VISIÓN CONJUNTA

FACULTAD MILITAR CONJUNTA

Año 17 . Nº 33 . Diciembre 2025

FMC
Facultad Militar Conjunta

TECNOLOGÍA

FRICCIÓN Y C4ISR EN EL SIGLO XXI

Por **Santiago Luis Aversa**

INSTITUTO DE INTELIGENCIA DE LAS FUERZAS ARMADAS

ESCUELA SUPERIOR DE GUERRA CONJUNTA DE LAS FUERZAS ARMADAS

INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS

FMC
Facultad Militar Conjunta

AUTORIDADES

VICERRECTOR DE EDUCACIÓN MILITAR CONJUNTA
General de Brigada Horacio Luis Alonso

DECANO
Coronel (R) VGM Alberto V. Aparicio

DIRECTORES DE LAS SEDES EDUCATIVAS UNIVERSITARIAS

Instituto de Inteligencia de las FFAA
Comodoro
Pablo Gabriel Falzone

Escuela Superior de Guerra Conjunta de las FFAA
Comodoro de Marina
Eduardo Ignacio Llambí

Instituto de Ciberdefensa de las FFAA
Coronel
Néstor Antonio Pontoni

STAFF

DIRECTOR EDITORIAL
Mónica M. Boretto

SECRETARIA DE REDACCIÓN
Victoria Álvarez

DISEÑO
Juan Gallelli

EDITOR
Facultad Militar Conjunta

PROPIETARIO
Estado Mayor Conjunto
de las Fuerzas Armadas

EUMIC
Editorial Universitaria de la Facultad Militar Conjunta

ISSN: 1852-8619

Correo electrónico:
publicaciones@fmc.undef.edu.ar

Visión Conjunta es una publicación de divulgación de temas militares iniciada en 2009 en el ámbito de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de la República Argentina, actual Sede Educativa Universitaria de la Facultad Militar Conjunta (FMC).

CONTENIDOS

FRICCIÓN Y C4ISR EN EL SIGLO XXI

¿PUEDE LA TECNOLOGÍA VENCER A CLAUSEWITZ?

Por **SANTIAGO LUIS AVERSA**

Palabras Clave:
> Clausewitz
> Fricción
> C4ISR
> Guerra moderna
> Fricción
> OODA
> Infoxicación

ARTÍCULO CON REFERATO

La irrupción de sistemas C4ISR *(Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance)* ha transformado profundamente las operaciones militares contemporáneas, prometiendo una superioridad basada en el acceso, procesamiento y explotación acelerada de la información. Esta evolución ha llevado a ciertos sectores teóricos y doctrinarios a postular que el dominio tecnológico podría suprimir los factores de incertidumbre y caos tradicionalmente asociados a la guerra. Sin embargo, este artículo sostiene que, a pesar de los avances en recolección de información y capacidades de mando y control, el concepto de fricción desarrollado por Carl von Clausewitz permanece no solo vigente, sino que se manifiesta bajo nuevas formas.

A partir de un análisis conceptual y casos recientes, como los conflictos de Irak (2003) y Ucrania (2022–2025), se argumenta que el C4ISR mitiga ciertos aspectos tradicionales de la fricción (como la distancia y el retraso en las comunicaciones), pero introduce otros tipos: fricción cibernética, cognitiva, cultural y moral. La proliferación de ataques electrónicos, la sobrecarga informativa y los dilemas éticos vinculados a la autonomía de sistemas son ejemplos de las nuevas tensiones emergentes.

Se concluye que la guerra sigue siendo un fenómeno eminentemente humano y caótico, donde la fricción, lejos de desaparecer, se adapta a las tecnologías emergentes. Por ende, la superioridad en C4ISR debe ser acompañada por doctrinas de resiliencia, adaptabilidad y conciencia de la permanencia estructural del azar y la incertidumbre en la guerra.

Introducción

Desde los albores del pensamiento militar moderno, Carl von Clausewitz planteó que la guerra está inmersa en una atmósfera de incertidumbre, caos y resistencia natural a los planes humanos, concepto que sintetizó bajo el término "fricción" (Clausewitz, 1984). En su obra De la Guerra, el prusiano advirtió que incluso las operaciones más simples se ven entorpecidas por un conjunto de factores físicos, humanos y organizacionales que degradan la ejecución de los planes.

La irrupción de tecnologías avanzadas, particularmente los sistemas de C4ISR *(Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance),* ha transformado radicalmente el modo en que las fuerzas armadas planifican y ejecutan operaciones. El objetivo central de C4ISR es otorgar superioridad de información: obtener datos, procesarlos rápidamente y convertirlos en decisiones operativas antes que el adversario, acortando el ciclo OODA *(Observe, Orient, Decide, Act) (Alberts & Hayes, 2003).* Esta transformación tecnológica llevó a teorizar que el dominio de la información podría eliminar los márgenes de incertidumbre clásicos de la guerra.

Sin embargo, la evidencia empírica sugiere lo contrario. Conflictos recientes como la Guerra de Irak (2003) y, de forma aún más contundente, la Guerra en Ucrania (2022–2025), han demostrado que la fricción persiste, adoptando nuevas formas adaptadas al entorno digital y cibernético. Las interrupciones de redes de mando, los errores humanos amplificados por la sobrecarga de información, y los dilemas éticos surgidos de sistemas automatizados, son manifestaciones contemporáneas de la vieja fricción *clausewitziana.*

Este artículo sostiene que, lejos de ser eliminada, la fricción ha sido transformada y complejizada en la era del C4ISR. A partir del análisis conceptual y el estudio de casos concretos, se argumenta que la superioridad informacional, aunque decisiva, no reemplaza la necesidad de resiliencia, adaptabilidad y juicio humano. Comprender y gestionar las nuevas formas de fricción es esencial para el diseño de estrategias militares realistas en el siglo XXI.

La fricción, según Clausewitz, representa la suma de todas aquellas pequeñas dificultades —meteorológicas, humanas, organizacionales, psicológicas— que, en conjunto, hacen que la ejecución de operaciones militares sea mucho más ardua que en la teoría.

El concepto de fricción en Clausewitz

Carl von Clausewitz introdujo el concepto de fricción como un elemento esencial y definitorio de la guerra real en su obra *De la Guerra* (Clausewitz, 1984). La fricción, según el autor prusiano, representa la suma de todas aquellas pequeñas dificultades —meteorológicas, humanas, organizacionales, psicológicas— que, en conjunto, hacen que la ejecución de operaciones militares sea mucho más ardua que en la teoría. "Todo en la guerra es muy simple, pero lo más simple es difícil" (Clausewitz, 1984, p. 119), subraya, ilustrando cómo las operaciones militares, incluso las mejor planificadas, encuentran resistencias que deforman su curso.

La fricción, para Clausewitz, no es un defecto accidental sino una condición estructural de la guerra. Afecta a todos los niveles —estratégico, operacional y táctico— y surge tanto de factores físicos como de la interacción humana bajo condiciones extremas. La guerra no puede entenderse simplemente como un problema de cálculo mecánico, sino como un fenómeno donde el error, el miedo, la fatiga y la confusión son parte inherente de la dinámica (Clausewitz, 1984).

Además, Clausewitz conceptualiza la fricción como algo que no puede eliminarse completamente. La experiencia, el entrenamiento y la disciplina pueden mitigar sus efectos, pero no erradicarla. Incluso los ejércitos más profesionales y las estrategias más ingeniosas son víctimas de esta fuerza invisible que distorsiona las intenciones originales.

Michael Howard, uno de los principales intérpretes contemporáneos de Clausewitz, señala que "la fricción es la diferencia entre la guerra como se planea y la guerra como realmente ocurre" (Howard, 1983, p. 15). Esta apreciación moderna enfatiza que la fricción no es simplemente un obstáculo técnico, sino una brecha fundamental entre teoría y práctica, impulsada por la naturaleza humana y el caos inherente al conflicto armado.

En este sentido, Clausewitz también introduce el concepto de "niebla de guerra" (Fog of War), relacionada estrechamente con la fricción. La niebla de guerra representa la falta de información precisa sobre las propias fuerzas, las del enemigo y el entorno. La combinación de fricción y niebla forma el entorno operativo real al que debe enfrentarse todo comandante.

La fricción también tiene una dimensión positiva: ofrece oportunidades. Si bien afecta a ambos bandos, quienes mejor la comprendan y se adapten a ella pueden explotarla en su beneficio. La flexibilidad, la iniciativa individual y la resiliencia son virtudes que permiten navegar la fricción más eficazmente que la simple adhesión mecánica a un plan preconcebido.

En tiempos modernos, autores como Antulio J. Echevarría II han reafirmado la importancia de la fricción clausewitziana. Echevarría destaca que, aun en escenarios de guerra moderna apoyados en tecnologías avanzadas, la fricción persiste, simplemente mutando en nuevas formas vinculadas a la información, la comunicación y la percepción (Echevarría, 2007).

La fricción no solo actúa a nivel de combate. También afecta los procesos políticos que enmarcan las decisiones estratégicas. El desfasaje entre las intenciones políticas y los resultados militares es, en gran parte, consecuencia de esta constante distorsión que provoca la fricción.

En síntesis, la fricción, para Clausewitz, es la representación de la realidad de la guerra, donde las acciones humanas, el azar, y el entorno material interactúan para impedir la ejecución perfecta de cualquier plan. Entender su inevitabilidad y aprender a operar dentro de sus límites constituye, en última instancia, el arte superior de la conducción militar.

2. El surgimiento del paradigma C4ISR

El paradigma C4ISR —sigla correspondiente a *Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance*— surge

como respuesta a la creciente complejidad de los campos de batalla modernos y a la necesidad de integrar eficazmente el flujo de información para la toma de decisiones militares. A medida que los conflictos se volvieron más dinámicos y dispersos, las fuerzas armadas, especialmente las de Estados Unidos, buscaron maneras de acelerar el ciclo de observación y respuesta para obtener ventaja estratégica (Alberts & Hayes, 2003).

El desarrollo conceptual de C4ISR tiene sus raíces en la Guerra Fría, cuando el enfrentamiento tecnológico con la Unión Soviética impulsó una inversión masiva en capacidades de vigilancia, comunicaciones y comando. Programas como Assault Breaker, impulsados por la DARPA en los años 70, anticiparon la necesidad de fusionar sensores, plataformas de mando y armas de precisión en redes integradas para combatir un enemigo convencional numeroso y bien armado (Krepinevich, 1992).

La Primera Guerra del Golfo en 1991 marcó la primera demostración práctica de capacidades C4ISR avanzadas. El uso combinado de vigilancia satelital, ataques de precisión basados en GPS, sistemas de comunicaciones encriptadas y centros de comando móviles permitió a la coalición liderada por Estados Unidos destruir las fuerzas iraquíes con una eficiencia sin precedentes. Esto consolidó la idea de que el dominio de la información podría ser tan decisivo como la superioridad numérica o el poder de fuego (Libicki & Johnson, 1995).

El núcleo del C4ISR radica en su capacidad para acelerar el ciclo de decisión. Aplicando el modelo OODA (Observe, Orient, Decide, Act) de John Boyd, las fuerzas con C4ISR robusto buscan observar más rápido, orientar su conocimiento de la situación más acertadamente, decidir antes que el adversario y actuar de manera efectiva antes de que el enemigo pueda reaccionar (Boyd, 1987). Esta aceleración no solo permite golpear primero, sino hacerlo de manera más precisa y adaptativa.

Además, el C4ISR promete integrar operaciones conjuntas y multinacionales. Redes de comunicación seguras, plataformas compartidas de inteligencia y sistemas de mando interoperables son diseñados para permitir a unidades terrestres, aéreas, navales y cibernéticas actuar en concierto, como una "fuerza de red" distribuida pero coordinada.

No obstante, el C4ISR no está exento de desafíos. La dependencia tecnológica lo vuelve vulnerable a ciberataques, interferencias electrónicas, sabotajes satelitales y errores de integración. Además, como advierten Alberts y Hayes (2003), el volumen masivo de información recolectada puede sobrepasar la capacidad de procesamiento humano y generar un fenómeno conocido como "parálisis por análisis", donde el exceso de datos retrasa o entorpece la toma de decisiones.

Otro riesgo inherente al C4ISR es la sobre-centralización del mando. La posibilidad técnica de supervisar detalles minuciosos desde niveles superiores puede inducir a prácticas de microgestión que inhiben la iniciativa táctica en el terreno. Esto va en contra de los principios de mando tipo misión (Auftragstaktik), basados en la flexibilidad y la delegación de autoridad (Builder, 1989).

En suma, el surgimiento del paradigma C4ISR representó un cambio profundo en la concepción de la guerra moderna, basado en la información como arma y en la velocidad de procesamiento como ventaja competitiva. Sin embargo, como se analizará en los siguientes apartados, esta transformación no ha eliminado los factores de fricción clausewitzianos, sino que los ha desplazado hacia nuevas dimensiones.

3. Fricción persistente en la era del C4ISR

A pesar de los extraordinarios avances técnicos en materia de comando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento, la fricción clausewitziana no ha desaparecido en los conflictos modernos. De hecho, el entorno C4ISR, lejos de suprimir las fuentes tradicionales de incertidumbre y error, ha introducido nuevas formas de

fricción adaptadas a las dinámicas contemporáneas de la guerra.

Así, no es ocioso recordar que, a comienzos del siglo XX, Giulio Douhet anticipó que el avance tecnológico, particularmente en el ámbito de la aviación militar, transformaría la naturaleza de la guerra, permitiendo ataques decisivos desde el aire que superarían las limitaciones de los combates terrestres. En su obra The Command of the Air, Douhet argumentó que el dominio del aire permitiría a una nación neutralizar rápidamente la resistencia enemiga, reduciendo así la fricción inherente a los conflictos prolongados. Sin embargo, la experiencia acumulada en conflictos posteriores ha demostrado que, a pesar de los avances tecnológicos, la fricción persiste en formas nuevas y complejas, como la guerra cibernética, la saturación informativa y los dilemas éticos asociados al uso de sistemas autónomos. Estas manifestaciones contemporáneas de fricción reflejan que la tecnología no ha eliminado las incertidumbres y desafíos inherentes a la guerra, sino que los ha transformado y, en algunos casos, amplificado.

3.1 Limitaciones tecnológicas

La infraestructura que sostiene el C4ISR es altamente dependiente de satélites, redes digitales y sistemas de procesamiento de datos distribuidos. Esta dependencia la hace vulnerable a operaciones de guerra electrónica (EW), ciberataques y sabotaje espacial. La interferencia de señales GPS, los ataques de denegación de servicio (DDoS) contra centros de comando, y el spoofing de comunicaciones representan amenazas que pueden degradar o inutilizar total o parcialmente los sistemas de mando y control (Rid, 2011).

Además, la gestión de grandes volúmenes de datos genera una nueva forma de fricción: la saturación informativa. Como señalan Alberts y Hayes (2003), la sobrecarga de información puede producir un fenómeno conocido como "parálisis por análisis", donde la cantidad de datos supera la capacidad humana de procesamiento eficiente, generando demoras en la toma de decisiones o errores de priorización.

El problema no reside únicamente en la cantidad de información, sino en su calidad, relevancia y oportunidad. Datos desactualizados, mal interpretados o desconectados del contexto operativo pueden inducir a conclusiones erróneas y a decisiones contraproducentes, a pesar de contar con sistemas de recopilación tecnológicamente avanzados.

3.2 Limitaciones humanas

La fricción en la guerra no desaparece simplemente porque los datos sean más abundantes o precisos. Los seres humanos siguen siendo el eslabón crítico en el procesamiento de la información, la toma de decisiones y la ejecución de las operaciones.

Daniel Kahneman (2011) destaca cómo los sesgos cognitivos afectan las decisiones incluso en condiciones de alta información.

Entre ellos, el confirmation bias (tendencia a favorecer información que confirma creencias previas) y el availability bias (dar mayor peso a información fácilmente disponible) son especialmente peligrosos en entornos saturados de datos. A medida que el volumen informativo crece, también lo hacen las oportunidades de error humano.

La presión temporal que impone el modelo OODA, exacerbada por la disponibilidad casi instantánea de datos, puede llevar a decisiones precipitadas, basadas más en reflejos cognitivos rápidos que en razonamientos estratégicos profundos. Este fenómeno se agrava en situaciones de combate de alta intensidad, donde el estrés psicológico incrementa la probabilidad de error.

3.3 Limitaciones organizacionales

El C4ISR, para ser efectivo, requiere interoperabilidad perfecta entre diferentes ramas de las fuerzas armadas y, frecuentemente, entre coaliciones multinacionales. Las diferencias doctrinales, culturales, tecnológicas y de procedimientos entre aliados pueden generar nuevas formas de fricción organizacional.

Problemas como la incompatibilidad de sistemas de comunicaciones, los desacuerdos sobre reglas de enfrentamiento y los distintos enfoques sobre manejo de inteligencia pueden obstaculizar la integración efectiva de unidades en el campo de batalla (NATO, 2018). Asimismo, la concentración de información en niveles superiores puede inducir a prácticas de microgestión que afectan negativamente la iniciativa táctica.

La arquitectura organizacional requerida para manejar sistemas C4ISR de alta complejidad tiende a ser pesada, burocrática y lenta para adaptarse a cambios dinámicos en el entorno operativo. Esto contrasta con las necesidades de flexibilidad y adaptación que exige la guerra moderna, especialmente en escenarios irregulares o híbridos.

4. Nuevas formas de fricción en conflictos modernos

La persistencia de la fricción en el entorno operativo moderno se manifiesta no sólo en las limitaciones técnicas, humanas y organizacionales tradicionales, sino también en la aparición de nuevas formas de fricción adaptadas a las dinámicas contemporáneas. La teoría clásica de la guerra, que identificaba el azar, la incertidumbre y el esfuerzo humano como fuentes esenciales de fricción, sigue plenamente vigente. Sin embargo, los conflictos actuales, marcados por la interdependencia tecnológica y la aceleración de los flujos de información, presentan capas adicionales de complejidad que incrementan los riesgos de disrupción, error y descoordinación, incluso en escenarios donde la superioridad tecnológica parece garantizada.

El desarrollo y despliegue de sistemas C4ISR ha transformado radicalmente el modo en que las fuerzas armadas perciben, interpretan y actúan en el campo de batalla. No obstante, esta transformación no ha suprimido la

incertidumbre y el caos; más bien, los ha desplazado hacia nuevos dominios que hasta hace poco ocupaban un lugar marginal en la teoría militar. El ciberespacio, por ejemplo, se ha convertido en un campo de batalla en sí mismo, donde la capacidad de un actor para interferir, engañar o sabotear los sistemas de información del adversario puede alterar decisivamente el equilibrio operacional. Asimismo, el dominio informacional, donde se libran batallas narrativas y se disputan percepciones, introduce un nivel de fricción cognitiva que impacta tanto en las tropas como en las poblaciones civiles.

A estas dimensiones se suman las diferencias culturales, que pueden afectar la interoperabilidad entre fuerzas aliadas y la comprensión de entornos sociales complejos, así como los dilemas éticos surgidos del uso creciente de sistemas automatizados y de inteligencia artificial en decisiones operativas críticas. Cada uno de estos factores agrega nuevas capas de fricción que las fuerzas modernas deben anticipar y gestionar. La ética de la automatización, en particular, plantea interrogantes sobre la delegación de decisiones letales a máquinas y el riesgo de deshumanizar el proceso de la guerra, generando tensiones morales tanto a nivel táctico como estratégico. En consecuencia, el desafío actual ya no consiste únicamente en dominar los sistemas tecnológicos, sino en construir organizaciones resilientes que integren, comprendan y operen eficazmente dentro de este entorno multidimensional de fricción ampliada.

4.1 Fricción cibernética

La guerra cibernética ha inaugurado una dimensión de fricción completamente nueva. Los sistemas C4ISR, al depender de redes digitales, resultan vulnerables a ataques que degradan su funcionamiento o manipulan la información transmitida.

Thomas Rid (2013) sostiene que la ciberacción puede interrumpir el flujo de mando, la percepción situacional y la coordinación táctica sin necesidad de enfrentamientos físicos directos.

Ataques de spoofing (suplantación de señales GPS), denegación de servicios en redes de comando y sabotaje de infraestructuras críticas mediante malware son prácticas frecuentes que afectan de manera sustancial la capacidad de actuar basada en información confiable.

El caso del ataque a la red eléctrica ucraniana en 2015 por el grupo Sandworm, analizado por Greenberg (2019), demuestra cómo actores cibernéticos pueden paralizar sistemas críticos sin necesidad de intervención militar convencional.

La fricción cibernética se caracteriza por su velocidad, su invisibilidad inicial y su capacidad de producir efectos estratégicos a partir de acciones tácticas de bajo costo.

4.2 Fricción cognitiva

El volumen y la velocidad de la información en las operaciones

El C4ISR, para ser efectivo, requiere interoperabilidad perfecta entre diferentes ramas de las fuerzas armadas y, frecuentemente, entre coaliciones multinacionales. Las diferencias doctrinales, culturales, tecnológicas y de procedimientos entre aliados pueden generar nuevas formas de fricción organizacional.

C4ISR plantean una carga cognitiva sin precedentes para los comandantes y operadores.

Daniel Kahneman (2011) advierte que el cerebro humano, aunque poderoso, tiene recursos limitados para procesar datos, especialmente bajo estrés.

