lo que se sabe que podrá hacer muy pronto.

Otra tecnología emergente con alto valor disuasorio es la de las **armas de energía dirigida**, como los láseres de alta potencia o las microondas. Son capaces de inutilizar drones, misiles o sensores sin proyectiles explosivos, actuando a la velocidad de la luz, sin dejar huella visible y con un coste por disparo muy bajo. Esto permite proteger instalaciones o plataformas de forma silenciosa, pero eficaz. Para un adversario, saber que hay un sistema capaz de neutralizar una amenaza sin previo aviso y con total precisión impone una cautela inmediata.

En el ámbito de la seguridad interna, la **biometría avanzada y la identidad digital soberana** son claves. Permiten verificar de forma inequívoca quién accede a los sistemas, detectar intentos de suplantación o sabotaje, y blindar los entornos de decisión ante intrusiones híbridas. La disuasión aquí no se ejerce hacia fuera, sino hacia dentro: mostrando que es inútil intentar infiltrar o manipular un sistema cerrado y vigilado desde dentro.

También destacan los **procesadores neuromórficos**, que imitan el funcionamiento del cerebro humano. Aplicados a plataformas militares o sistemas autónomos, permiten que aprendan del entorno, se adapten a cambios imprevistos y mejoren su rendimiento de forma autónoma. Es decir, pueden volverse más eficaces con el tiempo y durante el propio combate. Para un adversario, esto representa un reto difícil de anticipar y planificar.

En última instancia, lo más poderoso de estas tecnologías no está en su capacidad individual, sino en su **integración**. Cuando se combinan sistemas autónomos, sensores inteligentes, inteligencia artificial, redes seguras y armas de energía dirigida en un solo ecosistema operativo, se genera un entorno altamente resistente, anticipativo y eficaz. Es esa capacidad de respuesta inteligente y coordinada la que mejor disuade: porque muestra que la tecnología está al servicio de una estrategia superior.

DISUASIÓN DEMOSTRATIVA Y DISUASIÓN AMBIGUA: EL ARTE DE SEMBRAR INCERTIDUMBRE

En la lógica clásica de la disuasión nuclear, la clave era la credibilidad: se disuade si el adversario cree que la amenaza es real, que la capacidad existe y que el líder está dispuesto a usarla. En el mundo de las tecnologías disruptivas, esa lógica se matiza: ya no se trata únicamente de mostrar una capacidad o de mantenerla oculta, sino de gestionar estratégicamente lo que el adversario sabe, cree saber o intuye.

Este enfoque da lugar a dos modalidades complementarias de disuasión tecnológica: **la disuasión demostrativa** y **la disuasión ambigua.** Ambas forman parte de una estrategia de comunicación implícita que busca alterar el cálculo de riesgos del adversario sin necesidad de recurrir a la confrontación abierta.

Disuasión demostrativa: mostrar lo justo, en el momento adecuado

La disuasión demostrativa consiste, en esencia, en mostrar lo justo en el momento adecuado. Se trata de enseñar determinadas capacidades tecnológicas o doctrinales de forma medida, calculada, sin necesidad de poner todas las cartas sobre la mesa. El objetivo no es revelar el arsenal completo, sino dejar ver aquellas piezas que refuerzan una narrativa clara: «tenemos medios avanzados, difíciles de igualar, y estamos preparados». Esa imagen proyectada de superioridad o invulnerabilidad es, en sí misma, una poderosa herramienta disuasoria.

Este tipo de demostración se concreta en gestos cuidadosamente diseñados: una prueba pública de un arma hipersónica o de un láser de defensa; el despliegue visible de sistemas fotónicos o estaciones de comunicaciones cuánticas en maniobras internacionales; incluso un simulacro cibernético que se realiza, convenientemente, ante la presencia de observadores extranjeros. También cuentan las publicaciones científicas o industriales que, sin entrar en detalles sensibles,

revelan avances significativos y dejan entrever una capacidad tecnológica muy avanzada.

Estas acciones, más allá de su contenido técnico, cumplen una función estratégica. Refuerzan la percepción de que enfrentarse a quien posee estas capacidades sería extremadamente costoso, quizá incluso inútil. Y no solo disuaden al adversario externo: también fortalecen la moral interna, cohesionan a las fuerzas armadas, y envían un mensaje político nítido de compromiso con la innovación y la modernización.