La fricción cognitiva surge cuando la cantidad de información, su complejidad y su ambigüedad superan la capacidad del personal militar para interpretarla de manera adecuada.

La sobrecarga de datos puede llevar a errores de apreciación, retrasos en la toma de decisiones o dependencia excesiva de herramientas automatizadas de análisis.

Además, en entornos donde la información es intencionalmente manipulada por actores enemigos mediante operaciones de desinformación, el riesgo de interpretación errónea se incrementa exponencialmente.

4.3 Fricción cultural

En escenarios multinacionales, donde las coaliciones operan integrando fuerzas de distintos países, culturas militares y niveles tecnológicos, la fricción cultural se convierte en un obstáculo operacional serio.

Diferencias en doctrina, valores, estilos de mando, percepción del riesgo y expectativas de resultados generan tensiones que afectan la cooperación efectiva (NATO, 2018).

Ejemplos recientes en Afganistán (2001–2021) muestran que, a pesar de compartir plataformas C4ISR comunes, las unidades estadounidenses, británicas, canadienses y de otros países enfrentaron dificultades para coordinar reglas de enfrentamiento, prioridades operativas y procedimientos de intercambio de inteligencia (Jones, 2008).

La fricción cultural no solo ralentiza la operación conjunta, sino que puede minar la confianza entre aliados, afectando la cohesión y la eficacia de la misión.

4.4 Fricción moral

La incorporación creciente de sistemas autónomos, drones armados y algoritmos de inteligencia artificial en operaciones militares plantea nuevos dilemas éticos.

La fricción moral surge cuando decisiones de vida o muerte son trasladadas parcial o totalmente a sistemas automáticos, reduciendo el control humano directo.

Paul Scharre (2016) alerta sobre los riesgos de la automatización letal: errores en la identificación de objetivos, ataques colaterales no intencionados, y la pérdida de responsabilidad clara sobre las decisiones tomadas por máquinas.

La existencia de fricción moral obliga a replantear principios tradicionales de la guerra justa *(just war theory)* y a establecer marcos de control que aseguren la rendición de cuentas, incluso en entornos de combate altamente digitalizados.

5. Estudios de caso breves

La persistencia de la fricción en el entorno C4ISR no es solo una construcción teórica: ha quedado demostrada de manera concreta en conflictos recientes. Dos casos particularmente ilustrativos son la Guerra de Irak (2003) y la Guerra en Ucrania (2022–2025). Ambos muestran cómo, a pesar del uso intensivo de tecnologías avanzadas de información y mando, la fricción no solo se mantuvo, sino que adoptó nuevas formas de expresión.

5.1 Guerra de Irak (2003): La ilusión del dominio informacional

La operación Iraqi Freedom de 2003 fue concebida como una demostración de la eficacia del dominio informacional. Las fuerzas estadounidenses desplegaron un conjunto sin precedentes de capacidades C4ISR, que incluían satélites de vigilancia de alta resolución, sistemas de comunicaciones tácticas seguras, redes de mando digitalizadas y misiles guiados por GPS (Ferris, J., 2003).

En la fase inicial de la campaña, estos medios permitieron una operación rápida y efectiva, caracterizada por ataques de precisión y maniobras rápidas conocidas como “Thunder

Runs" hacia Bagdad. Parecía que el C4ISR había reducido la fricción al mínimo: la coalición destruía objetivos estratégicos con precisión quirúrgica y mantenía la superioridad situacional sobre las fuerzas iraquíes (Air Force Historical Support Division, 2003).

Sin embargo, tras la caída de Bagdad, emergieron nuevas dinámicas que pusieron en evidencia las limitaciones del enfoque. La insurgencia iraquí, descentralizada, adaptativa y operando en células pequeñas, anuló muchas de las ventajas tecnológicas de la coalición.

La falta de inteligencia humana (HUMINT) efectiva, las diferencias culturales no comprendidas y el exceso de confianza en sensores técnicos para identificar amenazas demostraron que el C4ISR no podía reemplazar la necesidad de conocimiento situacional cualitativo (Metz, 2007).

El General Stanley McChrystal reconocería más tarde que "poseíamos una visión casi perfecta del campo de batalla... pero no entendíamos lo que estábamos viendo" (McChrystal, 2013). La fricción no desapareció: simplemente cambió de forma.

5.2 Guerra en Ucrania (2022–2025): La degradación deliberada del C4ISR

El conflicto en Ucrania desde 2022 ha proporcionado una nueva perspectiva sobre la fricción en un entorno donde ambos bandos emplean intensivamente medios C4ISR.

Tanto las fuerzas ucranianas como las rusas desplegaron capacidades de vigilancia satelital, drones de reconocimiento, redes de comunicaciones cifradas y sistemas de targeting de precisión.

No obstante, una característica distintiva de este conflicto ha sido la degradación deliberada del entorno C4ISR por medios de guerra electrónica, ciberataques y sabotaje de infraestructura.

Los sistemas de comunicación fueron bloqueados o saturados, los drones fueron derribados mediante interferencias electromagnéticas, y los datos de inteligencia fueron manipulados o retrasados a través de ataques cibernéticos coordinados.

La capacidad de operar de manera resiliente frente a la pérdida o degradación de C4ISR se volvió crucial. La experiencia de combate en el conflicto ruso-ucraniano evidenció diferencias significativas en los modelos de mando y control adoptados por las fuerzas en contienda. Las fuerzas ucranianas demostraron una capacidad superior de adaptación, impulsada por la descentralización operativa y la delegación de autoridad a los niveles tácticos, lo que les permitió responder con agilidad a las dinámicas del campo de batalla. Este enfoque contrastó con la rigidez estructural de las fuerzas rusas, cuya dependencia de esquemas jerárquicos tradicionales y su escasa promoción de la iniciativa a nivel subalterno resultaron en recurrentes descoordinaciones operativas y limitaciones para explotar oportunidades tácticas emergentes (Liang, 2025).

Este caso demuestra que la fricción tecnológica y organizacional en entornos altamente contestados puede neutralizar la ventaja teórica del C4ISR, volviendo a colocar en primer plano la importancia de la resiliencia, la iniciativa táctica y el juicio humano.

6. Reconciliando C4ISR y Clausewitz: Hacia una teoría actualizada de la fricción

El análisis de los conflictos modernos demuestra que, a pesar de los avances tecnológicos, la guerra sigue estando sometida a la fricción clausewitziana. La aparición del C4ISR no elimina la incertidumbre, el error, el caos o el azar; simplemente los desplaza hacia nuevas dimensiones. Comprender esta persistencia es fundamental para el diseño de estrategias realistas en el siglo XXI.

6.1 Fricción como constante estructural

Clausewitz enseñó que la fricción es inherente al fenómeno bélico debido a la interacción del azar, la incertidumbre, el peligro y el esfuerzo humano (Clausewitz, 1984). Esta concepción mantiene plena vigencia, aún en el contexto de las guerras modernas. No

importa cuánto se perfeccionen los medios de observación, mando y control: la dinámica de la guerra sigue caracterizándose por su resistencia a la ejecución fluida de los planes, producto de factores tanto materiales como psicológicos. Como ha señalado el Departamento de Defensa de los Estados Unidos, incluso en entornos dominados por tecnologías avanzadas, las operaciones militares están continuamente expuestas a "fricciones operativas imprevistas" que limitan la eficacia de la planificación inicial (U.S. Department of Defense, 2018).

El entorno digital no es una excepción a esta regla de la fricción. Muy por el contrario, la incorporación masiva de sistemas de mando y control basados en redes, sensores inteligentes y comunicaciones satelitales ha introducido nuevos vectores de vulnerabilidad. La creciente dependencia de la infraestructura cibernética expone a las fuerzas armadas a riesgos de interrupciones, ataques de denegación de servicio, manipulaciones de información y saturación deliberada del flujo de datos (NATO Cooperative Cyber Defence Centre of Excellence, 2013). En vez de eliminar la fricción, la digitalización ha transformado su naturaleza, agregando capas de complejidad y ampliando el espectro de posibles contingencias disruptivas.

La sobrecarga de información constituye otra fuente crítica de fricción moderna. En operaciones caracterizadas por la disponibilidad de datos en tiempo real, la dificultad no reside ya en la falta de información, sino en la capacidad de procesarla de manera oportuna y relevante. El fenómeno de la "parálisis por análisis" puede neutralizar los potenciales beneficios de los sistemas C4ISR si las organizaciones no desarrollan doctrinas ágiles de priorización y toma de decisiones bajo presión (Joint Chiefs of Staff, 2020). La necesidad de filtrar, jerarquizar y traducir la información en acciones concretas se convierte, así, en una nueva expresión de la fricción clausewitziana.

Por lo tanto, lejos de erradicar la fricción, la era de la guerra digital la ha reformulado, multiplicando sus manifestaciones y exigiendo nuevas competencias para su gestión. Reconocer esta realidad implica asumir que la superioridad tecnológica no garantiza automáticamente la superioridad operacional. Más aún, el exceso de confianza en sistemas digitales puede generar vulnerabilidades estratégicas si no se acompaña de resiliencia organizacional, pensamiento crítico y adaptabilidad táctica. La comprensión moderna de la fricción debe evolucionar junto con las tecnologías que la moldean, pero sin perder de vista el principio fundamental enseñado por Clausewitz: la guerra siempre será más difícil de lo que parece en el papel.

CV

SANTIAGO LUIS AVERSA

Abogado (UTDT). Master of Laws (Chicago Kent College of Law). Subteniente de Reserva (Colegio Militar de la Nación – CUFOR). Oficial Asesor de E.M. Especial en Asuntos Territoriales (Escuela Superior de Guerra). Teniente de Corbeta de la Armada Argentina (RN). Profesor Asociado (USAL). Profesor Invitado (George Washington University, Instituto de Inteligencia de las Fuerzas Armadas, Escuela De Guerra Conjunta, Centro de Educación de Inteligencia de Combate).

El Departamento de Defensa de EE. UU. enfatiza la necesidad de sistemas que puedan resistir y recuperarse rápidamente de perturbaciones, destacando que la preparación y la adaptabilidad son fundamentales para mantener la eficacia operativa.

6.2 C4ISR como mitigador y generador de fricción

Si bien el desarrollo de sistemas C4ISR (Comando, Control, Comunicaciones, Computadoras, Inteligencia, Vigilancia y Reconocimiento) ha permitido reducir ciertos tipos de fricción tradicionales en el campo de batalla —como la falta de conocimiento oportuno del terreno o la demora en las comunicaciones entre unidades dispersas—, también ha introducido nuevas fuentes de fricción que afectan la conducción de operaciones. La posibilidad de disponer de imágenes satelitales en tiempo real, enlaces de datos seguros y sistemas automatizados de mando y control no elimina el azar ni la incertidumbre inherentes al fenómeno bélico. Al contrario, la saturación informativa, la creciente dependencia de infraestructuras tecnológicas vulnerables y la amenaza constante de ataques cibernéticos constituyen manifestaciones contemporáneas de la fricción clausewitziana, ahora adaptadas a la era digital.

Dentro de este contexto, la cantidad de datos disponibles puede, paradójicamente, convertirse en un obstáculo para la toma de decisiones oportuna y eficaz. Alberts y Hayes (2003) advierten que el verdadero desafío del entorno informacional contemporáneo no reside en recolectar más datos, sino en desarrollar organizaciones capaces de filtrar, interpretar y actuar sobre la información de manera adecuada bajo condiciones de presión e incertidumbre. La "parálisis por análisis", en la que los niveles de mando se ven abrumados por la sobrecarga de datos sin lograr traducirla en acciones concretas, es una de las nuevas formas en que la fricción opera en conflictos de alta tecnología. De este modo, la capacidad para distinguir información relevante de ruido se convierte en una competencia operacional crítica.

La resiliencia y la flexibilidad organizacional emergen así como elementos tan importantes como las capacidades técnicas en la guerra moderna. No basta con tener acceso a mejores sensores, redes de comunicación o plataformas de procesamiento de datos; es necesario construir estructuras doctrinarias y culturales que permitan operar de manera efectiva aun cuando los sistemas tecnológicos sean degradados o saboteados. Esto implica entrenar a los niveles subalternos para actuar de manera autónoma, preparar redundancias organizacionales y fomentar una cultura de adaptabilidad táctica que pueda suplir las fallas tecnológicas momentáneas. De lo contrario, las

organizaciones militares corren el riesgo de volverse tecnológicamente avanzadas pero operacionalmente frágiles frente a entornos dinámicos y contestados.

En definitiva, el C4ISR, aunque representa una revolución en la forma de conducir operaciones militares, no ha abolido la fricción; simplemente la ha desplazado hacia nuevos dominios. La guerra sigue siendo un fenómeno profundamente humano y, por ende, inherentemente imperfecto. Entender las limitaciones de los sistemas informacionales y reforzar la resiliencia organizacional frente a fallos tecnológicos se presenta, entonces, como una tarea ineludible para las fuerzas armadas que aspiren a sostener ventajas competitivas en los escenarios bélicos contemporáneos.

6.3 La resiliencia y la adaptabilidad como respuesta a la fricción moderna

En los conflictos recientes, la capacidad de operar en ambientes de información degradada, bajo presiones cognitivas extremas y frente a adversarios que atacan deliberadamente las redes C4ISR, se ha convertido en un factor decisivo para el éxito militar. La evolución del campo de batalla hacia entornos caracterizados por la volatilidad, la incertidumbre, la complejidad y la ambigüedad (VICA) ha demostrado que ninguna superioridad tecnológica puede garantizar por sí misma la continuidad de las operaciones. Las fuerzas armadas que dependen de sistemas de información centralizados y rígidos son particularmente vulnerables ante ataques cibernéticos, sabotajes electrónicos y disrupciones físicas que alteran o interrumpen el flujo de datos esenciales para la conducción de operaciones. En este contexto, la capacidad de mantener la funcionalidad y la cohesión organizacional, incluso bajo condiciones de degradación severa de las comunicaciones, se revela como una condición crítica para la supervivencia y la victoria.

La resiliencia organizacional —entendida como la habilidad de absorber choques, adaptarse rápidamente y reorganizarse frente a la adversidad— emerge como una competencia esencial para las fuerzas armadas contemporáneas. Esta resiliencia no depende exclusivamente de la robustez tecnológica, sino que reside fundamentalmente en factores humanos y organizativos: flexibilidad en los procedimientos, entrenamiento para la toma de decisiones autónoma y una cultura que fomente la iniciativa individual dentro de un marco doctrinario claro. Como sostiene Van Creveld (1985), en entornos de guerra donde la incertidumbre y el caos predominan, las organizaciones más exitosas no son aquellas que logran imponer un control perfecto, sino aquellas que distribuyen el poder de decisión de manera inteligente y preparan a sus unidades para actuar de forma independiente cuando las comunicaciones o las órdenes superiores se ven interrumpidas.

En lugar de confiar exclusivamente en el flujo centralizado de información, las fuerzas exitosas son aquellas que descentralizan la toma de decisiones, promueven la iniciativa táctica y forman unidades capaces de actuar de manera autónoma bajo principios de misión (Van Creveld, 1985). El concepto de *"Auftragstaktik"* o conducción por objetivos, desarrollado en el ejército prusiano del siglo XIX, ha recobrado una actualidad notable en la era de los sistemas C4ISR degradables. La descentralización no implica ausencia de control, sino un modelo basado en la confianza, la capacitación rigurosa y la claridad en los fines estratégicos, permitiendo que las unidades subordinadas interpreten y ejecuten las misiones asignadas adaptándose a las circunstancias cambiantes del entorno operativo.

El desempeño de las fuerzas ucranianas durante el conflicto 2022–2025 constituye un ejemplo particularmente ilustrativo de la resiliencia organizacional en contextos de alta disrupción tecnológica. A pesar de sufrir daños severos en su infraestructura de comunicaciones y tecnología debido a ataques cibernéticos y electrónicos rusos, la adopción de una estructura de mando flexible y adaptativa les permitió sostener niveles elevados de eficacia operacional. La descentralización de la toma de decisiones, combinada con la capacitación intensiva de los comandantes de nivel táctico, mitigó los efectos adversos sobre las capacidades de comando y control, permitiendo a las unidades ucranianas reaccionar con agilidad ante situaciones imprevistas y explotar las vulnerabilidades enemigas de manera oportuna (Liang, 2025). Esta experiencia reafirma que, en el siglo XXI, la resiliencia organizacional es tan crucial como la superioridad tecnológica para sostener la eficacia militar en ambientes altamente contestados.

6.4 Hacia una teoría actualizada de la fricción

Actualizar el concepto de fricción para el siglo XXI implica reconocer que:

- La fricción persiste como fenómeno estructural en la guerra, aunque sus formas cambien;
- El dominio de la información mitiga algunos aspectos de la fricción, pero introduce nuevos desafíos;
- La resiliencia organizacional, la descentralización y la adaptabilidad son respuestas críticas a las nuevas formas de fricción;
- El juicio humano, la intuición táctica y la flexibilidad siguen siendo elementos insustituibles.

La implementación de sistemas C4ISR (Comando, Control, Comunicaciones, Computadoras, Inteligencia, Vigilancia y Reconocimiento) ha transformado significativamente las operaciones militares modernas. Sin embargo, esta transformación no ha eliminado la fricción inherente a los conflictos armados. Como señala el informe del Atlantic Council, la interoperabilidad y la resiliencia son esenciales para que las fuerzas armadas operen eficazmente en entornos complejos y cambiantes (Atlantic Council, 2023).

La resiliencia en los sistemas C4ISR implica la capacidad de adaptarse y continuar operando frente a interrupciones o ataques. El Departamento de Defensa de EE. UU. enfatiza la necesidad de sistemas que puedan resistir y recuperarse rápidamente de perturbaciones, destacando que la preparación y la adaptabilidad son fundamentales para mantener la eficacia operativa (Mann, S., Endersby, J., & Searle, T., 2001).

Además, la integración de tecnologías emergentes, como la inteligencia artificial y la computación cuántica, presenta nuevas oportunidades y desafíos. El informe de la Comisión de Postura Estratégica de EE. UU. subraya que, si bien estas tecnologías pueden mejorar las capacidades C4ISR, también aumentan la complejidad y la posibilidad de fricciones imprevistas, lo que requiere doctrinas y estructuras organizativas que puedan operar eficazmente dentro de estas nuevas dinámicas (Congressional Commission, 2023).

Conclusiones

La evolución tecnológica experimentada en el ámbito militar durante las últimas décadas, particularmente a través de los sistemas C4ISR, ha revolucionado las formas de planificar, conducir y ejecutar operaciones. La promesa de alcanzar una superioridad informacional casi absoluta, acelerando el ciclo de decisión y reduciendo la incertidumbre, llevó a ciertos sectores teóricos y doctrinarios a cuestionar la vigencia de conceptos clásicos como la fricción clausewitziana.

Sin embargo, el análisis realizado demuestra que la fricción no ha sido superada. A pesar de los notables avances en capacidad de recolección, procesamiento y diseminación de información, los conflictos modernos evidencian que la incertidumbre, el azar, el error humano y la resistencia activa del enemigo siguen presentes en nuevas formas. La fricción persiste en dominios cibernéticos, cognitivos, culturales y éticos, manifestándose como vulnerabilidad tecnológica, sobrecarga informativa, malinterpretaciones interculturales y dilemas en la autonomía de los sistemas de armas.

Los casos de Irak (2003) y Ucrania (2022–2025) muestran que incluso fuerzas altamente equipadas con tecnologías C4ISR enfrentan fricciones insalvables cuando el entorno se torna dinámico, adversarial y degradado. La resiliencia organizacional, la adaptabilidad táctica y la descentralización del mando emergen como elementos cruciales para operar eficazmente bajo condiciones de fricción moderna.

En consecuencia, el pensamiento estratégico actual no debe caer en la trampa de la "ilusión tecnológica". La superioridad informacional, aunque valiosa, no elimina la naturaleza caótica e incierta de la guerra. Clausewitz permanece vigente: comprender y gestionar la fricción, en todas sus dimensiones, continúa siendo la piedra angular de una estrategia militar realista y exitosa.

El futuro de la guerra, más que una progresión lineal hacia el control perfecto del campo de batalla, parece una evolución hacia escenarios donde la tecnología y la fricción conviven en una tensión permanente. Aceptar esta realidad, y diseñar fuerzas capaces de navegar en ella, será la verdadera ventaja estratégica del siglo XXI.

BIBLIOGRAFÍA

Air Force Historical Support Division. (2003). 2003 - *Operation Iraqi Freedom*. Disponible en https://www.afhistory.af.mil/FAQs/Fact-Sheets/Article/458942/2003-operation-iraqi-freedom/

-

Alberts, D. S., & Hayes, R. E. (2003). Power to the Edge: Command and Control in the Information Age. Department of Defense Command and Control Research Program (CCRP). Disponible en: www.dodccrp.org/files/Alberts_Power.pdf

-

Atlantic Council. (2023). *In brief: C4ISR - A five-step guide to maintaining NATO's comparative military edge over the coming decade*. Disponible en: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/in-brief-c4isr-a-five-step-guide-to-maintaining-natos-comparative-military-edge-over-the-coming-decade/

-

Boyd, J. (1987). A Discourse on Winning and Losing. Air University Library. Disponible en: https://www.coljohnboyd.com/static/documents/2018-03__Boyd_John_R__edited_Hammond_Grant_T__A_Discourse_on_Winning_and_Losing.pdf

-

Builder, C. H. (1989). The Masks of War: American Military Styles in Strategy and Analysis. RAND Corporation.