Disuasión ambigua: sembrar dudas estratégicas

A diferencia de la disuasión demostrativa, que juega con lo visible, la disuasión ambigua se basa en todo lo contrario: en la gestión deliberada del desconocimiento. No se trata de enseñar músculo, sino de sembrar dudas. ¿Qué capacidades tienen realmente? ¿Hasta dónde están dispuestos a llegar? ¿Y qué ocurriría si se les desafía? Es una estrategia que juega con la percepción del adversario, con su miedo a lo que no puede ver ni calcular con certeza.

Este tipo de disuasión funciona especialmente bien cuando se apoya en tecnologías invisibles o poco comprensibles: sistemas cibernéticos que pueden activarse sin dejar rastro, algoritmos de inteligencia artificial que operan por debajo del umbral de detección humana, desarrollos cuánticos aún secretos o técnicas de guerra electrónica que manipulan el entorno electromagnético sin que nadie lo perciba. Son capacidades difíciles de detectar y, precisamente por eso, extremadamente eficaces para generar incertidumbre.

A lo largo de la historia, varios actores han utilizado este tipo de ambigüedad estratégica como herramienta de disuasión. Israel, por ejemplo, nunca ha confirmado su capacidad nuclear, pero tampoco la ha negado, lo cual le ha permitido mantener un equilibrio disuasorio sin necesidad de declarar nada abiertamente. Un caso aún más ilustrativo —aunque con consecuencias trágicas— fue el de Saddam Hussein. A sabiendas de que no contaba con un arsenal de

armas de destrucción masiva, optó por mantener la ambigüedad, alimentando la idea de que sí las tenía, como forma de disuadir tanto a Irán como a otras potencias. El problema es que, en su caso, esa ambigüedad fue interpretada como una amenaza inaceptable, y acabó desencadenando la invasión de 2003. Un recordatorio de que la disuasión ambigua, aunque poderosa, debe manejarse con gran precisión.

Porque ahí radica su fuerza, pero también su riesgo: en dejar al adversario sin certezas. Si no sabe con qué se enfrenta, tenderá a sobrestimar nuestras capacidades, y eso, en muchos casos, basta para disuadirle. Por eso, este tipo de estrategia suele combinarse con campañas de influencia y operaciones psicológicas que refuerzan esa percepción de amenaza difusa pero real. Al final, la ambigüedad bien manejada puede condicionar el comportamiento del enemigo sin haber desplegado un solo sistema. Basta con que él piense que podríamos hacerlo.

El equilibrio entre lo visible y lo invisible

La combinación de disuasión demostrativa y ambigua exige un equilibrio fino. Mostrar demasiado puede provocar una carrera armamentística o perder el factor sorpresa; mostrar poco puede llevar al adversario a subestimar nuestras capacidades. Por eso, los estrategas modernos deben gestionar el conocimiento como parte del arsenal disuasorio: decidir qué se muestra, qué se sugiere y qué se silencia es tan importante como el propio desarrollo tecnológico.

Además, este enfoque tiene un impacto en la narrativa política: cuando un país demuestra capacidades tecnológicas avanzadas y mantiene un entorno de innovación visible pero parcialmente opaco, refuerza su imagen internacional como actor serio, competente y con voluntad estratégica. Esto disuade no solo a actores estatales hostiles, sino también a posibles interferencias tecnológicas, ataques cibernéticos, chantajes industriales o campañas de desinformación.

En definitiva, la disuasión en el siglo XXI no consiste solo en poseer medios, sino en proyectar intenciones, capacidades y límites de forma ambigua, calculada y eficaz. En este tablero estratégico, la percepción lo es todo: quien logra gestionar el conocimiento, la sorpresa y la duda, impone su ritmo, incluso antes de que empiece el conflicto.

REQUISITOS PARA UNA DISUASIÓN TECNOLÓGICA EFECTIVA: MÁS ALLÁ DEL ARTILUGIO

La disuasión tecnológica no es algo que pueda improvisarse. No basta con adquirir sistemas avanzados o hacer gala de prototipos deslumbrantes: se trata de construir un ecosistema robusto, coherente y sostenible, capaz de transformar el potencial tecnológico en ventaja operativa real. Y para eso, hay que cimentar bien los pilares sobre los que se sostiene esa capacidad disuasoria.