-

Clausewitz, C. v. (1984). On War (M. Howard & P. Paret, Eds. and Trans.). Princeton University Press.

-

Congressional Commission on the Strategic Posture of the United States. (2023). *America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States*. Recuperado de https://www.armed-services.senate.gov/imo/media/doc/americas_strategic_posture_the_final_report_of_the_congressional_commission_on_the_strategic_posture_of_the_united_states.pdf

-

Douhet, G. (1921). The Command of the Air (D. Ferrari, Trans.). Air University Press. Disponible en: https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0160_DOUHET_THE_COMMAND_OF_THE_AIR.pdf

-

Echevarría II, A. J. (2002). Clausewitz's Center of Gravity: Changing Our Warfighting Doctrine—Again!. US Army War College Press

-

Ferris, J. (2003). *A New American Way of War? C4ISR in Operation Iraqi Freedom, A Provisional Assessment*. Journal of Military and Strategic Studies. Recuperado de https://jmss.org/article/view/57813/43487

-

Greenberg, A. (2019). Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Doubleday.

-

Jones, S. G. (2008). *Counterinsurgency in Afghanistan*. Disponible en: https://www.rand.org/pubs/monographs/MG595.html Kahneman, D. (2011). Thinking, Fast and Slow. Farrar, Straus and Giroux.

-

Liang, C. S. (2025, marzo 7). *Ten lessons from the Russia-Ukraine war*. Geneva Centre for Security Policy.. Disponible en: https://www.gcsp.ch/publications/ten-lessons-russia-ukraine-war

-

Libicki, M & Johnson S. (eds.)(1995). The Commander's Call: Information Dominance and the Future of War. Naval Institute Press. Disponible en: www.usni.org/press/books/commanders-call

-

Mann, S., Endersby, J., & Searle, T. (2001). *Thinking Effects: Effects-Based Methodology for Joint Operations*. Department of Defense. Recuperado de https://media.defense.gov/2017/Nov/21/2001847048/-1/-1/0/CP_0015_MANN_ENDERSBY_SEARLE_THINKING_EFFECTS.PDF

-

NATO Allied Command Transformation. (2018). Framework for Future Alliance Operations. Disponible en: https://www.act.nato.int/wp-content/uploads/2023/06/180514_ffao18-txt.pdf

-

NATO Cooperative National Cyber Security Strategy Guidelines. (2013) National Cyber Security Strategy Guidelines. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

-

Rid, T. (2011) Cyber War Will Not Take Place, Journal of Strategic Studies, 35:1, 5-32. Disponible en http://dx.doi.org/10.1080/01402390.2011.608939

-

Scharre, P. (2016). Army of None: Autonomous Weapons and the Future of War. W. W. Norton & Company. Disponible en: https://ftp.idu.ac.id/wp-content/uploads/ebook/tdg/MILITARY%20PLATFORM%20DESIGN/Army%20of%20None%20Autonomous%20Weapons%20and%20the%20Future%20of%20War.pdf

-

U.S. Department of Defense. (2018). *Joint Concept for Operating in the Information Environment* (JCOIE). Disponible en: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf

-

Van Creveld, M. (1985). Command in War. Harvard University Press.

LIDERAZGO: CONSTRUYENDO PUENTES

EL LÍDER COMO NEXO ENTRE EL PROPÓSITO PERSONAL Y EL ORGANIZACIONAL

Por **CN (RE) CLAUDIO GROSSI; CNIM (RE) ALEJANDRO DI TELLA; CNIM DIEGO GORDILLO; CN (RE) FELIX PLAZA; CF (RE) MARTÍN RODRÍGUEZ; CL (RE) JULIO SANGUINETTI**

Palabras Clave:
> Liderazgo
> Liderazgo institucional
> Propósito personal
> Propósito institucional
> Cultura organizacional
> Vocación
> Contrato psicológico
> Anclas de carrera
> Salario emocional

Resumen
El presente trabajo aborda el papel del líder como nexo entre los propósitos individuales de los integrantes de una organización y el propósito institucional que la orienta. Se sostiene que el liderazgo requiere no solo de la dirección hacia objetivos estratégicos, sino también de la capacidad de articular sentido y significado compartido. A partir de un análisis conceptual de las dimensiones del propósito personal y organizacional y teniendo en cuenta aspectos como vocación, contrato psicológico, anclas de carrera y salario emocional, se propone que el líder actúa como un puente que permite alinear ambos niveles de sentido, y favorece con ello el compromiso, la cohesión y la sostenibilidad institucional.

Introducción
En el ámbito laboral actual, el compromiso de las personas con la organización se ha convertido en un factor determinante para la productividad, la resiliencia y la lealtad organizacional. Este compromiso se fortalece cuando los individuos logran alinear su propósito personal con el propósito organizacional, de tal modo que encuentran en su trabajo una fuente de sentido y realización. Para que esto ocurra, el liderazgo desempeña un papel fundamental y actúa como un puente que facilita la integración entre las aspiraciones individuales y los objetivos estratégicos de la organización.

Esta dinámica es particularmente desafiante en instituciones con estructuras jerárquicas bien definidas, como las organizaciones militares. En estos entornos, la incorporación de nuevos integrantes desde la base –debido a que las Fuerzas Armadas incorporan personal militar a sus cuadros solo a través de sus institutos de formación–, implica no solo una adaptación funcional, sino también una integración cultural y motivacional. El liderazgo, en sus

diferentes niveles, debe acompañar este proceso y ayudar a los miembros a consolidar su vocación, definir sus anclas de carrera y descubrir cómo su propósito individual puede alinearse con la misión institucional.

El propósito personal es el motor que impulsa a las personas en su desarrollo profesional. Según estudios recientes (Dhingra, Samo, Schaninger, & Schrimper, 2021), aquellos logran conectar su trabajo con su propósito experimentan mayores niveles de satisfacción y compromiso, lo que a su vez impacta positivamente en su desempeño y en la organización en su conjunto. Sin embargo, este propósito no es estático, sino que evoluciona con el tiempo. Lo que motiva a un individuo en sus primeros años de carrera puede no ser lo mismo que lo impulsa en etapas posteriores. Por eso, es esencial que los líderes reconozcan y acompañen estos cambios, y proporcionen un entorno en el que las personas puedan redescubrir y redefinir su propósito dentro de la organización.

En este contexto, conceptos como vocación, contrato psicológico, anclas de carrera y salario emocional adquieren relevancia. No se trata solo de asignar tareas o establecer objetivos, sino de generar una cultura organizacional que brinde seguridad, desarrollo y sentido de pertenencia. Las investigaciones han demostrado que los trabajadores definen su sentido de propósito a partir de su trabajo, lo que convierte al liderazgo en una herramienta clave para guiar y potenciar esta conexión.

En definitiva, el liderazgo institucional debe ir más allá de la simple gestión de recursos humanos y convertirse en un facilitador del desarrollo individual dentro del marco de la organización. Un jefe[1] que comprende la importancia del propósito en el trabajo no solo optimiza el rendimiento de su equipo, sino que también contribuye a la construcción de una cultura organizacional más fuerte, cohesionada y sostenible en el tiempo.

Propósito organizacional

El propósito organizacional es la razón de ser de una organización, es decir, el motivo fundamental por el cual existe más allá de sus objetivos financieros. Define su identidad, orienta sus decisiones estratégicas y proporciona un marco de referencia para la cultura organizacional y el liderazgo.

No se trata solo de lo que la organización hace, sino del impacto que busca generar en su entorno. Un propósito bien definido inspira a los empleados, fortalece el compromiso de los *stakeholders* y permite diferenciarse en el mercado.

Para ser efectivo, el propósito debe integrarse en la cultura

1. Entendemos como Jefe a todo individuo con autoridad que se encuentra en una posición de conducción, con abstracción de la magnitud de su Unidad dentro de la organización.

Un jefe que comprende la importancia del propósito en el trabajo no solo optimiza el rendimiento de su equipo, sino que también contribuye a la construcción de una cultura organizacional más fuerte, cohesionada y sostenible en el tiempo.

organizacional y ser una fuente de identidad para la organización. No basta con que los jefes conozcan su importancia; cada miembro de la organización debe internalizarlo y alinearlo con sus propios valores. De este modo, el propósito se convierte en un factor diferenciador que permite a la organización posicionarse en su sector, atraer talento y fidelizar clientes.

Además, un propósito bien definido mejora el bienestar y la satisfacción de los empleados, lo que impacta en su compromiso y desempeño. Las organizaciones que logran que sus colaboradores se identifiquen con su propósito fortalecen su reputación y generan una ventaja competitiva sostenible.

En el caso de las organizaciones militares, si bien este propósito le viene impuesto, éstas pueden comunicarlas de manera que se hagan entendibles, fundamentalmente hacia el ámbito interno.

El propósito organizacional de las fuerzas armadas argentinas es proteger los intereses vitales de la nación, preservar su soberanía, integridad territorial y garantizar la defensa nacional frente a amenazas externas. Esto significa, en el caso particular de la Armada, preparar sus medios materiales y en especial a su personal para un lance determinante, cual es combatir en y desde el mar. (Herrera, 2015) (Lleó de Nalda, Montaner, & Edmonson, 2022)

Vocación, Anclas de Carrera, Contrato Psicológico, Motivación y Cultura

El desarrollo de una carrera profesional significativa en contextos organizacionales —y particularmente en instituciones como las Fuerzas Armadas— no puede desligarse de tres conceptos fundamentales: la vocación, las anclas de carrera y el contrato psicológico. Estos tres pilares constituyen un continuo que comienza con una inclinación personal y se proyecta hacia una relación duradera y mutuamente significativa con la organización.

La **«vocación»** representa el punto de partida de este proceso. Se trata de una inclinación profunda que siente una persona hacia un determinado modo de vida o actividad profesional. Esta tendencia está influenciada por tres elementos clave: gustos, intereses y habilidades. Los gustos se relacionan con aquello que la persona disfruta hacer de manera natural, sin imposiciones externas. Los intereses marcan aquello que llama la atención y que genera entusiasmo o motivación. Por último, las habilidades refieren a las capacidades desarrolladas o potenciales que permiten a una persona desempeñarse eficazmente en determinada actividad.

El proceso de descubrimiento vocacional es crucial en los primeros años de la carrera profesional, especialmente en instituciones jerárquicas y demandantes como las militares. En ese sentido, el mensaje institucional durante el proceso de reclutamiento debe ser claro, sincero y coherente con las exigencias de la vida profesional posterior. Una vocación sólida no solo facilitará la adaptación del individuo, sino que contribuirá a su permanencia y compromiso a largo plazo. (Salas, 2020)

Sin embargo, para que esa vocación sea sostenible y se transforme en una carrera motivadora, es necesario que encuentre anclaje en la actividad profesional. Aquí es donde entran en juego las **«anclas de carrera»**, un concepto desarrollado por Edgar Schein (1982), que describe las motivaciones y valores centrales que orientan el desarrollo profesional de las personas.

> Schein identificó ocho anclas de carrera que representan distintas motivaciones profundas:
> Seguridad y estabilidad, orientada a quienes valoran la permanencia y pertenencia a una organización.
> Creatividad, motivación por innovar, crear e implementar nuevas ideas.
> Independencia, deseo de autonomía en la gestión del tiempo y las formas de trabajo.
> Dirección general, inclinación por liderar, organizar y tener influencia en los equipos.
> Competencia técnica o funcional, deseo de ser

especialista y perfeccionarse en un área concreta.
> Desafío, búsqueda de situaciones complejas y retos permanentes.
> Servicio o dedicación a una causa, motivación por contribuir al bienestar social o causas significativas.
> Estilo de vida, búsqueda de equilibrio entre vida personal y profesional.

Es evidente que no todas las anclas son compatibles con todos los entornos laborales. En el caso de las Fuerzas Armadas, algunas anclas como la de seguridad, desafío, dirección o servicio pueden alinearse más naturalmente con su cultura organizacional. Por ello, los procesos de selección y formación deben identificar y fomentar la compatibilidad entre las vocaciones individuales y las oportunidades que ofrece la carrera militar.

Cuando una persona ingresa a una organización se establece de manera implícita un **«contrato psicológico»**. Este contrato no está escrito, pero regula las expectativas mutuas entre el individuo y la institución. El ingresante espera desarrollo profesional, reconocimiento, coherencia institucional y condiciones de trabajo que respeten sus valores. A su vez, la organización espera compromiso, rendimiento y alineación con su misión y cultura, y esto significa formarse para el combate, con todo el esfuerzo que ello demanda.

El éxito de esta relación dependerá de cuánto coincidan las expectativas de ambos lados, de la capacidad de adaptación mutua, y del alineamiento entre la vocación personal, las anclas de carrera dominantes y las propuestas de valor de la organización. Cuando se logra esta sintonía, se generan relaciones laborales sólidas, significativas y perdurables. (Reyes Contreras & Martinez de León, 2007)

La **«motivación»** es una de las fuerzas más determinantes en el comportamiento humano dentro de las organizaciones. Cuando nos preguntamos por qué las personas trabajan, la primera respuesta suele ser "por dinero". Este es un motivador clásico de tipo extrínseco, que se manifiesta a través de la retribución económica directa como el sueldo, aguinaldo o beneficios adicionales. Sin embargo, esta visión simplista no alcanza a comprender la complejidad que subyace a la motivación humana, especialmente en contextos laborales complejos y exigentes.

Desde una perspectiva más integral, la motivación puede entenderse como la sensibilidad de una persona hacia diferentes tipos de motivos: motivos extrínsecos, motivos intrínsecos y motivos trascendentes. Los extrínsecos están vinculados a recompensas externas como el salario o los beneficios; los intrínsecos, a la satisfacción personal que se obtiene al realizar una tarea por sí misma; y los trascendentes, al impacto que la acción tiene en otros o en una causa superior. (Pérez López, 2018)

La habilidad del líder consiste en identificar qué tipo de motivo moviliza a cada subordinado y trabajar sobre ese eje para lograr una mayor efectividad en la conducción.

En este sentido, las creencias de la alta conducción sobre la naturaleza humana y organizacional son fundamentales, ya que condicionan los mecanismos que se utilizarán para guiar y controlar el comportamiento. Se pueden identificar tres paradigmas que modelan estas creencias:
> Paradigma mecánico: considera a las personas como engranajes en una máquina, controladas mediante normas, procedimientos y estructuras rígidas.
> Paradigma biológico: concibe a las organizaciones como sistemas vivos que se adaptan, evolucionan y dependen de relaciones entre sus partes.

> Paradigma sociocultural: pone el foco en los significados compartidos, valores, símbolos y cultura organizacional. (Visca, 2004)

A la hora de valorar su empleo, los individuos consideran la Compensación Total, que no se limita solo a la dimensión monetaria. Esta incluye tanto el sueldo y los programas variables (como planes médicos, seguros o subsidios), como el Programa de Valor Cualitativo, el cual constituye el llamado **«salario emocional»**.

Este salario emocional comprende aspectos más difíciles de cuantificar, pero altamente valorados por los empleados, tales como: oportunidades de desarrollo profesional, formación continua, reconocimiento, pertenencia a proyectos desafiantes, sentido de pertenencia, flexibilidad, apoyo psicológico, conciliación vida-trabajo (en la medida de lo posible), variedad de tareas, clima laboral, respeto por la persona, calidad de vida, y otras condiciones que otorgan sentido y bienestar al trabajo cotidiano. Cuando estos factores son gestionados de manera adecuada, inciden positivamente en el clima organizacional, promueven el compromiso, retienen el talento y potencian la productividad.

Pero el salario emocional está condicionado por la cultura organizacional y es por ello por lo que en las organizaciones militares a menudo se pasa por alto frente a cuestiones como la disciplina, la jerarquía o la operatividad.

En éstas, en general y sin exclusión de las ya mencionadas se manifiesta con: reconocimiento del servicio, dar sentido de propósito a la tarea (servir a la patria o proteger a la sociedad), una tarea desafiante, sentimiento de hermandad y apoyo mutuo, oportunidad de desarrollo, estabilidad y estructura, apoyo psicológico y manejo del estrés, conciliación familiar (manejo distintivo de los permisos, viviendas militares, apoyo entre familias).

Por último, un factor que incide de manera significativa en la motivación colectiva es la «cultura organizacional». Esta representa el sistema de valores, creencias, normas y símbolos compartidos que orientan la conducta dentro de la organización hacia sus objetivos. La cultura puede motivar o desmotivar, dependiendo de cuánto se alinee con las necesidades y aspiraciones de sus integrantes. La construcción de una cultura sólida y coherente requiere liderazgo estratégico, que tenga la capacidad de modelar el comportamiento deseado a través del ejemplo, el discurso y las decisiones organizativas.

La cultura organizacional en una institución militar tiene una base muy particular que la diferencia de otros tipos de organizaciones, principalmente por su naturaleza jerárquica, su rol en la defensa nacional y la necesidad de actuar bajo condiciones de alta exigencia. Estas características a la vez se presentan como un desafío en la demanda de evolucionar para seguir siendo eficaz, ética y humana.

Propósito personal

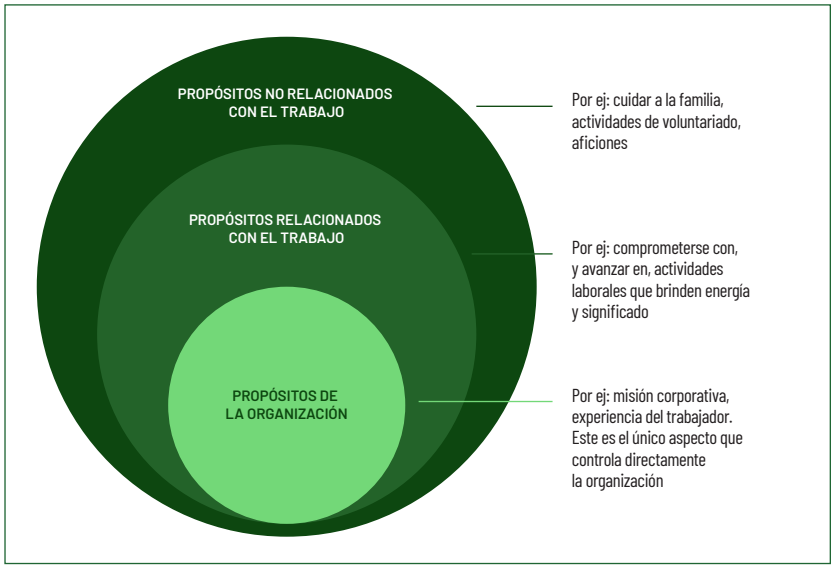
El propósito personal es una fuerza interna que otorga dirección, significado y coherencia a nuestra vida. No se trata simplemente de alcanzar metas o cumplir con expectativas externas, sino de conectar profundamente con aquello que consideramos verdaderamente importante. El propósito personal es un sentido duradero e integral sobre lo que tiene valor en la vida, y se manifiesta cuando una persona se esfuerza por lograr algo que considera significativo. (Dhingra, Samo, Schaninger, & Schrimper, 2021)

Este propósito no depende de títulos académicos, cargos profesionales ni frases inspiradoras vacías. Como indican Craig y Snook (2023), el propósito auténtico es aquello que nos define como ser humano, lo que nos impulsa y lo que los demás reconocen como nuestro sello distintivo. Es profundamente personal, muchas veces invisible, pero esencial para orientar nuestras decisiones, nuestra actitud y nuestra relación con el entorno.

Hansen y Keltner (2023) destacan que hoy muchas personas encuentran su propósito en el contexto organizacional, debido a factores como el sentido de pertenencia, la autonomía o la posibilidad de aportar a una causa colectiva. No obstante, como afirma Coleman (2023), el propósito no debe ser buscado pasivamente en el trabajo, sino construido activamente por cada persona a través de la reflexión y el sentido que les imprime a sus acciones cotidianas.

El propósito personal no es estático. Evoluciona a lo largo de la vida, al compás de nuestras experiencias, roles y circunstancias. Cambia desde la infancia hasta la adultez, desde la etapa de la formación hasta la de la

ILUSTRACIÓN 1. RELACIÓN ENTRE EL PROPÓSITO PERSONAL Y EL TRABAJO



Fuente: Dhingra, Samo, Schaninger, & Schrimper, 2021

realización personal o profesional. Esta transformación no refleja falta de compromiso, sino un proceso natural de maduración. Por ello, más que buscar "el propósito", conviene dotar de sentido lo que hacemos día a día y permitir que nuestros diversos propósitos se desplieguen y convivan.

Se sostiene que incluso los trabajos que no se asocian tradicionalmente con una vocación pueden adquirir propósito cuando son concebidos como una forma de servicio a los demás. Así, cualquier tarea (por rutinaria o sencilla que parezca) puede ser una fuente de sentido si se conecta con una intención más profunda, como es caso de las actividades dentro de las Fuerzas Armadas.

Desde una perspectiva existencial, Ramos e Iñaki Vélaez (2023) proponen tres formas de abordar el propósito: como vocación (una llamada o causa que descubrimos), como objetivo (algo que decidimos perseguir libremente), y como expresión de nuestra autonomía (la capacidad de autodeterminarnos). En todos los casos, el propósito personal actúa como una guía que orienta nuestras elecciones y fortalece nuestra motivación.