Una base industrial, científica y tecnológica soberana

El primer paso es tener una base propia, sólida y bien conectada entre industria, ciencia y tecnología. Sin esa base, cualquier estrategia de disuasión queda expuesta a dependencias externas, cuellos de botella logísticos o vulnerabilidades críticas. Hablamos de contar con empresas tecnológicas que trabajen con visión de largo plazo, centros de investigación que comprendan las necesidades operativas reales, redes de universidades y startups que mantengan vivo el pulso de la innovación, y capacidad para producir y mantener componentes clave sin depender de terceros. En resumen, no se trata de comprar tecnología, sino de dominarla. Y un país que no domina su tecnología no puede disuadir con credibilidad.

Integración doctrinal y operativa

La tecnología, por sí sola, no disuade. Necesita estar integrada de verdad en la forma de operar, en la cultura de las Fuerzas Armadas, en los procedimientos y en la toma de decisiones. Una IA sin una doctrina

detrás no pasa de ser un procesador potente; un enjambre sin concepto de empleo sigue siendo un grupo de drones sin dirección. Por eso es tan importante revisar y adaptar las doctrinas con regularidad, ensayar nuevas formas de hacer las cosas, y contar con equipos operativos desde el principio del desarrollo tecnológico. Solo así se consigue que la tecnología piense y actúe como parte del sistema, sin romper la interoperabilidad ni generar desajustes en el campo de batalla. La disuasión real nace de esa integración invisible que hace que todo funcione como un bloque coherente y ágil.

Talento especializado y liderazgo con visión

La tecnología sin personas no tiene rumbo. La disuasión tecnológica sostenida requiere talento humano del más alto nivel: ingenieros, sí, pero también estrategas, operadores, innovadores y líderes que entiendan el impacto real de cada nueva capacidad. No se trata solo de saber programar, sino de comprender cómo una herramienta digital transforma un sistema de mando, una operación conjunta o una lógica de combate. Para lograrlo, es fundamental atraer, formar y retener a ese talento, crear puentes entre la academia, la industria y la defensa, y dotar de visión tecnológica a quienes toman decisiones. Porque sin personas capacitadas y comprometidas, la tecnología se estanca. Y sin evolución, no hay poder real, ni mucho menos disuasión.

Inversión sostenida y enfoque estratégico

Ninguna tecnología disruptiva madura de la noche a la mañana. Innovar en defensa exige tiempo, constancia y visión de futuro. Por eso es vital contar con una estrategia nacional que alinee ciencia, seguridad, industria y defensa en una misma dirección. Los programas de I+D deben tener continuidad más allá de los vaivenes políticos, los mecanismos de gobernanza deben conectar la innovación con las necesidades reales de capacidades, y hay que saber aprovechar los instrumentos de cooperación europea para escalar proyectos que, de

forma aislada, serían inviables. La disuasión se construye con coherencia y constancia, no con anuncios puntuales.

Un marco normativo y ético a la altura de los desafíos

La disuasión también necesita legitimidad. Las tecnologías emergentes abren debates complejos: desde el uso de sistemas autónomos letales hasta la ciberdefensa ofensiva o la inteligencia artificial en decisiones críticas. Si no se abordan con claridad, pueden generar dudas internas o incluso rechazo social. Por eso, hay que avanzar hacia marcos éticos sólidos, legislación nacional que proteja la innovación sin ahogarla, acuerdos internacionales que eviten vacíos legales, y un grado razonable de transparencia que inspire confianza sin comprometer la seguridad. La tecnología no puede disuadir si no está alineada con nuestros valores y principios democráticos.

En definitiva, la disuasión tecnológica no se compra ni se hereda: se construye, paso a paso, con visión a largo plazo, con voluntad política y con una cultura operativa que sepa aprovechar el cambio. Porque en este nuevo tablero global, quien no disuade acaba obedeciendo.

ESPAÑA ANTE EL DESAFÍO: UNA OPORTUNIDAD PARA EL LIDERAZGO

Vivimos un momento clave. En un mundo marcado por la competencia tecnológica, la fragmentación geopolítica y la necesidad urgente de garantizar una autonomía estratégica europea real, España tiene delante una oportunidad que no se presenta todos los días. Las tecnologías disruptivas no solo están cambiando la forma en que se concibe el poder militar, sino que están redibujando el mapa de influencia entre países. En este nuevo terreno de juego, la disuasión tecnológica se ha convertido en una palanca esencial para proyectar soberanía, relevancia internacional y seguridad duradera.