En definitiva, el propósito personal no es un destino fijo, sino un proceso continuo de autoconocimiento, elección y compromiso. Vivir desde el propósito nos permite alinear nuestra vida con nuestros valores más profundos, fortalecer nuestra resiliencia y hacer una contribución auténtica al mundo que nos rodea.

De esta manera, en el individuo actúan los siguientes aspectos relacionados:

Liderazgo

El liderazgo desempeña un rol fundamental como puente entre el propósito personal de las personas y el propósito organizacional. Lejos de limitarse a gestionar recursos o dirigir tareas, los jefes, como conductores, tienen hoy la responsabilidad de generar sentido, alinear valores y movilizar voluntades hacia una meta compartida. El desafío radica en crear un entorno donde cada individuo pueda identificar un propósito en su trabajo cotidiano y a su vez sentirse parte de una misión colectiva.

Como ya hemos visto, los empleados actuales no solo buscan estabilidad o remuneración. Aspiran a que su trabajo tenga un significado personal, que contribuya a sus aspiraciones y les permita realizar una contribución valiosa a la sociedad. El compromiso y la satisfacción laboral están profundamente ligados a la posibilidad de encontrar propósito en el trabajo. Los líderes pueden ser catalizadores de este propósito individual a través de una escucha activa, conversaciones significativas que permiten resignificar incluso las tareas más rutinarias.

Un **«liderazgo transformacional»** resulta especialmente potente en este proceso. Este tipo de liderazgo se caracteriza por inspirar y motivar a los colaboradores, transmitir entusiasmo, sentido y visión de futuro. El líder transformacional no se limita a coordinar esfuerzos, sino que moviliza motivos profundos como el logro, la afiliación o el poder, en función de la tarea y el perfil del equipo. Al actuar desde este enfoque, los líderes pueden expandir el "círculo de propósito" que une al individuo con la organización, tal como plantea Dhingra (2021) y se ve en la anterior ilustración.

En este modelo, el propósito organizacional se entiende como el núcleo desde el cual la empresa puede influir positivamente en el propósito individual. Sin embargo, dicha influencia es limitada: no se puede imponer sentido, pero sí crear las condiciones para que este emerja. La clave está en promover una cultura de escucha, reconocimiento e inclusión, donde los colaboradores se sientan seguros para expresar sus valores y conectar con los valores institucionales (Bermudez, 2021).

Cuando se logra alinear el propósito personal con el organizacional, los beneficios son múltiples: aumenta la satisfacción

laboral, mejora el desempeño y se fortalece el compromiso. Más aún, se genera una sinergia donde el crecimiento personal y el logro colectivo no se excluyen, sino que se potencian mutuamente. En este sentido, el liderazgo funciona como un puente que facilita esta conexión trascendental y guía al equipo hacia una experiencia laboral más plena y significativa.

En cuanto al **«liderazgo estratégico»**, el desafío no se limita únicamente a establecer objetivos y diseñar estrategias; también implica generar una cultura organizacional que permita alinear los propósitos personales de los miembros con el propósito organizacional. Esta tarea es particularmente crítica en instituciones con fuertes estructuras jerárquicas, como las Fuerzas Armadas, donde el compromiso y la motivación de las personas deben armonizar con valores colectivos y misiones superiores.

En este contexto, el rol del líder estratégico consiste en traducir la misión institucional en comportamientos observables, decisiones coherentes y símbolos culturales que den sentido a la acción organizacional. Este tipo de líder no impone una cultura, sino que la construye participativamente, mediante la escucha activa, la comunicación significativa y la creación de espacios donde los individuos puedan expresar sus aspiraciones.

Además, el liderazgo estratégico debe facilitar el reconocimiento de los talentos y motivaciones individuales, permitiendo que cada miembro encuentre su lugar y propósito dentro del sistema organizacional. Esto se logra a través de prácticas como la delegación con sentido, la retroalimentación constructiva y la promoción del desarrollo profesional. Así, el trabajo no se percibe como una obligación impuesta, sino como una oportunidad para desplegar el propio potencial en línea con un propósito colectivo mayor.

La cultura organizacional generada por el líder estratégico se convierte entonces en un espacio simbólico que integra, da sentido y orienta la conducta. Esta cultura es dinámica, capaz de adaptarse a los cambios del entorno, pero sin perder de vista los principios fundacionales que le dan identidad. Cuando esta cultura es coherente y viva, se convierte en el motor que alinea los propósitos individuales con los de la organización.

Construyendo puentes

En el contexto actual, donde la gestión del talento humano se ha vuelto una prioridad estratégica, la figura del líder adquiere un rol central como mediador clave entre el propósito personal y el propósito organizacional. Esta conexión no es meramente un ideal, sino una necesidad concreta para generar entornos de trabajo sostenibles, motivadores y alineados con los desafíos del entorno. La alineación entre lo que una persona busca en su vida profesional —su vocación, sus valores, su motor interno— y lo que la organización necesita y ofrece —su misión, visión y cultura— constituye uno de los pilares fundamentales para alcanzar altos niveles de compromiso, rendimiento y sentido de pertenencia.

La vocación, entendida como esa inclinación profunda hacia una actividad que se experimenta como significativa, se entrelaza con el propósito personal, es decir, con la razón de ser individual que guía decisiones, aspiraciones y conductas. Por otro lado, el propósito organizacional se refiere a la razón de existir de una institución, más allá del mero logro de objetivos económicos: es su impacto en la sociedad, su legado, su aporte colectivo. Un liderazgo efectivo reconoce estos planos y actúa como puente de integración entre ambos, de modo tal que genera espacios de trabajo donde las personas puedan expresar lo mejor de sí mismas, a la vez que contribuyen a metas superiores.

El líder cumple un rol de traductor del propósito organizacional que se vuelve tangible a través de la asignación de tareas significativas, la comunicación de metas claras y la generación de narrativas que conecten con los valores de los integrantes del equipo.

Pero, además, debe actuar como facilitador del autoconocimiento, y ayudar a los colaboradores a identificar su vocación, sus motivaciones profundas y sus anclas de carrera. Esta labor implica conversaciones significativas, espacios de reflexión, *feedback* y la promoción de experiencias que refuercen la identidad profesional.

Asimismo, el líder es el gestor por excelencia del contrato psicológico, ese conjunto de expectativas no escritas que determinan la calidad del vínculo entre la persona y la organización. Mediante el cumplimiento de promesas tácitas —como el reconocimiento, las oportunidades de crecimiento o la coherencia entre el discurso y la práctica—, se fortalece el compromiso mutuo y se refuerza la confianza. En este sentido, el salario emocional, compuesto por elementos intangibles como el clima laboral, el desarrollo personal, la autonomía o el sentido del trabajo, pasa a ser un recurso clave que el líder debe administrar con sensibilidad e inteligencia.

En definitiva, el líder como puente entre el propósito personal y el propósito organizacional no solo maximiza el potencial humano dentro de las instituciones, sino que también actúa como catalizador del bienestar individual y del logro colectivo. En tiempos donde la motivación no se garantiza únicamente por incentivos económicos, sino por la posibilidad de vivir una vida con sentido dentro del trabajo, el liderazgo se transforma en un factor diferenciador y esencial.

Una mirada cruzada con nuestras conclusiones

En el ámbito de la Escuela de Guerra Naval se viene desarrollando el Observatorio de Liderazgo, que a partir de un trabajo sistemático y en el tiempo, busca entender el liderazgo que opera en la Armada Argentina. Para ello se consulta a sus miembros sobre cuáles son los valores de la organización que consideran los más importantes, respecto del liderazgo, y que le dan contenido en la actualidad.

Según los registros analizados por el Observatorio de Liderazgo 2024, los miembros de la Armada se identifican con distinta aceptación y con particularidades que escapan al interés de este artículo los siguientes valores: Disciplina, Lealtad,

CV

OBSERVATORIO DE LIDERAZGO DE LA ESCUELA DE GUERRA NAVAL

El presente trabajo se realizó en el ámbito del Observatorio de Liderazgo, espacio académico y de investigación que funciona en la Escuela de Guerra Naval y que aborda la problemática sobre las presunciones básicas de los miembros de la organización Armada Argentina, que darían sustento al modelo de liderazgo ejercido en la actualidad.

Profesionalismo, Liderazgo, Honor, Juicio y criterio, Responsabilidad, Camaradería, Templanza, Compromiso, Vocación, entre otros.

Se destaca especialmente el valor *disciplina*, no como una sumisión ciega, sino como una aceptación racional y ética del ordenamiento institucional que permite la eficacia colectiva, la seguridad y la convivencia en entornos complejos.

Asimismo, se enfatiza la *lealtad* como vínculo de fidelidad hacia la institución y hacia los compañeros, condición indispensable para la confianza organizacional y la eficacia operativa. Esta lealtad se apoya en la *vocación de servicio,* entendida como el sentido profundo que le otorgan los integrantes a su pertenencia, y el reconocimiento de su contribución al bienestar social y a la protección de la Nación, lo cual incide en el compromiso.

Se reconoce también la necesidad de promover valores como el *profesionalismo*, indispensable para llevar adelante las actividades propias de la profesión militar y que le den marco al accionar del jefe.

Rol fundamental tiene el *liderazgo*, para inspirar y motivar a los colaboradores, y transmitir entusiasmo, sentido y visión de futuro.

Otros valores centrales en estas conclusiones fueron la *responsabilidad,* como el cuidado por lo que se hace y se decide y la «camaradería», como esa relación cordial entre los miembros que permite el trabajo en equipo y el respeto.

Del análisis de lo propuesto en el artículo y a manera de ejemplo, ya que esta es una decisión de cada organización, la cultura esperada debería responder a valores como: compromiso con la Nación, respeto por la dignidad de las personas, servicio, integridad, responsabilidad, lealtad, disciplina consciente, vocación de liderazgo, espíritu de equipo, adaptabilidad, justicia y sentido del propósito.

Como vemos, las aspiraciones de los miembros de la Armada están alineados con esta necesidad y es un camino sobre el que habrá que trabajar. ▮

BIBLIOGRAFÍA

Arola, E. (2018). *La magia de los equipos extraordinarios.* España: Profit.

-

Bermudez, D. (17 de julio de 2021). *Empresas que inspiran: cómo conectar el propósito personal con el laboral.* Obtenido de Blog Great Place to Work: http:blog.greatplacetowork.com.ar

-

Coleman, J. (2023). ¿No encuentras tu propósito? Crelo tu mismo. En Harvard Business School Publishing Corporation, *Propósito, sentido y pasión.* Serie Inteligencia emocional de HBR (págs. 23-32). Barcelona: Reverté.

-

Craig, N., & Snook, S. (2023). Del propósito a marcar diferencias. En Harvard Business School Publishing Corporation, *Propósito, sentido y pasión* (págs. 51-84). Barcelona: Reverté.

-

Dhingra, N., Samo, A., Schaninger, B., & Schrimper, M. (5 de abril de 2021). *Ayude a sus trabajadores a encontrar un sentido de propósito ... u observe como se van de su empresa.* Obtenido de McKinsey: www.McKinsey.com

-

Hansen, M., & Keltner, D. (2023). Encontrar un sentido a tu trabajo, aunque este sea aburrido. En Harvard Business Scholl Publishing Corporation, *Propósito, sentido y pasión.* Serie inteligencia emocional de HBR (págs. 1-12). Barcelona: Reverté.

-

Hedges, K. (2023). Cinco preguntas para ayudar a tus empleados a que encuentren un propósito interior. En Harvard Business School Publishing Corporation, *Propósito, sentido y pasión* (págs. 85-92). Barcelona: Reverté.

-

Herrera, D. (2015). Propósito organizacional y liderazgo Servidor vinculados a la propuesta de Valor. *Unaciencia. Revista de estudios e investigación,* 36.

-

Molinsky, A. (2023). Qué debes hacer cuando pierdas la pasión por lo que haces. En Harvard Business School Publishing Corporation, Propósito, sentido y pasión. *Serie inteligencia emocional de HBR* (págs. 13-23). Barcelona: Reverté.

-

Pérez López, J. (2018). *Fundamentos de la Dirección de Empresas.* Madrid: RIALP.

-

Ramos e Iñaki Vélaez, L. (2023). El propósito personal y sus fuentes de sentido. *Nuevas tendencias,* 2-15.

-

Reyes Contreras, Y., & Martinez de León, I. (2007). *Universidad politécnica de Cartagena.* Obtenido de Los contratos psicológicos: sus efectos en los resultados de la organización: www.repositorio.upct.es

-

Salas, J. M. (5 de 10 de 2020). *Perseguir el propósito individual en tiempos de crisis.* Obtenido de Blog ADN Aprendiendo de Negocios: www.blgroup.com.mx

-

Schein, E. (1982). *Dinámica de la carrera empresarial.* Estados Unidos de América: Fondo Educativo Interamericáno, Inc.

-

Smith, E. (2023). Cómo dar sentido a un trabajo que no es tu vocación. Descubrir las oportunidades de ayudar a los demás. En Harvard Business School Publishing Corporation, *Propósito, sentido y pasión* (págs. 33-40). Barcelona: Reverté.

-

Visca, G. (2004). Una visión de la complejidad. Motivación humana, paradigma directivo y desempeño organizacional. Material didactico. Especialización en Conducción y Gestión Estratégico. Buenos Aires: Escuela Superior de Guerra del Ejercito Argentino.

LA GUERRA DE UCRANIA EN CLAVE OPERACIONAL

ESBOZO DE UN DISEÑO OPERACIONAL

Por **CR (R) MARCELO JAVIER CALDERÓN**

El Arte Operacional soviético

Todavía es materia de debate si el arte operacional fue aplicado por primera vez por Napoleón o en la Guerra Civil estadounidense, y surge según las interpretaciones de quien lo lea o investigue. De lo que existe evidencia concreta es que fueron los teóricos militares soviéticos del período de entreguerras quienes desarrollaron la teoría del arte operacional (Blythe, 2018: 39). Cuando los niveles de conducción militar todavía eran un dilema sin resolver con claridad, el general ruso Aleksandr Svechin abordó el problema proponiendo una categoría intermedia, a la que llamó arte operacional (en ruso оперативное искусство).

Algunos atribuyen a Svechin la siguiente definición de arte operacional: *"la totalidad de maniobras y batallas en una parte dada de un teatro de acción militar dirigidas a la consecución del objetivo común, fijado como final en el período dado de la campaña"* (Svechin, 1927: 50), la cual fue reproducida por Nikolai Varfolomeev según sus notas de las cátedras de Svechin. Estas cátedras fueron compiladas en su obra que fuera publicada en 1927 "Estrategia", y en dicho libro consta un concepto similar sobre el arte operacional:

"Normalmente, este camino hacia el objetivo final se divide en una serie de operaciones separadas por pausas más o menos largas, que tienen lugar en diferentes áreas de un teatro y difieren significativamente entre sí debido a las diferencias entre los objetivos inmediatos que las fuerzas de uno aspiran temporalmente" (Svechin, 1927: 88).

Aunque este pensamiento sobre este nivel de conducción se desarrolló con la impronta soviética de asegurar su extenso territorio por medio de la batalla profunda, y de la vertical subordinación al nivel estratégico nacional, el concepto es plenamente aplicable a las campañas contemporáneas en las que la resolución de crisis no depende necesariamente del éxito militar (UK Ministry of Defence, 2008).

En la actualidad los norteamericanos entienden al arte operacional como *"el enfoque cognitivo de los comandantes y el estado mayor, respaldado por sus habilidades, conocimientos, experiencia, creatividad y juicio, para desarrollar estrategias, campañas y operaciones, y organizar y emplear fuerzas militares integrando fines, formas y medios".* (Joint Publication 5-0, 2020: IV-1); y muy similarmente en nuestra doctrina expresamos que *"es un enfoque cognitivo, tanto racional como intuitivo, creativo para desarrollar campañas u operaciones, a través de la estructuración eficiente de medios, espacios y tiempo en acciones tácticas*

con propósitos articulados" (Estado Mayor Conjunto, 2023: 31).

Podemos coincidir que el conductor del nivel operacional es el "artista que esboza un diseño" que facilita interpretar y traducir una situación, la cual abre las puertas de un futuro planeamiento. Es por ello que emplearemos los elementos del diseño operacional para comprender mejor lo que está sucediendo en Ucrania desde el 24 de febrero de 2022, en uno de los conflictos más relevantes desde el fin de la Segunda Guerra Mundial y que mantiene en vigilia al mundo entero. Paradójicamente los actores en pugna son parte del tronco genealógico soviético, herederos de ese pensamiento militar que supo delinear este nivel de conducción operativo.

Este análisis está basado en fuentes abiertas de información y se deja constancia de que no constituye una respuesta unívoca ni que no puedan efectuarse otros diseños distintos sobre esta misma situación. Todo dependerá de quién desempeñe el rol de artista operacional. Con dicha finalidad se empleó como referencia doctrinaria lo establecido en la Publicación Conjunta 20-01 "Planeamiento para la Acción Militar Conjunta Nivel Operacional", vigente en nuestras fuerzas armadas.

Fases de la campaña en Ucrania desde la escalada en febrero de 2022

Si bien los períodos o fases de una campaña surgirían como producto de un plan, es decir posterior a contar con un diseño operacional concreto, estamos describiendo un acontecimiento que ya está en desarrollo. Solo a los fines prácticos para su análisis se propone la siguiente división en fases de la "Operación Militar Especial", la cual es permeable a que se le efectúen las rectificaciones a medida que este breve estudio se vaya enriqueciendo con aportes de otros interesados en la temática:

Fase 1 : "Operación Militar Especial" / Ofensiva Rusa (24 de febrero a 25 de marzo 2022):

La maniobra operacional rusa consistió en una ofensiva aérea preparatoria, con fuego de misiles y ataques aéreos contra los sistemas aéreos y de defensa aérea, la infraestructura de comando y control (C2) y logística, seguido por una maniobra terrestre desde cuatro direcciones:

- **Norte:** su punto de aplicación fue Kiev, con dos ejes convergentes que partieron desde Bielorrusia al oeste y al este del Río Dniepr, y un tercer eje convergente a través de Chernihiv en dirección a Kiev. Las fuerzas empeñadas fueron el 35to, 36to y el 41ro Ejércitos de Armas Combinadas con Fuerzas Aerotransportadas.
- **Noreste:** sus puntos de aplicación fueron Sumy y Kharkiv, compuesto por las fuerzas de la Flota del Norte, el 6to Ejército de Armas Combinadas y el 1er Ejército de Tanques de la Guardia.
- **Este:** el esfuerzo estaba volcado sobre Donetsk y Lugansk, con el 8vo y el 49no Ejércitos de Armas Combinadas.
- **Sur:** los esfuerzos fueron dirigidos hacia Kherson y Melitopol, conformados con fuerzas del 22do Cuerpo de Ejército, el 58vo Ejército de Armas Combinadas y Fuerzas Aerotransportadas.

Las acciones más importantes fueron la Batalla de Kiev, en la que las fuerzas de Ucrania lograron evitar su ingreso por parte de Rusia, y las conquistas rusas de Kherson y localidades del sur ucraniano (Brand Ukraine, 2025a).

El 25 de marzo de 2022 el General Sergei Rudskoy realizaba la siguiente declaración oficial: "En general, se han cumplido los principales objetivos de la primera etapa de la operación. El potencial combativo de las Fuerzas Armadas de Ucrania se ha reducido significativamente, lo que permite, subrayo una vez más, concentrar los principales esfuerzos en lograr el objetivo principal: la liberación del Donbass" (MoD Russia, 2022a)

Fase 2: "Campaña del Dombas" (marzo a septiembre 2022)

En esta fase se produce el verdadero cambio de actitud estratégica rusa en la cual desiste "de facto" de buscar la desnazificación (la neutralización de la capacidad gubernamental ucraniana) para enfocarse en la desmilitarización y en la protección del Dombas.

Por ello, el esfuerzo principal fue desde el este, envolviendo las tropas ucranianas entre las provincias de Izyum, Donetsk y Luhansk; esfuerzo

secundario desde el noreste sobre Kharkiv y desde el sur sobre Kherson y Zaporizhyia.

En esta fase Rusia finaliza el Sitio de Mariupol el 20 de mayo, conquista la provincia de Lugansk el 3 de julio y comienza la Batalla por Bakhmut en agosto de 2022.

Fase 3: Contraofensiva ucraniana (septiembre a octubre 22)

Los ucranianos aprovecharon el esfuerzo principal ruso en la liberación total del Dombas para lanzar contraataques hacia el norte en dirección Kharkiv y hacia el sur en dirección Kherson que les permitieron recuperar importantes porciones de territorio.

El 10 de septiembre, el Ministerio de Defensa ruso informó sobre la retirada de sus fuerzas, afirmando que "se decidió reagrupar las fuerzas rusas estacionadas en Balakliia e Izium para aumentar los esfuerzos en el frente de Donetsk"(Lutska, 2022).

Las fuerzas rusas lograron avances graduales al sur de Bakhmut y continuaron los ataques terrestres al norte, noroeste y suroeste de la ciudad de Donetsk.

Fase 4: Consolidación del Dombas (octubre 2022 a junio 2023):

En esta fase surge por primera vez la visibilidad del comandante de tropas conjuntas rusas, y con cierto protagonismo. El general Surovikin, quien había asumido el comando el 8 de octubre de 2022, accede a dar una entrevista, donde se lo percibe muy incómodo y con una retórica guionada y acartonada. Pero alcanza a esbozar que lo que buscaba concretar era un cambio de estrategia para desgastar del enemigo y preservar a la propia tropa, en la que "no se buscan altos ritmos de avance sino proteger y preservar a cada soldado ruso mientras se aplasta al enemigo" (MoD Russia, 2022b).

El 10 de octubre las fuerzas rusas llevaron a cabo ataques con misiles masivos y coordinados impactando el centro de Kiev y otras 20 ciudades ucranianas, dirigidos principalmente contra infraestructuras críticas de energía, provisión de agua y calefacción.

El presidente Vladimir Putin afirmó que los ataques con misiles coordinados fueron una represalia por la explosión en el puente del estrecho de Kerch.

El General Surovikin ordenó la construcción de una serie de líneas defensivas a lo largo de la totalidad de la línea de contacto de 1000 km, que consiste en una combinación de trincheras, trampas para tanques, obstáculos y minas, apoyada por fuegos de artillería y misiles guiados antitanque (ATGM) para detener y/o canalizar cualquier intento de penetración ucraniano (Grisé et al., 2025).

El 11 de enero de 2023 se produce el cambio de comandante de las fuerzas rusas en Ucrania, asumiendo el General Valery Gerasimov quien a su vez mantiene sus roles de 1er Viceministro de Defensa y Jefe de Estado Mayor de las Fuerzas Armadas de Rusia, centralizando en el más alto nivel facultades que ningún otro comandante puede acceder (Calderón, 2023).

Luego de nueve meses de combates Bakhmut cae finalmente ante las fuerzas de la Compañía Militar Wagner en mayo de 2023, con una estimación de haber sufrido 20.000 bajas rusas y más de 50.000 ucranianas (Powers, 2025).

Fase 5: Contraofensiva ucraniana de verano (junio a diciembre 2023)

Con insuficiente cobertura aérea, apoyos de fuego y fuerzas medianamente adiestradas, Ucrania lanza una maniobra ofensiva sobre las posiciones fortificadas rusas, con esfuerzo principal en la zona de Zaporizhia, con la finalidad de avanzar hacia la ciudad de Tokmak y luego a Melitopol, centro logístico para las fuerzas rusas. Los esfuerzos secundarios fueron con dirección a Berdiansk y Bakhmut. La defensa rusa pudo negar accesos y canalizar los ataques con éxito, gracias a las profundas y extensas zonas de barreras preparadas lo que redujo el ritmo de avance e impidió la concreción de maniobras, obligando a las fuerzas ucranianas a empeñarse en combates posicionales de gran desgaste en bajas humanas y de material (Zafra y McClure, 2023).

Fase 6: Estabilización del frente (diciembre 2023 a mayo 2024)

Rusia ha ejecutado una ofensiva aérea sobre la infraestructura crítica de Ucrania. La estabilización del frente la lleva a cabo desde seis direcciones distribuidas en toda la línea de contacto, mediante agrupamiento de fuerzas Sever (Norte), Zapad (Oeste), Tsentr (Centro), Yug (Sur), Vostok (Este) y Dnepr (Kyiv Post, 2024). Sus acciones principales consisten en golpear la profundidad de las fuerzas en contacto, sus reservas y apoyos de fuego. En esta fase Rusia conquista Avdeyevka en febrero, Ocheretyne en abril y comienza el asalto a Chasiv Yar en abril de 2024 (MoD Russia, 2024).

Fase 7: Ofensiva rusa de desgaste (mayo 2024 a ene 2025)

Rusia mantiene las acciones ofensivas aéreas sobre la infraestructura crítica ucraniana, logrando afectar su funcionamiento en un 70%. El 10 de mayo las fuerzas rusas penetraron en la zona fronteriza cerca de Kharkiv, controlando las localidades de Lyptsi, Starytsia y Vovchansk, tratando de avanzar con el grupo de fuerzas Sever, mientras las fuerzas ucranianas intentan apuntalar un frente debilitado (Kirby, 2024).

En agosto de 2024 las fuerzas ucranianas realizaron una incursión para conquistar una importante porción de territorio ruso en la región de Kursk, de

aproximadamente 1000 km2. La finalidad de dicha conquista sería para contar con un recurso de negociación que le permita a Ucrania recuperar su integridad territorial (Salgado, 2025). Lentamente esa ganancia en terreno fue perdiéndose ante la contraofensiva rusa en su propio territorio hasta quedar prácticamente neutralizada.

Fase 8: Operaciones de desgaste (enero 2025 - presente)

Ucrania ejecuta acciones aéreas con drones de largo alcance sobre territorio ruso, causando importantes daños sobre infraestructura crítica de energía y logística. Los grupos de fuerzas rusos concretan avances de poca profundidad y de gran desgaste mutuo, aprovechando la superioridad de masa de fuerzas sobre la debilitada defensa ucraniana. Los avances más visibles fueron en Kharkiv, Kupiansk, Chasiv Yar, Pokrovsk.

En los primeros días de junio Ucrania concreta una audaz infiltración de drones para golpear los sistemas aéreos estratégicos rusos, en lo que se denominó "Operación Telaraña", causando graves daños a sus sistemas de proyección misilísticos. También Ucrania ejecuta una nueva voladura en uno de los pilares del Puente de Kerch, dejando graves daños estructurales en uno de sus segmentos.

Una aproximación a los Elementos del Diseño Operacional aplicados en el conflicto en Ucrania.

Tanto el sentido común como la doctrina militar coinciden en que cualquier proceso de planeamiento surge desde el más alto nivel de conducción emanando directivas hacia los niveles inferiores, las cuales van contando con mayor detalle a medida que esos planes u órdenes continúan bajando hacia los estratos de ejecución. En el caso del conflicto en Ucrania los actores del nivel estratégico como Vladimir Putin y Volodimir Zelenski representan el máximo nivel (Estratégico Nacional) y junto con sus principales asesores (consejo de seguridad nacional, gabinete ministerial, etc.) elaboran sus condiciones a conseguir, las metas a alcanzar y los efectos a lograr (Estado Mayor Conjunto, 2023: 66).

Considerando lo expuesto es que observaremos en el siguiente diseño una sucesión de ideas, datos y conclusiones que pretende respetar el proceso metodológico del Diseño Operacional, buscando reflejar mi interpretación personal de las causas inmediatas desencadenantes de la escalada del 24 de febrero de 2022 y el desarrollo de los sucesos más relevantes en el nivel operacional, discriminándolos a través de los elementos enunciados en el capítulo 2 del PC 20-01. Los primeros cinco elementos del diseño fueron obtenidos de discursos, declaraciones y documentos de la dirigencia de ambas partes contendientes, mientras que el resto, expuesto en formato de tabla, es elaboración personal.

CV

MARCELO JAVIER CALDERÓN

Es coronel retirado del Ejército Argentino. Licenciado en Estrategia y Organización (UNDEF) y Doctor en Relaciones Internacionales (Universidad del Salvador). Fue Agregado de Defensa, Militar, Naval y Aeronáutico en la Federación de Rusia (2018 – 2021).

	RUSIA	UCRANIA
Criterios de Terminación de la Guerra	> Que se establezca el estatus de neutralidad de Ucrania, para que no ingrese a la OTAN ni a la UE. > Que Ucrania se someta a un proceso de desarme. > Que se proteja la lengua rusa en territorio ucraniano. > Se concrete la "Desnazificación" de Ucrania. > Reconocimiento de Crimea como territorio de la Federación de Rusia. > Reconocimiento de Donetsk y Lugansk (Simpson, 2022).	> Seguridad radiológica y nuclear. > Seguridad alimentaria. > Seguridad energética. > Liberación de todos los presos y deportados. > Implementación de la Carta de las Naciones Unidas y restablecimiento de la integridad territorial de Ucrania y del orden mundial > Retirada de las tropas rusas y cese de las hostilidades. > Justicia. > Protección inmediata del medio ambiente. > Prevención de la escalada. > Confirmación del fin de la guerra (Brand Ukraine, 2025b).
Estado Final Estratégico Deseado	Que Rusia disponga de las garantías de seguridad ante los países de Occidente y la OTAN de un "Status Quo Ante" la firma del Acta Fundacional OTAN – Rusia de 1997 (Arciniegas, 2021).	Que el territorio de Ucrania se encuentre integrado y completo; que forme parte de la Unión Europea y de la OTAN; y que cuente con garantías de seguridad ante una posible amenaza rusa.
Objetivo Estratégico Nacional	Impedir una mayor expansión de la OTAN hacia el Este (Sky News, 2021) y el despliegue de sus sistemas de armas en las fronteras rusas (Presidencia, 2014).	Preservar la soberanía, restituir el control territorial, garantizar la seguridad futura y crear las condiciones para poder ingresar a la OTAN y a la Unión Europea (Presidencia, 2021).
Estado Final Estratégico Militar Deseado	Las Fuerzas Armadas de Rusia (FAR) han neutralizado las capacidades militares ofensivas de Ucrania, establecido el control ruso o prorruso sobre el Dombás y otras regiones estratégicas, y han impuesto una reconfiguración del sistema político-militar ucraniano que lo aleje de Occidente y elimine su interoperabilidad con la OTAN.	Las Fuerzas Armadas de Ucrania (FAU) han neutralizado la capacidad militar ofensiva de Rusia contra su territorio, han restaurado el control efectivo sobre todas las áreas ocupadas, cuentan con una fuerza nacional interoperable con la OTAN y han creado las condiciones necesarias para una solución negociada del conflicto.
Objetivo Estratégico Militar	Desmilitarización y la desnazificación de Ucrania, para proteger a las personas que han sido objeto de intimidación y genocidio por parte del régimen de Kiev durante ocho años (Warta Publika, 2022).	Restaurar la integridad territorial, degradar la capacidad militar rusa y preparar una defensa interoperable con aliados estratégicos (Presidencia, 2021).
Estado Final Operacional Deseado	Las FAU han sido neutralizadas en su capacidad de combate organizada; el aparato gubernamental central de Ucrania ha sido desarticulado o ha perdido el control efectivo del país; las principales ciudades, incluidos centros de poder político y logístico, se encuentran bajo control ruso.	Las FAU han restablecido el control sobre sectores clave del territorio ocupado, han degradado significativamente la capacidad ofensiva y logística de las fuerzas rusas en el teatro, y mantienen una situación que ofrece ventajas para una resolución negociada del conflicto.
Objetivos Operacionales	> Destruir la capacidad ofensiva y defensiva de las FAU. > Desintegrar el funcionamiento gubernamental ucraniano.	Recuperar el control de las áreas ocupadas; degradar la capacidad de combate y apoyo logístico de las FAR en el teatro, y crear las condiciones favorables para una negociación.

	RUSIA	UCRANIA
Efectos deseados	> Paralización de las FAU (C2, logística, moral). > Desorganización del gobierno central en Kiev. > Control territorial del Dombás, Kherson, Zaporizhia y corredor a Crimea. > Disuasión de otros países exsoviéticos frente a la OTAN. > Fragmentación de la voluntad nacional ucraniana.	> Defensa exitosa de Kiev y principales centros urbanos. > Recuperación territorial. > Debilitamiento progresivo de las capacidades rusas. > Fortalecimiento del apoyo internacional (militar, político y económico). > Elevación de la moral nacional y cohesión de la población.
Efectos no deseados	> Alta resistencia militar y moral de Ucrania. Cohesión política e identidad nacional ucraniana. > Consolidación del apoyo militar occidental hacia Ucrania. > Sanciones económicas severas yaislamiento internacional. > Bajas humanas, morales y materiales. > Daños colaterales y crímenes de guerra que socavan legitimidad.	> Destrucción masiva de infraestructura crítica. > Pérdidas civiles y desplazamiento interno de millones de personas. > Dependencia estructural del apoyo occidental (armamento, munición). > Agotamiento de personal entrenado. > Impacto económico prolongado (recesión, necesidad de reconstrucción externa).
Centro de Gravedad (CDG)	Fase 1: Capacidad ofensiva en profundidad. Resto de la campaña: Defensa en profundidad mediante un sistema de armas combinadas con apoyo de fuegos masivos, sostén logístico y rotación de fuerzas.	Fase 1: Sistema de Comando y Control estratégico y operacional, ubicado en Kiev. Resto de la campaña: Apoyo militar, logístico y financiero de los países de Occidente.
Capacidades criticas	> Producción y reposición continua de munición, blindados, drones y artillería. > Fortificación extensiva del frente y defensa en profundidad. > Sostén logístico desde territorio nacional. > Rotación de fuerzas mediante movilización parcial y reclutamiento constante. > Integración de medios de guerra electrónica, drones, reconocimiento y artillería.	> Capacidad de obtención y empleo de armamento occidental. > Integración operativa con inteligencia OTAN. > Redes logísticas internas y externas activas. > Reemplazo de pérdidas con entrenamiento aliado. > Sostenimiento de operaciones combinadas.
Requerimientos críticos	> Infraestructura logística protegida (ferrocarriles, depósitos de munición, cruces de ríos). > Mano de obra suficiente y disciplinada (reservistas, prisioneros, contratistas). > Coordinación eficiente entre niveles táctico y operacional.	> Infraestructura de recepción logística. > Transferencia continua de recursos clave. > Mando flexible para integrar capacidades. > Mantenimiento de material bélico de origen soviético y OTAN. > Enlace y vías de comunicación seguras con países OTAN. > Sistemas de armas aéreos (aeronaves, UAV).
Vulnerabilidades Críticas	> Escasos corredores logísticos claves. > Fragilidad moral en tropas mal entrenadas y forzadas a combatir. > Exposición de centros industriales y logísticos a misiles de largo alcance o sabotaje. > Rigidez en la toma de decisiones por estructura verticalizada y burocrática.	> Escasa capacidad de defensa aérea y su sistema de artillería. > Posible fatiga o fragmentación del apoyo occidental. > Logística expuesta a ataques. > Reemplazo lento de personal especializado. > Vulnerabilidad de la red C2 si es atacada electrónicamente.

	RUSIA	UCRANIA
Puntos decisivos	> Kiev y Base Aérea Hostomel (en Fase 1) > Sistema C2 ucraniano (en Fase 1) > Lugansk > Melitopol y corredor a Crimea. > Tokmak > Zaporizhia y su central nuclear. > Mariupol > Berdiansk > Dzhankoi > Puente de Kerch > Nodos logísticos profundos (Bryansk, Kursk, Belgorod, Rostov del Don).	> Kiev (Fase 1). > Kharkiv > Kherson > Lugansk. > Donetsk > Corredor logístico Melitopol – Tokmak > Centros y nodos logísticos en Dzhankoi, Rostov del Don, Belgorod y Kursk.
Líneas de operaciones y de esfuerzo (Fase 1)	LDO: > Norte: Bielorrusia - Kiev. > Noreste: Belgorod - Sumy y Kharkiv. > Este: Donetsk y Lugansk. > Sur: Crimea - Kherson y Melitopol. LDE: > Ciberguerra y guerra electrónica. > Narrativa de desnazificación. > Desinformación y control reflexivo.	LDO: > Kiev – Hostomel - Irpin. > Sumy - Kharkiv. > Sloviansk - Severodonetsk. > Kherson – Mykolaiv LDE: > Continuidad de gobierno, comando y control. > Resistencia nacional y moral. > Apoyo internacional. > Ciberguerra, guerra electrónica e infraestructura crítica.
Líneas de operaciones y de esfuerzo (resto de la campaña)	LDO: > Norte: Lugansk – Kupiansk. > Este: Donetsk – Bakhmut - Kramatorsk. > Sur: Crimea - Melitopol – Tokmak – Zaporizhia. LDE: > Apoyo logístico e industrial. > Guerra de información. > Guerra de recursos energéticos. > Incidencia sobre infraestructura crítica	LDO: > Noreste: Kharkiv – Kupiansk – Lugansk. > Este: Sloviansk – Bakhmut - Donetsk. > Sur: Zaporizhia – Tokmak - Melitopol. LDE: > Apoyo internacional sostenido. > Guerra de información y moral nacional. > Interoperabilidad OTAN. > Ciberguerra, guerra electrónica e infraestructura crítica.
Aproximación (directa / indirecta)	Fase 1: Aproximación Directa Operación tipo "Blitzkrieg" e intento de "decapitación" política sobre Kiev. Resto de la campaña: Aproximación Indirecta. Defensa en profundidad, desgaste sostenido y superioridad de fuego. Ataque a la voluntad nacional ucraniana (vía infraestructura crítica). Interdicción del apoyo occidental (intentos de dividir OTAN, desinformación). Apoyo a movimientos internos disidentes y campañas de propaganda.	Fase 1: Aproximación Indirecta Defensa en ejes críticos, dispersión. Protección del sistema político-militar nacional. Ataques localizados a logística y columnas rusas. Resto de la campaña: Aproximación Directa e Indirecta. Ataques a la logística y C2 rusos. Golpes al COG ruso desde los requerimientos críticos. Contraofensivas localizadas y empleo de elementos mecanizados para romper líneas defensivas.
Anticipación	Fase 1: subestimó la resistencia ucraniana y la velocidad de reacción occidental.	Alta anticipación desde febrero 2022 gracias a inteligencia occidental.

	RUSIA	UCRANIA
Anticipación	Resto de la campaña: anticipó una guerra larga y adaptó su industria militar y reservas humanas.	Anticipó ataques contra Kiev, Hostomel y su C2; preparó redes redundantes y maniobra defensiva escalonada.
Objetivo Estratégico Militar	Fase 1: Sobre extensión operacional. Resto de la campaña: reducción del alcance y potenciación de la defensa en profundidad.	Fase 1: empleo de alcance interior para una defensa efectiva. Resto de la campaña: Expande alcance con precisión y logística de países de Occidente.
Punto culminante	Culminación en Kiev en marzo 2022: redespliegue hacia el Dombás.	Culminación en la contraofensiva de agosto 2023: estancamiento por falta de superioridad aérea, sistemas contra minas y logística insuficiente. Disminución y agotamiento de la capacidad de defensa aérea, antimisiles y suministros desde Occidente en 2024.
Enlace operacional	Fase 1: Enlace débil. El objetivo de "desnazificación" no se conectaba claramente con los medios ni con los efectos tácticos. Resto de la campaña: mayor coherencia: Defender territorios, degradar al enemigo, inducir negociación o congelamiento del conflicto.	Enlace muy sólido: cada objetivo estratégico (restaurar soberanía) se vincula directamente con objetivos operacionales claros (recuperar terreno, erosionar logística) y tareas tácticas (contraofensivas, interdicción con HIMARS).
Fuerzas	> Fuerzas mecanizadas y blindadas. > Fuerzas aerotransportadas. > Artillería de largo alcance. > CMP Wagner. > Rosgvardia. > Fuerzas estratégicas (de misiles, aeroespaciales)	> Fuerzas mecanizadas y de maniobra. > Defensa territorial. > Artillería occidental. > Drones y guerra electrónica.. > Fuerzas de operaciones especiales. > Sistema de C2 e inteligencia.
Funciones	> Ofensiva mecanizada inicial (fase 1) > Defensa en profundidad; capas fortificadas. > Fuegos masivos y negación de área. > Represión de resistencia local; control civil > Sostén logístico mediante nodos profundos. > Disuasión nuclear; guerra energética, narrativa.	> Defensa urbana y estratégica (fase 1) > Contraofensiva territorial limitada. > Interdicción profunda sobre logística rusa > Protección del COG nacional y continuidad del gobierno > Movilización nacional y resiliencia social > Adaptación doctrinal y técnica a estándares OTAN

Reflexiones finales

Este trabajo no pretende imponer un criterio rector, sino que busca generar el interés por el análisis de los conflictos desde el punto de vista militar en el nivel operacional y puede ser considerado como un estudio de caso de "la Guerra en Ucrania". Como tal, procura realizar un ejercicio intelectual que cualquier asesor o conductor del Nivel Operacional puede llevar a cabo, con los lógicos debates, aciertos y errores que esto conlleva.

Tanto el tratamiento de las Fases como el del Diseño Operacional son sintéticos, entendiendo que puede haber ciertas omisiones o fragmentaciones de sucesos que reduzcan la información, ya que el propósito de esta síntesis es que todo el procedimiento analítico pueda ser incluido en la extensión del presente el artículo.

Considerando el caso de "la Guerra en Ucrania", estamos observando un conflicto del siglo XXI en pleno continente europeo, en el que ninguna alianza ni organización de seguridad multilateral tiene implicancia directa, con abordajes conceptuales similares a la Primera Guerra Mundial como el desgaste posicional, pero con procedimientos y destrezas de alta tecnología y letalidad como el empleo de masivo de sistemas no tripulados (drones) con un creciente espectro de finalidades. Esta tecnología cambiante y adaptativa en el desarrollo de armas fue la razón principal del cambio en la estrategia, la táctica, las formas y los métodos de empleo de las tropas, como una especie de nueva guerra de maniobras basada en una guerra científica y tecnológica.

La lectura del cuadro comparativo nos deja entrever una de las características de los conflictos de la actualidad que nos compartiera el general ruso Valery Gerasimov, que es la dificultad de diferenciar los niveles de conducción en función de las acciones y sus finalidades. Y es este tipo de entrenamiento intelectual lo que nos permitirá identificar las posibles soluciones a los problemas militares que nos toque enfrentar, como parte de nuestra preparación en el rol de asesores y decisores en el próximo conflicto armado, para lograr la victoria.