A diferencia de revoluciones anteriores, España no parte de cero. Al contrario: ya contamos con una base industrial y científica sólida

en ámbitos punteros como la fotónica, la optrónica, la guerra electrónica, la ciberseguridad, las comunicaciones seguras o los sensores inteligentes. Empresas como Navantia, Grupo Oesía, Indra, Sener o GMV —junto a una red creciente de pymes, startups y centros tecnológicos— forman un ecosistema capaz de generar capacidades tecnológicas propias con potencial real para reforzar nuestra capacidad de disuasión. Y aún más si se conecta con las iniciativas y programas que Europa está desplegando.

A nivel institucional, no son pocas las apuestas que ya están en marcha. España participa activamente en proyectos de enorme calado como el NGWS/FCAS, que definirá el futuro del combate aéreo; las fragatas F110 y los submarinos S-80, que incorporan soluciones de vanguardia en sensores, mando y control; el programa nacional de espacio o la creación de unidades ciberconjuntas. Todos ellos no son solo plataformas militares: son vectores de innovación, tanto tecnológica como doctrinal, y tienen la capacidad de proyectar disuasión creíble en nuestro entorno inmediato y dentro del marco de seguridad europeo.

Pero todo esto necesita algo más: una estrategia clara, coherente y sostenida en el tiempo. No basta con participar en programas o captar financiación puntual. Hace falta construir un modelo nacional que conecte inversión, talento, capacidades y visión. Un modelo que se base en apostar de verdad por las tecnologías disruptivas, en integrarlas en la operativa real de nuestras Fuerzas Armadas, en formar y retener a quienes van a liderar ese cambio, y en reforzar el control nacional sobre las tecnologías críticas que definen nuestra soberanía.

Si España consigue articular este modelo con decisión y ambición, tiene ante sí la posibilidad real de ejercer un cierto papel de liderazgo en el campo de la disuasión tecnológica. Y no solo dentro del marco europeo, sino como un actor que sabe defender la paz a través de la innovación, que garantiza la seguridad desde la anticipación y que proyecta influencia desde la tecnología, no desde la dependencia.

En definitiva, en un mundo donde el que no innova queda relegado o expuesto, España tiene el talento, los recursos y la oportunidad de

convertirse en un referente disuasorio creíble. Pero debe dar el paso. No con palabras, sino con visión de Estado.

CONCLUSIÓN: DISUADIR PARA EVITAR, DOMINAR PARA NO COMBATIR

Estamos viviendo un cambio de época. Durante décadas, la disuasión se entendió como la capacidad de responder con fuerza abrumadora a una agresión. Hoy, en cambio, se trata de algo más sutil y, al mismo tiempo, más sofisticado: anticipar, neutralizar y hacer que el adversario desista antes siquiera de actuar. Ya no se mide el poder por el número de tanques o fragatas, sino por cuánta inteligencia tecnológica, resiliencia y capacidad de decisión rápida puede desplegar una nación en el momento justo.

En este nuevo escenario, las tecnologías disruptivas no son meros instrumentos tácticos. Son herramientas estratégicas que permiten proyectar voluntad, generar incertidumbre y controlar el entorno sin necesidad de recurrir a la violencia. Disuadir, hoy, no es amenazar con el castigo, sino hacer que el adversario piense que no tiene nada que ganar y mucho que perder.

Pero para que eso funcione, no basta con comprar tecnología o acumular dispositivos avanzados. Hace falta algo más profundo: una cultura de innovación real, una base industrial y científica robusta, un ecosistema digital seguro, y, sobre todo, una visión estratégica sostenida. Porque la credibilidad no se improvisa: se construye con coherencia, con preparación y con voluntad política. El futuro no se adivina: se diseña.

España —y Europa en su conjunto— tiene una oportunidad histórica. No para competir en cantidad, sino para destacar en calidad. No para replicar lo que hacen otros, sino para integrar capacidades de forma inteligente, flexible y soberana. Si somos capaces de combinar nuestro talento, nuestra industria y una narrativa clara de propósito, podremos convertirnos en un actor disuasorio relevante, capaz de garantizar su seguridad y su voz en el mundo.

Lo dijo Clausewitz: «la guerra es la continuación de la política por otros medios». Hoy podríamos decir que la tecnología es la continuación de la disuasión. Y quien domina la tecnología, domina el futuro. No para imponerlo por la fuerza, sino precisamente para evitar que la fuerza tenga que usarse. Porque en el fondo, disuadir es eso: evitar el conflicto antes de que empiece.