BIBLIOGRAFÍA

ARCINIEGAS, Yurany (2021). "Rusia exige a la OTAN que abandone Europa del Este, EE. UU. responde que es´inaceptable´". France 24, sitio web, publicado el 17 de diciembre. París, Francia. https://www.france24.com/es/europa/20211217-rusia-otan-estados-unidos-ucrania

-

BLYTHE, Wilson (2018). "A History of Operational Art". Military Review, November – December, pp. 39. Fort Leavenworth, Kansas, EEUU. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/ND-18/Blythe-Operational-Art.pdf

-

BRAND UKRAINE (2025a). "How long does Russia's aggression against Ukraine really last?". Official web site. Kiyv, Ucrania. https://war.ukraine.ua/the-histrory-of-russian-aggression-in-ukraine/

-

BRAND UKRAINE (2025b). "What is Zelenskyy's 10-point peace plan?". Official web site. Kiyv, Ucrania. https://war.ukraine.ua/faq/zelenskyys-10-point-peace-plan/

-

CALDERON, Marcelo (2023). "Gerasimov y el conflicto en Ucrania: el riesgo de acumular poder". LinkedIn, sitio web, publicado el 13 de febrero. Buenos Aires, Argentina. https://www.linkedin.com/pulse/gerasimov-y-el-conflicto-en-ucrania-riesgo-de-poder-calder%C3%B3n

-

ESTADO MAYOR CONJUNTO (2023). "Planeamiento para la Acción Militar Conjunta - Nivel Operacional". Ministerio de Defensa, Publicación Conjunta 20-01. Buenos Aires, Argentina.

-

GRISÉ, Michelle; COZAD, Mark; DOWD, Anna; HVIZDA, Mark; KENNEDY, John; KEPE, Marta; LATAILLADE, Clara de; MARCINEK, Krystyna y WOODWORTH, David (2025). "Russia's Military After Ukraine: Potential Pathways for the Russian Armed Forces". Rand Corporation. Santa Monica, California, EEUU. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2700/RRA2713-1/RAND_RRA2713-1.pdf

-

KIRBY, Paul (2024). "Key weeks ahead for Russia's war in Ukraine". BBC News, sitio web, publicado el 17 de mayo. Londres, Reino Unido. https://www.bbc.com/news/articles/c2jd3k1zyjro

-

KYIV POST (2024). "Russia Forms New 'North' Military Group in Regions Bordering Ukraine". Kyiv Post, sitio web, publicado el 15 de abril. Kiev, Ucrania. https://www.kyivpost.com/post/31127

-

LUTSKA, Veronika (2022). "Ukrainian forces liberated most of the Kharkiv region in a rapid counter-offensive". War in Ukraine, official web site, publicado el 18 de septiembre. Kiev, Ucrania. https://war.ukraine.ua/articles/ukrainian-forces-liberated-most-of-the-kharkiv-region-in-a-rapid-counter-offensive/

-

MoD RUSSIA (2022a). "Speech of the Head of the Main Operational Directorate of the General Staff of the Armed Forces of the Russian Federation Colonel General Sergei Rudskoy on the course of a special military operation". Ministry of Defense of Russia, canal de Telegram (en inglés), publicado el 25 de marzo. Moscú, Rusia. https://t.me/mod_russia_en/409

-

MoD RUSSIA (2022b). "Notes of the interview with Commander of Joint Group of Troops (forces) in special military operation area General of the Army Sergei Surovikin". Ministry of Defense of Russia, canal de Telegram (en inglés), publicado el 18 de octubre. Moscú, Rusia. https://t.me/mod_russia_en/4597

-

MoD RUSSIA (2024). "The Units of the Tsentr Group of Forces have taken full control of Avdeyevka". Ministry of Defense of Russia, canal de Telegram (en inglés), publicado el 18 de febrero. Moscú, Rusia. https://t.me/mod_russia_en/12447

-

POWERS, Bryan (2025). "The Battle for Bakhmut: When Is a Battlefield Loss a Strategic Victory?". U.S. Army, sitio web, publicado el 31 de marzo. Washington, EEUU. https://www.army.mil/article/284124/the_battle_for_bakhmut_when_is_a_battlefield_loss_a_strategic_victory

-

PRESIDENCIA (2014). "Sobre la Doctrina Militar de la Federación de Rusia". Decreto Nro 2976 del 25 de diciembre, Art. 12, a) y 34. Moscú, Rusia. https://docs.cntd.ru/document/420246589

PRESIDENCIA (2021). "Sobre la estrategia de seguridad militar de Ucrania". Decreto Nro 121 del 25 de marzo. Kiev, Ucrania. https://www.president.gov.ua/documents/1212021-37661

-

SALGADO, Samuel (2025). "Fuerte batalla por Kursk en la antesala de eventuales negociaciones de paz entre Ucrania y Rusia". France 24, sitio web, publicado el 9 de marzo. París, Francia. https://www.france24.com/es/europa/20250309-fuerte-batalla-por-kursk-en-la-antesala-de-eventuales-negociaciones-de-paz-entre-ucrania-y-rusia

-

SIMPSON, John (2022). "Rusia y Ucrania: las demandas que Putin puso sobre la mesa para detener la invasión en una llamada con el presidente de Turquía". BBC News, sitio web, publicado el 18 de marzo. Londres, Reino Unido. https://www.bbc.com/mundo/noticias-internacional-60789848

-

SKY NEWS (23 de diciembre de 2021). "Russia's Putin: The US is parking missiles ´on the porch of our house´" [archivo de video], minuto 0:45. YouTube. https://www.youtube.com/

-

SVECHIN, Aleksandr (1927). "Strategy". Traducido en 1991. East View Information Services, pp. 50. Minneapolis, Minnesota, EEUU.

-

UK MINISTRY OF DEFENCE (2008). "Campaigning". Joint Doctrine Publication 01, 2nd edition. Londres, Reino Unido.

-

US JOINT CHIEFS OF STAFF (2020). "Joint Planning". Joint Publication 5-0, pp. IV-1. Washington, EEUU.-zwatch?v=MOkI2XgZIw0&list=PLAQbqxdfLuig7NZwNGJZektSbw1D8t8BR&index=2

-

WARTA PUBLIKA (24 de febrero de 2022). "Vladimir Putin's Speech Before Declaring Special Military Operations in Ukraine" [archivo de video], minuto 20:25. YouTube. https://www.youtube.com/

-

ZAFRA, Mariano y McCLURE, Jon (2023). "Four factors that stalled Ukraine´s counteroffensive". Reuters, sitio web, publicado el 21 de diciembre. Londres, Reino Unido. https://www.reuters.

REVISIÓN DEL CICLO EDUCATIVO DE ESTRATEGIA MILITAR

Por **BM (R) ALEJANDRO MORESI**

Palabras Clave:
> Estrategia
> Educación
> Competencias
> Analista

Introducción

Durante el 2023, la carrera de Maestría en Estrategia Militar de la Escuela Superior de Guerra Conjunta inició los procesos de acreditación de su segundo ciclo, tal como lo establece la Comisión Nacional de Evaluación y Acreditación Universitaria (CONEAU). La tarea implicó una completa revisión de la carrera, la actualización de programas y la documentación presentada.

La Estrategia Militar es un arte y ciencia en cambio permanente, y más aún en el siglo XXI, cuando la cuarta revolución tecnológica ha introducido nuevas disciplinas, como aquellas relacionadas al uso de la Inteligencia Artificial, cuyo impacto continúa generando discusiones en diferentes áreas del quehacer humano –incluyendo la militar, donde se aprecian las ventajas que conlleva, pero también se cuestionan sus sesgos.

Anualmente, el cuerpo docente revisa los contenidos y aspectos que hacen a la formación de aquellos que aspiran al título de Magister en Estrategia Militar. Esta revisión se realiza teniendo como guía dos preguntas base: **¿Cuáles son las habilidades que requerirán los estrategas de los próximos diez a veinte años?** Y ¿El programa de materias y ejercitaciones dota de esas habilidades a los alumnos? A partir de ellas, se piensa cómo actualizar y mejorar los contenidos y ejercitaciones de los actuales y futuros maestrandos, lo cual requiere adaptar los procesos y procedimientos educativos de los futuros magister y reanalizar las habilidades, para que a partir de ello se hagan las propuestas adecuadas.

Con ese fin, se trabajó sobre los autores contemporáneos de estrategia militar y de la educación en dicha disciplina, tratando de extraer lo que se requiere del pensador y analista estratégico. Como parte del desafío que imponen las nuevas tecnologías, se consultaron programas de inteligencia artificial de uso libre, y finalmente se involucró a los alumnos actuales de la Maestría en Estrategia Militar.

Metodología

El siguiente análisis se basó en tres fuentes: Los autores estratégicos –que ofrecen un pensamiento crítico sobre la formación de analistas y especialistas en estrategia militar–; las nuevas tecnologías del conocimiento –ChatGPT 3.5, GEMINI y PILOT–; y por último los cursantes

actuales de la Maestría en Estrategia Militar de la ESGCFFAA, a quienes como parte del taller de "conflictos nuevos y futuros" se les preguntó *¿Cuáles consideran que serían las habilidades o competencias que ellos desearían tener para enfrentar estos conflictos?* Luego, se realizó un trabajo de síntesis sobre las respuestas obtenidas, para acotarlas a diez habilidades o competencias que resumen la postura de los actuales maestrandos.

A través de la articulación de estas tres fuentes, se estableció un marco común que se contrastó con el plan curricular de la carrera, para intentar responder la siguiente pregunta: **¿La propuesta de la Maestría en Estrategia Militar de la ESCGFFAA provee las adecuadas herramientas para los futuros analistas y asesores en materia de Estrategia Militar?**

Desarrollo

Los estrategas no se desarrollan simplemente por sus condiciones naturales, sino que es una demanda de las organizaciones dotarlo de las mejores herramientas dentro de los sistemas educativos y de gestión, que alienten la evolución de talentos tendientes a generar profesionales de la estrategia más creativos y adaptables.

La problemática en la formación de analistas estratégicos debe orientarse hacia sistemas de educación continua, bajo un concepto de aprendizaje dinámico y permanente, complementado con la observación de especialistas en ciencias humanas. De este modo, es posible la selección temprana de potenciales estrategas orientarlos sobre aspectos como la gestión de nuevos talentos y desarrollar la tendencia a la innovación como parte de los objetivos de las carreras orientadas a la estrategia (Williamson y Millet, 1996).

Estos aspectos parten de considerar a la estrategia como un conocimiento necesario para respaldar los enfoques nacionales u organizacionales hacia los desafíos geopolíticos, tecnológicos y demográficos en evolución, considerando esta es:

> Es necesaria para implementar una estrategia, como aglutinador de los elementos de poder en la concepción de planes y programas de seguridad y defensa nacional;
> Resulta determinante en desarrollo y la ejecución de estrategias futuras a través de la inteligencia biológica y la capacidad de los analistas de explotar al máximo y de manera adecuada la inteligencia artificial en el desarrollo, ensayo, implementación y adaptación de propuestas estratégicas;
> Aporta a la opciones y caminos a la incertidumbre del enigma de la guerra futura en una era de ventajas transitorias. La competencia violenta es la regla en toda la naturaleza. Los humanos no son una excepción a esta pauta" (Gat, 2006);
> Constituye un adecuado ensamble entre lo racional e intuitivo, por eso hablamos de ciencia y arte para "la determinación de los intereses vitales de una nación, las cosas que son esenciales para su seguridad, sus propósitos fundamentales en sus relaciones con otras naciones y sus prioridades con respecto a los objetivos" (Craig y Gilbert, 1986);
> Y es parte integral en el planeamiento de todo el espectro de la competencia y el conflicto, donde la pertinencia de constructos como paz y guerra, tan frecuentes en occidente devienen en una realidad de competencia continua.

El tratamiento de estos aspectos deriva de la pregunta por **¿Qué habilidades pretendemos de los analistas estratégicos para gestionar en el futuro?** Bajo este título se realizaron los trabajos que permitieron definir la Tabla 2: Resumen final para la evaluación.

Habilidades Clásicas

Las habilidades clásicas son una serie de aspectos considerados,

de manera discrecional, como deseables para los futuros analistas estratégicos. Estos aspectos fueron obtenidos a través de la consulta de los distintos autores mencionados previamente, y constituyen las características que se espera que reúna un analista estratégico como resultado de la carrera. Entre ellas se encuentran las siguientes:

> Conocimientos y experiencia en geopolítica, relaciones internacionales, tecnología y ciencias duras. Con los cuales se espera que el analista genere un enfoque holístico y multifacético.
> Adaptación a un entorno global cambiante, donde las ventajas son transitorias y a veces subrepticias, por los cual su detección requiere habilidades avanzadas en tecnología, análisis de datos y pensamiento estratégico.
> Capacidad de liderazgo que le permita realizar trabajos interagenciales y compartir con equipos diversos, interdisciplinarios y multinacionales.
> Una combinación de experiencia, conocimiento e intuición que lo haga adaptable y resiliente a los desafíos cambiantes en el ámbito de la defensa y la seguridad, sosteniendo una ética incontrastable.
> Conocimiento de tecnología, análisis de datos, pensamiento estratégico, inteligencia, liderazgo, comunicación, adaptación y evaluación de riesgos.
> "La combinación entre imaginación creativa y dinámica energía y la capacidad de explotar la oportunidad con excelentes resultados es también destacable" (Guderian, 1954)[1].
> Una *capacidad dual*: en primer lugar, de anticipar problemas y diseñar soluciones, y luego de hacer que la gente ejecute los planes resultantes (Ricks, 2013)[2].

De forma general, se podría decir que la mirada clásica pretende que el futuro analista estratégico sea un individuo que pueda diseñar, influir e implementar la estrategia nacional y militar de forma holística, así como orquestar todos los instrumentos del poder nacional en un plan coherente para lograr los objetivos nacionales, en un período en el que la competencia es constante y las ventajas son transitorias; con manejo y conocimiento de las capacidades de las herramientas que le permitan un diseño adecuado y equilibrado de fuerzas militares operacionalmente eficaces, para garantizar la capacidad de alinear los conceptos y decisiones estratégicas y operacionales actuales y futuras con las tecnologías disponibles (Murray y Millet, 20120).

1. Aporte de GD Gustavo Motta
2. Aporte de GD Gustavo Motta
3. Se refiere al empleo de sistemas de IA bajo el concepto de "golpe de Ojo Humano con un ciber-vistazo de datos fusionados que apoyen la toma de decisiones intuitivas" (Ryan, 2019).
4. Mick Ryan, op. *Cit.*
5. Frank Hoffman, op.Cit.

A partir de estas ideas fuerzas se plasmaron **10 habilidades básicas requeridas**:

1. Conocimiento tecnológico extensamente cultivado.
2. Gestión de la adaptación organizacional, tanto en lo militar como civil.
3. Capacidad de lidiar y dirigir el cambio.
4. Disposición para aprender cosas nuevas, sosteniendo bases éticas sólidas.
5. Resiliencia y equilibrio mental en situaciones inusuales.
6. Comprender y conceptualizar las claves de la cultura institucional.
7. Comprender el creciente ritmo de cambio del entorno.
8. Capacidad para operar interfases hombre-máquina en apoyo de las decisiones estratégicas[3].
9. Conocer cómo garantizar mecanismos de control de calidad en el entorno de apoyo a la toma de decisiones (Hoffman, 2019).
10. Incorporar la educación continua y la re-educación rápida, que considere la tecnología algo esencial.

Habilidades Versión Cibernética

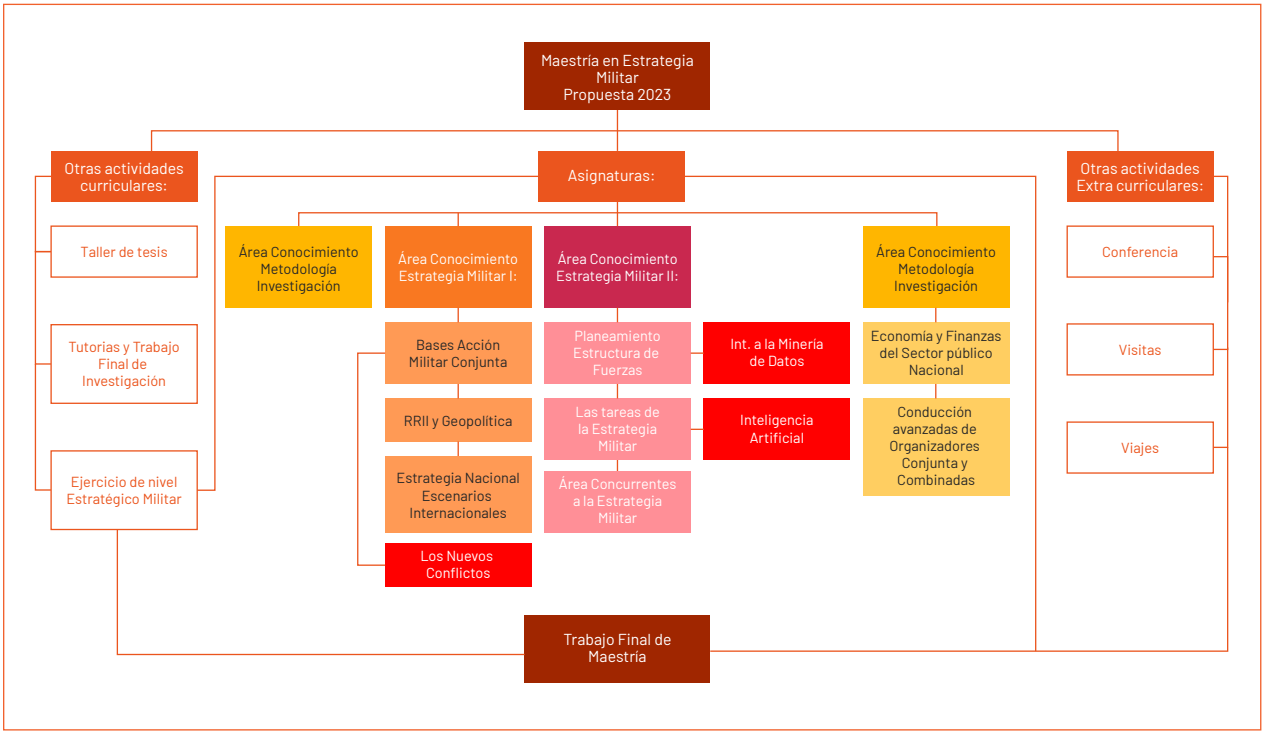
En este caso se consideraron como fuentes de información las nuevas tecnologías, en especial las inteligencias artificiales generativas de uso libre, a las cuales se les efectuó la pregunta de "¿Qué competencias se esperan de un analista estratégico militar en los próximos diez a veinte años?". En base a las respuestas generamos las denominadas "Habilidades Versión Cibernética", las cuales constituyen la visión que tienen los sistemas, basados en la información disponible en el ciberespacio. A continuación, se resume la respuesta de los programas consultados:

> **ChatGPT 3.5:** Estas competencias reflejan la necesidad de un enfoque holístico y multifacético para abordar los desafíos de seguridad y defensa en un entorno global en constante cambio. Es probable que los analistas estratégicos militares del futuro requieran habilidades avanzadas en tecnología, análisis de datos y pensamiento estratégico, así como la capacidad de liderar y colaborar eficazmente en equipos interdisciplinarios y multinacionales (ChatGPT 3.5, consultado el 18 de marzo de 2024).
> **GEMINI:** Los analistas estratégicos militares del futuro deberán ser expertos en una amplia gama de temas, desde la geopolítica hasta la tecnología, y ser capaces de adaptarse a un entorno en constante cambio (GEMINI, consultado el 18 de marzo de 2024).
> **Copilot:** En resumen, el analista estratégico militar del futuro debe ser un pensador crítico, versátil y comprometido con la seguridad y el bienestar de su país (Copilot, consultado el 18 de marzo de 2024) (Ciarla, 2017).

Las diferentes herramientas de IA por lo general coincidieron en relación a las competencias seleccionadas, y tan solo leves diferencias. Como resumen de las respuestas, se obtuvieron diez habilidades básicas a considerar:

TABLA 1. RESUMEN FINAL PARA LA EVALUACIÓN

HABILIDADES CLÁSICAS	HABILIDADES VISIÓN CIBERNÉTICA	HABILIDADES ESPERADAS
Conocimiento tecnológico extensamente cultivado	Conocimientos Tecnológicos	Conocimiento técnico y tecnológico
Gestionar la adaptación organizacional en lo militar como civil	Liderazgo y Comunicación	Habilidades de liderazgo
Capacidad de lidiar y dirigir el cambio	Pensamiento Estratégico	Análisis estratégico Gestión de riesgos
Disposición para aprender cosas nuevas sosteniendo bases éticas sólidas	Ética y Responsabilidad	Honestidad intelectual y ética profesional
Resiliencia y equilibrio mental en situaciones inusuales	Adaptabilidad y Resiliencia	Trabajo en equipo
Comprender y conceptualizar las claves de la cultura institucional	Inteligencia y Vigilancia	Conocimientos geopoliticos y relaciones internacionales
Comprender el creciente ritmo de cambio del entorno	Conocimiento en Áreas Especifica	Gestión de riesgos
Capacidad para operar interfases hombre-máquina en apoyo de las decisiones estratégicas[4]	Habilidades de Comunicación Efectiva	Comunicación efectiva
Conocer cómo garantizar mecanismos de control de calidad en el entorno de apoyo a la toma de decisiones[5]	Habilidades Analíticas y de Evaluación de Riesgos	Pensamiento estratégico
Incorporar la educación continua y la re-educación rápida, con base tecnología como esencial	Análisis de Datos y Modelado	Adaptabilidad y flexibilidad



Fuente: Ilustración SEQ Ilustración * ARABIC 1: Estructura general de la Maestría en Estrategia Militar de la ESGCFFAA

1. **Conocimientos Tecnológicos:** Comprensión profunda de las tecnologías emergentes en el ámbito militar, incluyendo inteligencia artificial, ciberseguridad, guerra cibernética, drones y tecnología espacial.
2. **Análisis de Datos y Modelado:** Habilidades avanzadas en análisis de datos y modelado para interpretar grandes volúmenes de información.
3. **Pensamiento Estratégico:** Capacidad para desarrollar estrategias y políticas efectivas para hacer frente a amenazas complejas y dinámicas.
4. **Inteligencia y Vigilancia:** Competencia en la recopilación, análisis y evaluación de información de inteligencia.
5. **Liderazgo y Comunicación:** Habilidades de liderazgo para dirigir equipos multidisciplinarios y colaborar con otras agencias gubernamentales y organizaciones internacionales.
6. **Adaptabilidad y Resiliencia:** Capacidad para adaptarse rápidamente a entornos cambiantes y a nuevas amenazas.
7. **Conocimiento en Áreas Específicas:** Conocimientos sólidos en áreas como geopolítica, seguridad internacional, conflictos armados, estrategia militar y relaciones internacionales.
8. **Habilidades Analíticas y de Evaluación de Riesgos:** Capacidad para evaluar riesgos y oportunidades, considerando factores políticos, económicos, sociales y militares.
9. **Habilidades de Comunicación Efectiva:** Capacidad para comunicar hallazgos y recomendaciones de manera clara y concisa.
10. **Ética y Responsabilidad:** Compromiso con altos estándares éticos en todas las actividades y decisiones, incluyendo la responsabilidad en la toma de decisiones y la protección de la seguridad nacional.

Habilidades Esperadas

Por último, se realizó una consulta a los alumnos de la Maestría en Estrategia Militar de las ESGCFFAA, bajo la pregunta de ***¿Cuáles serían las habilidades o competencias que desearían obtener como analistas estratégicos, para enfrentar los conflictos nuevos y futuros?*** Sobre las 46 respuestas se realizó una síntesis con la cual se espera abarcar la totalidad de los aspectos expuestos por los maestrandos, y con la cual se espera representar también las expectativas de aquellos que emprenden el desafío de este tipo de capacitación.

Los resultados obtenidos fueron:

1. **Análisis estratégico:** Evaluar variables complejas desde un enfoque interdisciplinario para tomar decisiones fundamentadas.

2. **Comunicación efectiva:** Transmitir ideas claramente en diversos contextos.
3. **Pensamiento estratégico:** Desarrollar una visión global a largo plazo y adaptarse a entornos cambiantes.
4. **Trabajo en equipo:** Colaborar efectivamente con equipos interdisciplinarios.
5. **Conocimiento técnico y tecnológico:** Dominar tecnologías relevantes y comprender su impacto.
6. **Gestión de riesgos:** Identificar, evaluar y gestionar riesgos asociados con decisiones estratégicas.
7. **Conocimientos geopolíticos y relaciones internacionales:** Comprender la geopolítica y las relaciones internacionales para evaluar amenazas y oportunidades.
8. **Habilidades de liderazgo:** Inspirar y motivar a otros hacia objetivos estratégicos.
9. **Adaptabilidad y flexibilidad:** Ajustarse rápidamente a nuevos escenarios y cambios.
10. **Honestidad intelectual y ética profesional:** Actuar con integridad y transparencia en todas las acciones y decisiones.

Resultados

Si bien las tres fuentes revelan leves discrepancias en las habilidades que ponen en valor (ver Tabla 1. Resumen final para la Evaluación), podemos encontrar una amplia coincidencia en los resultados. A continuación se enumeran:

1. **Conocimientos tecnológicos:** Cultivar un conocimiento tecnológico extenso y profundo. Mantenerse actualizado con la educación continua y la re-educación rápida. Operar interfases hombre-máquina para el apoyo a la toma de decisiones.
2. **Liderazgo y comunicación:** Poseer habilidades de liderazgo y la capacidad de dirigir el cambio. Comunicarse efectivamente en diferentes contextos.
3. **Trabajo en equipo**, Colaborar efectivamente en equipos multidisciplinarios. Comprender y trabajar en entornos interdisciplinarios. Gestionar la adaptación organizacional en diferentes contextos.
4. **Adaptabilidad y flexibilidad.**
5. **Resiliencia y equilibrio mental en situaciones inusuales.**
6. **Conocimientos en áreas específicas geopolíticos y**

CV

BM (R) ALEJANDRO MORESI

Brigadier Mayor (R) de la Fuerza Aérea Argentina. Piloto de Caza, Aviador Militar. Se desempeñó como comandante Aeroespacial del Estado Mayor Conjunto, en la Fuerza Aérea Argentina. Master en Dirección de Empresas, MBA en Dirección de Recursos Humanos Oficial de Estado Mayor. Licenciado en Sistemas Aéreos y Espaciales y posee un postgrado en Gestión de Proyectos, es Analista Operativo. Es doctorando en Defensa Nacional por la Universidad de la Defensa Nacional. Actualmente se desempeña en la Universidad de la Defensa Nacional como director de la Maestría en Estrategia Militar de la Escuela Superior de Guerra Conjunta, es docente-investigador de la Escuela Superior de Guerra Aérea y en la Maestría de Ciberdefensa y Ciberseguridad de la Universidad de Buenos Aires.

relaciones internacionales: Desarrollar expertise en áreas específicas de interés o necesidad. Profundizar en áreas relevantes para la toma de decisiones.

7. **Ética y responsabilidad:** Actuar con honestidad intelectual y ética profesional. Sostener bases éticas sólidas en la toma de decisiones.
8. **Gestión de riesgos:** Comprender el creciente ritmo de cambio del entorno y r las claves de la cultura institucional.
9. **Habilidades analíticas:** Analizar datos y modelar escenarios. Evaluar riesgos y tomar decisiones estratégicas.
10. **Pensamiento estratégico:** Conocer cómo garantizar mecanismos de control de calidad en el entorno de apoyo a la toma de decisiones y Habilidades Analíticas y de Evaluación de Riesgos.

Análisis de contenidos y posibilidad incidir en las competencias requeridas

La propuesta educativa y las habilidades que permitiría alcanzar

A continuación, se presenta un desglose de las materias y contenidos de la Maestría en Estrategia Militar de la ESGCFFAA, a partir del cual se contrastarán los contenidos y actividades, con los requerimientos resultados de los tres procesos de consulta desarrollados previamente.

La estructura de la maestría se ejecuta en cuatro áreas de conocimiento: 1. Estrategia Militar I; 2. Estrategia Militar II; 3. Conducción Superior; y 4. Metodología de la investigación. Las cuales son apoyadas con otras Actividades Curriculares (taller de tesis, las tutorías y trabajo final de investigación y el ejercicio final integrador de Nivel Estratégico Militar) y Actividades No Curriculares (como conferencias asociadas a las materias, visitar a organismos gubernamentales, militares, científicos y de interés cultural; y viajes de estudio).

Por tratarse de una maestría profesional, las diferentes asignaturas poseen abundantes actividades de tipo práctica profesional que se desarrollan en equipos o de manera individual dentro y fuera del aula donde los maestrandos juegan roles como: (1) asesores políticos, (2) miembros de Estados Mayores estratégicos de naturaleza conjunta combinada (como jefes de personal, inteligencia , operaciones, logística, como comandante de componentes entre otros), (3) como agregado militar, (4) como jefes de proyectos de investigación o de inversión y (5) como miembro de una fuerza de Paz de ONU, siempre desde una perspectiva de analista estratégico o tomador de decisiones. Para cumplir con estas exigencias y estar en condiciones de afrontar los debates diarios de los temas a tratar en cada una de las asignaturas, los estudiantes deben leer abundante documentación y procesar diferentes tareas fuera del horario de clase.

Conocimientos tecnológicos

A lo largo de la maestría se presentan tres talleres específicos del tema Métodos Cuantitativos, Minería de Datos e Inteligencia Artificial, que son complementados con unidades temáticas (UU.TT.) relativas a Ciencia y Tecnología, Armamento e industria para la defensa, El ciberespacio y el espectro electromagnético, el espacio cibernético y la gestión del conocimiento militar a través de estos contenidos y actividades prácticas el maestrando, recibe una idea general del estado del arte tecnológico en el ámbito estratégico. Un colofón de estas actividades se consolida a través de visitas a Centro de Investigación, TANDANOR, FAdeA, INVAP, Instituto Balseiro, ARSAT, entre otros. Los alumnos tienen la oportunidad de realizar de manera extracurricular un curso de vigilancia tecnológica a través del Centro de Tecnología y Prospectiva Militar Gral. Mosconi de la Facultad de Ingeniería del Ejército.

Liderazgo y comunicación

Por las características de los participantes, la mayoría de ellos ya han ejercidos cargos de conducción destacados en las fuerzas o países de los cuales provienen.

El tratamiento del liderazgo en la maestría se presenta desde la perspectiva estratégica a través de la materia "Conducción Avanzada de Organizaciones Conjuntas y Combinadas" donde UU.TT. como "Estrategia de Organizaciones Complejas" se trata en detalle las relaciones cívico-militares las complejidades de organizaciones donde se gestiona el poder tanto político como militar, y "El Liderazgo Militar Indirecto" donde se tratan aspectos como la cultura de la organización militar, la gestión del personal militar, la modalidad de asesoramiento para la conducción superior y la gestión del conocimiento militar. Esta área se complementa con visitas a comandos como el de ciberdefensa, aeroespacial, marítimo, operacional y se vuelven a revisar en los viajes a las grandes unidades de combate y escuelas del Ejército, la Armada y la Fuerza Aérea.

Los aspectos relativos a la comunicación son parte de la asignatura "Áreas concurrentes con la estrategia militar", es tratada en UU.TT. como "Gestión de los medios de comunicación y la comunicación en las crisis" y "Las entrevistas: el vocero del comandante", donde diferentes situaciones son practicadas son presentadas, las que se complementan con conferencias de relevantes periodistas de medios gráficos, televisivos, radio e internet.

Trabajo en equipo

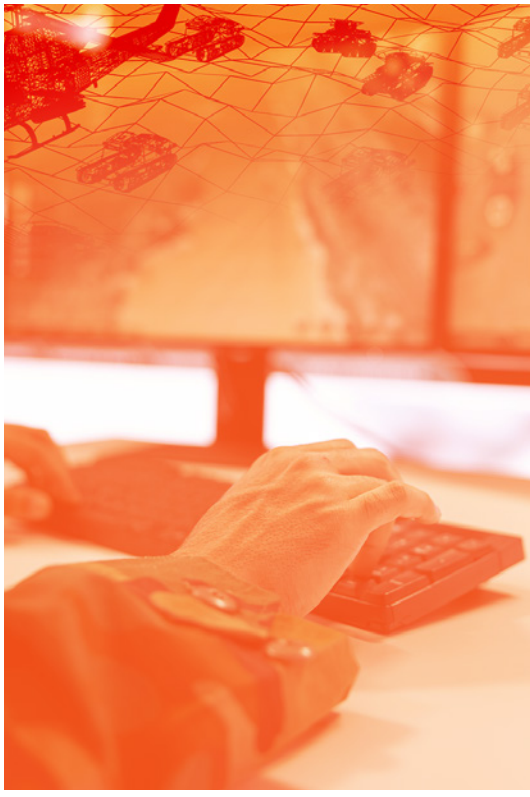
En la totalidad de las materias y actividades el trabajo en equipo resulta parte esencial de las tareas y prácticas a desarrollar, siendo su momento cúlmine el Ejercicio de Nivel Estratégico Militar, donde la única posibilidad de alcanzar los objetivos de los diferentes planteos que se realizan es a través de trabajo coordinados multidisciplinarios de investigación y resolución. La materia "Bases para la Acción Militar Conjunta" plantea la necesidad de resolver e interactuar en equipos a través de UU.TT. como "El Conflicto, La Política, la estrategia para la defensa" y "Comparación con otras políticas y estrategias nacionales", plantean trabajos donde la interacción del equipo es el modo de poder alcanzar resoluciones adecuadas a las problemáticas planteadas.

Adaptabilidad y flexibilidad

El tratamiento de la problemática estratégica en la asignatura Bases Para la Acción Militar Conjunta", donde el "taller de los nuevos conflictos" y los problemas y prácticas a resolver en UT como la "El conflicto la política , la estrategia para la defensa", así como los problemas que surgen en la ejercitación de materias como "Economía y Finanzas del Sector Público Nacional" que en sus ejercitaciones integradoras obliga a los equipos de maestrandos a resolver situaciones propias del día a día profesional en el ámbito presupuestarios y la gestión de proyectos de con Inversión obligan a los estudiantes a romper los esquemas mentales del propios del nivel operacional y la formación militar basada en la épica, para trasladarse al ámbito del pensamiento estratégico, donde el planteo épico se convierte en un frio análisis de fines y medios en función de alcanzar los objetivos que ha fijado la política.

Resiliencia y equilibrio mental en situaciones inusuales

Los estudiantes de la maestría son sometidos a un esfuerzo inicial de trabajo académico que en general los supera debido a la falta de entrenamiento la materia, este aspecto busca por un lado llevarlo rápidamente a un estado de óptima aptitud para la cursada y por otro poner a prueba la resistencia natural a incorporarse a una nueva disciplina como les la estrategia.



Para ello la materia "Bases para la acción Militar Conjunta" combina ejercitaciones prácticas, debates en línea y talleres donde las situaciones que se presentan y los problemas a resolver en general rompen los paradigmas del trabajo tradicional de Estado Mayor, aspectos que se ven complementados con el seminario de "Negociación y solución de conflictos internacionales" de la asignatura "Relaciones Internacionales y Geopolítica" donde ven un espectro completo de situaciones complejas y las soluciones alcanzadas en diferentes situaciones.

Conocimientos en áreas específicas geopolíticos y relaciones internacionales

Esto conocimiento se aporta desde las asignaturas "Relaciones Internacionales y Geopolítica" y "Estrategia Nacional y Escenarios Internacionales" a través de ellas se

obtiene un compendio actualizado que va desde las corrientes de pensamiento en relaciones internacionales, al tratamiento aspectos de la geopolítica actual que van de la problemática energética a las cuestiones comerciales y el tratamiento de los hoy llamados espacios comunes, para llegar al estado argentino y la política, las agendas internacionales y los aspectos de paz y seguridad en la región sudamericana, introduciendo los primeros conceptos asociados a la planificación estratégica y las políticas de defensa de un estado. Conferencistas de diferentes tendencias aportan aspectos de interés a la temática de la situación y las relaciones internacionales.

Ética y responsabilidad

Estos son aspectos intrínsecos a la profesión militar en nuestro país y también en las fuerzas armadas de países amigos que acompañan esta carrera, no obstante ambos son puesto de relieve de manera constante en las diferentes actividades prácticas y académicas, siendo objeto de debate en UUTT de diferentes asignaturas como: “Los nuevos conceptos de la guerra”, “La planificación estratégica y las políticas de defensa de un estado”, “Conducción política de la defensa”, “La dirección estratégica militar”, “Personal para la acción militar conjunta”, “Inteligencia estratégica”, “Las reglas de empeñamiento y el uso de la fuerza”, “Derecho internacional humanitario en los conflictos armados y las nuevas guerras”, “La protección de los bienes culturales y el medio ambiente”, “Estrategia de organizaciones complejas”, “El liderazgo militar indirecto” y “La gestión del conocimiento militar”.

Gestión del Riesgo

Aquí se busca la comprensión del creciente ritmo de cambio del entorno y las claves de la cultura institucional, para ello el conocimiento que aportan aspectos de la maestría como el tratamiento de Los nuevos conceptos de la guerra, negociación, el análisis de la naturaleza del conflicto futuro, el planeamiento de estructura de fuerzas, el uso de métodos cuantitativos relacionados con el planeamiento y la minería de datos, comprender las contingencias de empleo y los aspectos propios de la Inteligencia y la anticipación estratégica, la estrategia organizacional y el liderazgo militar indirecto, permiten al maestrando obtener una concepción integral de la dimensión del riesgo y lo que ella conlleva.

Habilidades analíticas

Resultan como una consecuencia, de todas y cada una de las actividades que se realizan en la maestría, ya que los participantes se ven permanentemente obligados a evaluar los conocimientos que reciben, el nivel y calidad de las conferenciantes en que

participan, los esfuerzos que demandan las ejercitaciones y las experiencias que resultan de las visitas y viajes que realizan. Todo ello constituye un acervo que le permite al maestrando ejercer de manera constante una visión crítica y analítica que es su conceptualización le permitirán entrar en la dimensión del analista estratégico militar.

Conclusión

El único aspecto difícil de explicar cómo objetivamente se puede alcanzar el pensamiento estratégico a través de una cursada de capacitación profesional, ya que si bien las totalidad de las habilidades explicadas hasta aquí son cruciales para permitirlo, el pensamiento estratégico implica navegar en la incertidumbre del futuro. El pensamiento estratégico es el que conforma al estratega, de acuerdo al GD Motta, este es el que:

"Puede elaborar una estrategia, formar conductores participantes de ese pensamiento estratégico, conducirla e implementarla. En síntesis, significa lograr los fines que éste se impuso con los medios que posee y con los menores costos; aprovechando al máximo sus fortalezas y minimizando sus debilidades en un tiempo y espacio determinado, creando y conduciendo el conflicto, según su racionalidad y la del oponente y fijando un destino (visión) común a través de la motivación. El estratega se forma a lo largo de toda su carrera".

De allí que la estrategia no sea sólo conocimiento científico, es también intuición y arte para poder conducirse de manera asertiva en un futuro incierto en el que se exige del estratega un liderazgo firme y seguro que lleve a superar las incertidumbres y vallas que impone el camino hacia el cumplimiento de los objetivos impuestos.

Ha llegado el momento de contestar la pregunta: ¿La propuesta de la Maestría en Estrategia Militar de la ESGCFFAA provee las adecuadas herramientas para el futuro analistas y asesores en materia de estrategia militar?, y la respuesta es que el proceso académico al que se lo somete al individuo resulta en una caja de herramientas completa y adecuada para lo que se espera de un futuro analista estratégico, pero no asegura el Pensamiento Estratégico en su esencia más profunda (el estratega), para ello debe acompañarse de experiencias vivencias y ciertas cualidades personales, que le permitirán desarrollar el Pensamiento Estratégico en su concepción integral.

Aquellos que lo logren serán los que pueden ser llamados estrategas, los que no, serán expertos conocedores y analistas de estrategia y eso les permitirá trabajar y asesorar en los equipos que asisten a los tomadores de decisiones con conocimientos firmes y objetivos a partir del desarrollo de todas las disciplinas presentadas a lo largo de la maestría en Estrategia Militar de la Escuela Superior de Guerra Conjunta.

BIBLIOGRAFÍA

Ciarla, G. A. (2017). El método de análisis de inteligencia en el modelo de planeamiento militar para la defensa argentino. Facultad de Ciencias Jurídicas y Sociales de la Universidad de La Plata.

Craig, G. A. y Gilbert, F. (1986). *"Reflections on Strategy in the Present and Future", en Makers of Modern Strategy:* from Machiavelli to the Nuclear Age (p. 869). Princeton University Press.

De Vergara, E. (2017). Estrategia: el camino. Universidad de la Defensa, Argentina.

Finney, N. K. (2020). *On Strategy: a Primer.* U. S. Army Combined Arms Center.

Freedman, L. (2013). *Strategy: A History.* Oxford University Press.

Freedman, L. (2017). *The Future of War:* A History. Public Affairs.

Gat, A. (2008). *War in Human Civilization.* Oxford University Press.

Guderian H. (1954). *Panzer Leader.* Citado del prólogo de Lidell Hart. (Aporte de GD Gustavo Motta).

Hoffman F. (2019) *"Healthy Scepticism about the Future of Disruptive Technology and Modern War".* Foreign Policy Research Institute blog.

Mc Fate S. (2019). Las nuevas reglas de la guerra: Victoria en la era del desorden permanente. Biblioteca del Oficial, Buenos Aires.

Millett, A. R., & Murray, W. (2010). *Military Effectiveness: Volume 1, The First World War.* Cambridge University Press, Nueva York.

Ricks, T. E. (2013). *The Generals: American Military Command from World War II to Today.* Penguin Publishing Group. (Aporte de GD Gustavo Motta).

Ryan M. (2019) *"An Australian Intellectual Edge for Conflict and Competition in the 21st Century".* Centro de Estudios Estratégicos y de Defensa, Universidad Nacional de Australia.

De Vergara E. (2012). Estrategia, Método y Rutinas. Editorial Universitaria del Ejército, Buenos Aires.

Wiliamson M. y Millet A. R. (2002). La Guerra que había que ganar. Grupo Planeta.

ESCUDO CUÁNTICO

LA VENTANA CRÍTICA PARA LA SOBERANÍA DIGITAL ANTE LA AMENAZA CRIPTOGRÁFICA EMERGENTE

Por **ADRIANA BARAVALLE**

Palabras Clave:
> Criptografía post-cuántica
> Inteligencia artificial
> Computación cuántica
> Infraestructuras críticas
> Ciberseguridad

Abstract
La convergencia de computación cuántica, inteligencia artificial y criptografía post-cuántica configura un nuevo paradigma geopolítico donde la supremacía tecnológica define ventajas estratégicas decisivas. Este artículo presenta un análisis exhaustivo del estado del arte global, identificando brechas críticas en capacidades nacionales y proponiendo un pensar en un marco de trabajo estratégico para el desarrollo de arquitecturas híbridas de ciberdefensa. La investigación revela que escasas publicaciones abordan la intersección de estos tres dominios críticos, mientras potencias tecnológicas consolidan ventajas asimétricas que comprometen la soberanía digital nacional.

Introducción

La revolución cuántica contemporánea representa una discontinuidad tecnológica de magnitud equivalente al desarrollo de la computación electrónica o la energía nuclear, con implicaciones geopolíticas que trascienden el ámbito puramente científico. La convergencia de tres dominios tecnológicos críticos —computación cuántica, inteligencia artificial y criptografía post-cuántica— configura un nuevo paradigma estratégico donde la supremacía tecnológica define ventajas asimétricas decisivas en el escenario internacional.[1]

La computación cuántica ha alcanzado un punto crítico donde las capacidades criptográficamente relevantes están proyectadas para 2028-2030. IBM Starling promete 100 millones de qubits para 2029, mientras Google Willow ha demostrado corrección de errores escalable. Estas capacidades permitirán descifrar RSA-2048 con aproximadamente 1 millón de

qubits físicos, comprometiendo el 95% de las comunicaciones militares actuales.

China[2] y Rusia lideran programas cuánticos estatales con objetivos militares específicos. Se suman países con capacidad financiera para adquirir esta tecnología desarrollada por los países líderes, programas civiles cuánticos civiles de aplicación dual, grupos de cibercrimen organizado y organizaciones que operan con apoyo de Estados.

Estados Unidos tiene un enfoque híbrido público-privado, con $1.2 mil millones de inversión federal.

La asimetría actual invita a pensar en marcos de cooperación regional en materia de innovación e investigación. Las fuerzas armadas argentinas ya enfrentan amenazas de phishing dirigido, ransomware, y espionaje cibernético. Las capacidades cuánticas futuras representan una escalación de estas amenazas existentes, donde los datos comprometidos hoy podrán ser descifrados retroactivamente, los sistemas de comando y control (C4ISR) actuales necesitan protección prospectiva y las vulnerabilidades de transición crean ventanas de oportunidad para adversarios.

Este artículo pretende iluminar sobre la necesidad apremiante de evaluar el estado actual del conocimiento global en estos campos convergentes, identificar las brechas críticas que comprometen la capacidad nacional de respuesta ante amenazas cuánticas emergentes, y proponer un marco de trabajo estratégico integral para la investigación y el desarrollo de arquitecturas defensivas híbridas. De este modo, la ventana de acción 2025-2027 es crítica para la implementación de criptografía post-cuántica en sistemas críticos, 2027-2029 para el desarrollo de capacidades cuánticas defensivas, y 2029-2032 para la operacionalización de sistemas híbridos cuántico-clásicos.

GRÁFICO 1. QPUS POR PAÍS Y MODALIDAD

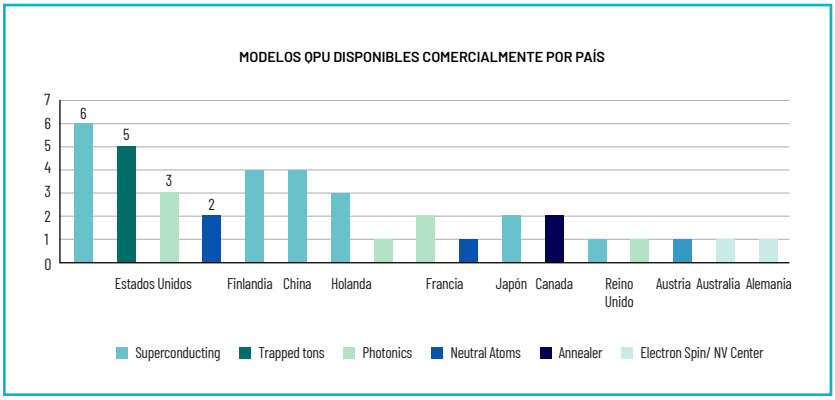
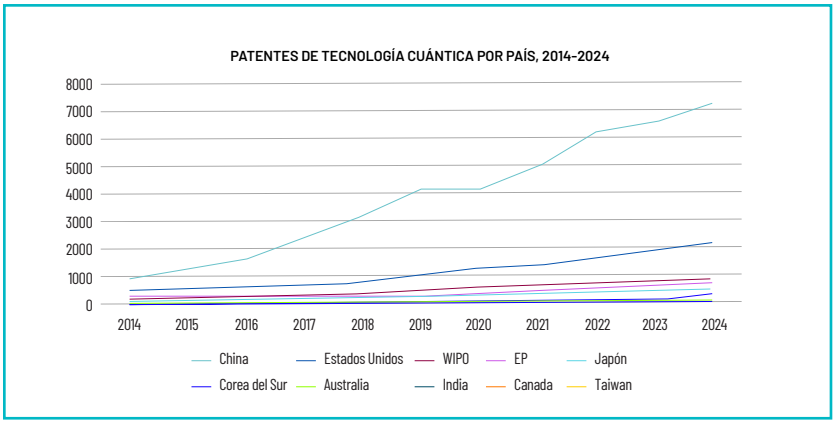


GRÁFICO 2. PATENTES POR PAÍS



Fuente: "The Quantum Index Report 2025"

Ecosistema global de computación cuántica

El ecosistema internacional de *Quantum Processing Units* revela una concentración geográfica crítica de capacidades avanzadas que configura un mapa geopolítico altamente asimétrico. Estados Unidos mantiene el liderazgo tecnológico mediante una combinación estratégica de iniciativas corporativas y gubernamentales, con IBM Quantum qque ha alcanzado los 100 qubits superconductores y Google Quantum AI superando los 200 qubits en sus sistemas más avanzados. Paralelamente, China ha desarrollado una ruta tecnológica alternativa centrada en sistemas fotónicos de escala masiva con Jiuzhang-2.0, que ha demostrado supremacía cuántica fotónica en problemas específicos de muestreo gaussiano.[3]

La aceleración exponencial de los desarrollos cuánticos, particularmente los avances de Google Willow[4] en corrección de errores cuánticos y el anuncio de IBM Starling[5] para 2029, comprimen dramáticamente las proyecciones temporales sobre la

1. https://revistafal.com/la-guerra-cuantica-el-nuevo-frente-de-batalla-geopolitico/
2. Especialización en sistemas fotónicos con Jiuzhang-2.0. Programa estatal centralizado con objetivos militares explícitos y red de comunicación cuántica nacional operativa.
3. https://qir.mit.edu/wp-content/uploads/2025/06/MIT-QIR-2025.pdf
3. https://qir.mit.edu/wp-content/uploads/2025/06/MIT-QIR-2025.pdf
4. https://blog.google/technology/research/google-willow-quantum-chip/
5. https://www.ibm.com/quantum/blog/large-scale-ftq

Fuente: *npj Quantum Inf*

CV

ADRIANA BARAVALLE

Magister en Explotación de Datos y Gestión del Conocimiento y Doctoranda en Ingeniería por la Universidad Austral. Profesora adjunta en Inteligencia Artificial aplicada a Estrategia Militar y Ciberseguridad. Investigadora principal en proyectos de IA aplicada a la defensa, Universidad de la Defensa Nacional. Directora académica synapsIA, Universidad Austral. Autora de múltiples publicaciones en ACM y Springer sobre IA y frameworks de gobernanza para IA en sistemas críticos. Especialista en intersección de tecnologías cuánticas, criptografía e inteligencia artificial para aplicaciones de seguridad nacional.

disponibilidad de computadoras cuánticas criptográficamente relevantes. Esta realidad tecnológica emergente exige una estrategia coordinada que trascienda los enfoques reactivos tradicionales hacia sistemas verdaderamente adaptativos y resilientes.

Esta convergencia tecnológica es particularmente significativa considerando que el algoritmo de Shor puede factorizar números enteros grandes en tiempo polinómico $O((\log N)^3)$, requiriendo aproximadamente 1 millón de qubits físicos para comprometer efectivamente claves RSA de 2048 bits según las estimaciones más recientes de Gidney y colaboradores del equipo de Google AI Quantum[6].

La distribución geográfica de estas capacidades revela patrones estratégicos claramente definidos. Estados Unidos concentra su fortaleza en empresas como IBM, Google, Rigetti e IonQ, y mantiene el liderazgo tanto en arquitecturas de qubits superconductores como en sistemas de iones atrapados. China, por su parte, ha desarrollado expertise específico a través de la Universidad Jiao Tong de Shanghai, focalizándose en sistemas fotónicos que ofrecen ventajas inherentes para aplicaciones de comunicación cuántica[7].

Europa muestra una estrategia de diversificación tecnológica mediante iniciativas como IQM en Finlandia y Oxford Quantum Computing en Reino Unido, mientras que Israel ha consolidado un ecosistema especializado altamente eficiente, con empresas como Quantum Machines y Classiq, que han recibido inversiones superiores a 100 millones de shekels durante 2023 para el establecimiento del Israel Quantum Computing Center.

Panorama de criptografía post-cuántica

El *National Institute of Standards and Technology*[8] ha culminado un proceso de estandarización crítico mediante la selección de cuatro algoritmos fundamentales que definen el nuevo paradigma criptográfico post-cuántico. CRYSTALS-Kyber establece el estándar para encapsulación de claves basada en problemas de retículos, mientras que CRYSTALS-Dilithium y FALCON proporcionan esquemas de firmas digitales cuántico-resistentes con diferentes perfiles de rendimiento y seguridad. SPHINCS+ complementa esta suite como sistema de firmas basado en funciones hash, y ofrece garantías de seguridad conservadoras fundamentadas en primitivas criptográficas bien establecidas.

Sin embargo, la evolución del panorama de amenazas revela la naturaleza dinámica de este campo tecnológico. El ataque de Castryck-Decru[9] contra SIKE en 2022 demostró cómo nuevos desarrollos matemáticos pueden comprometer sistemas considerados seguros e invalidar completamente a un candidato que había superado múltiples rondas de evaluación del proceso NIST. Más preocupante aún, la vulneración de CRYSTALS-Kyber[10] mediante técnicas de inteligencia artificial documentada por Sim,

Park y Han (2022) evidencia la emergencia de amenazas híbridas que combinan vectores cuánticos, clásicos y de aprendizaje automático de maneras anteriormente imprevistas.

Estos desarrollos ilustran la complejidad fundamental de desarrollar sistemas verdaderamente resistentes a amenazas multidimensionales que evolucionan a velocidades exponenciales. La investigación actual sugiere que la seguridad post-cuántica no puede concebirse como un problema estático de selección algorítmica, sino como un desafío dinámico que requiere arquitecturas adaptativas para sistemas militares (centros de operaciones, plataformas navales e infraestructura crítica) capaces de evolucionar proactivamente ante amenazas emergentes.

GRÁFICO 3. BANCO DE PRUEBAS DE REDES CUÁNTICAS EN ESTADOS UNIDOS

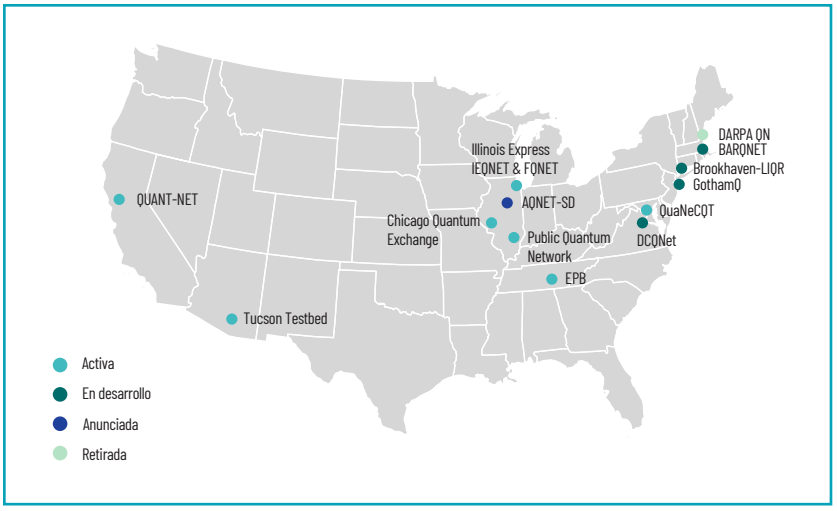
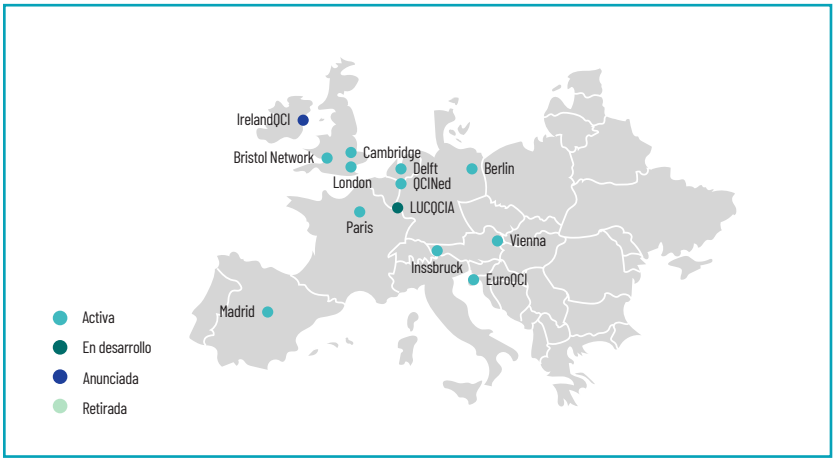


GRÁFICO 4. BANCO DE PRUEBAS DE REDES CUÁNTICAS EN EUROPA



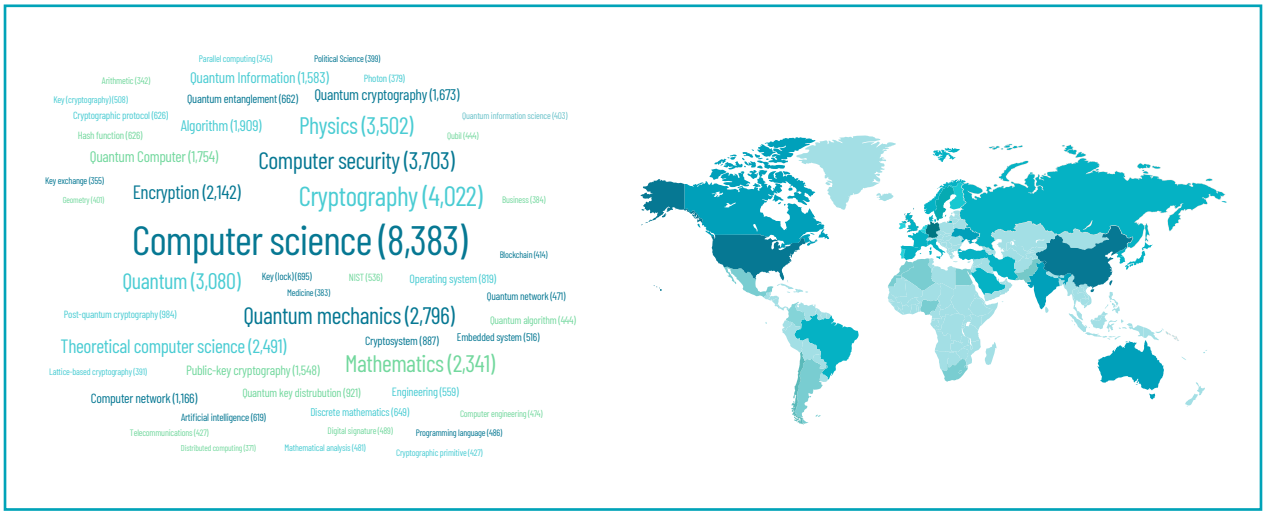
Fuente: "The Quantum Index Report 2025"

Convergencia con inteligencia artificial

La integración sinérgica de inteligencia artificial con computación cuántica representa uno de los desarrollos más significativos en el panorama tecnológico contemporáneo. La incorporación de Deep Neural Networks desarrolladas por Nvidia[11] para algoritmos de decodificación cuántica ha demostrado mejoras sustanciales en corrección de errores, y prácticamente ha validado el *threshold theorem*[12], que durante décadas permaneció como una construcción puramente teórica. Esta convergencia no solo acelera el desarrollo de sistemas cuánticos prácticos, sino que establece las bases para arquitecturas híbridas que aprovechan las fortalezas complementarias de ambos paradigmas computacionales.

Paralelamente, las técnicas de *quantum machine learning*[13] emergen como multiplicadores de fuerza para aplicaciones críticas de detección de amenazas y optimización criptográfica para el descifrado de comunicaciones en tiempo real, navegación, guiado y redes de comunicación resistentes a la interferencia cuántica. Los algoritmos cuánticos variacionales demuestran ventajas prometedoras en problemas de clasificación y reconocimiento de patrones, particularmente en contextos donde la dimensionalidad y complejidad de los datos exceden las capacidades efectivas de métodos clásicos. La investigación reciente sugiere que estos enfoques híbridos pueden proporcionar capacidades defensivas superiores, especialmente en la identificación de anomalías sutiles y la predicción de vectores de ataque emergentes. Este campo emergente presenta una oportunidad estratégica de gran magnitud.

6. https://arxiv.org/abs/2505.15917
7. Chen, HZ., Li, MH., Wang, Y.Z. *et al.* Implementation of carrier-grade quantum communication networks over 10000 km. *npj Quantum Inf* 11, 137 (2025). https://doi.org/10.1038/s41534-025-01089-8. https://www.nature.com/articles/s41534-025-01089-8
8. https://qir.mit.edu/wp-content/uploads/2025/06/MIT-QIR-2025.pdf
9. https://cacm.acm.org/news/nist-post-quantum-cryptography-candidate-cracked/
10. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9786796
11. https://www.nvidia.com/es-la/training/
12. https://quantum.cloud.ibm.com/learning/en/courses/foundations-of-quantum-error-correction/fault-tolerant-quantum-computing/threshold-theorem
13. https://arxiv.org/abs/2502.01146



Las publicaciones especializadas en criptografía post-cuántica hoy alcanzan un número aproximado de 11.317, mientras que son 37 los trabajos enfocados en inteligencia artificial cuántica, lo cual representa un corpus sustancial de conocimiento especializado.

Respecto de patentes la base de conocimiento, Lens.org cuenta con 12.217 relacionadas con criptografía post-cuántica y 1 relacionada con inteligencia artificial cuántica.

Sin embargo, la intersección específica de estos dominios con arquitecturas de ciberdefensa práctica está representada por escasos trabajos de investigación (4 publicaciones y ninguna patente). Esto evidencia un campo emergente con inmensas oportunidades estratégicas para contribuciones pioneras y desarrollo de ventajas competitivas sostenibles[14].

Casos de estudio internacionales

Un caso de estudio internacional exitoso que podría tomarse como referencia de modelo para marcos de trabajo conceptuales para el desarrollo de capacidades cuánticas, es el paradigma israelí, materializado en el *Israel Quantum Computing Center*[15][16], que representa un caso ejemplar de coordinación estratégica efectiva donde se integran sinérgicamente academia, industria y sector defensa. La inversión coordinada superior a 100 millones de shekels (aproximadamente 30 millones de dólares) ha generado un ecosistema altamente eficiente donde instituciones académicas de prestigio como el Technion colaboran estrechamente con empresas especializadas como Classiq y Quantum Machines, de modo que crean ciclos virtuosos de desarrollo tecnológico y transferencia de conocimiento.

La iniciativa europea materializada en el programa Quantum Flagship[17] constituye un modelo complementario de coordinación supranacional que demuestra cómo la agregación estratégica de recursos y expertise puede acelerar el desarrollo de capacidades críticas. El presupuesto de €1,000 millones distribuido a lo largo del período 2018-2028 ha permitido el pooling efectivo de recursos de investigación, la coordinación de estándares técnicos, y el desarrollo de masa crítica en áreas especializadas donde ningún país individual podría alcanzar competitividad global de manera independiente.

Los modelos estadounidense y chino completan el panorama de estrategias nacionales diferenciadas. Estados Unidos ha desarrollado un enfoque híbrido que combina liderazgo corporativo privado con inversión gubernamental estratégica, donde empresas como IBM y Google mantienen autonomía operacional mientras reciben apoyo federal para investigación básica y aplicaciones de seguridad nacional. El programa *National Quantum Initiative Act* de 2018 estableció un marco de coordinación que preserva la competencia comercial mientras asegura el desarrollo de capacidades críticas para defensa nacional.

China, por el contrario, ha implementado un modelo de planificación centralizada que integra objetivos tecnológicos con prioridades geopolíticas explícitas. La concentración de recursos en la Universidad Jiao Tong de Shanghai y el desarrollo acelerado de infraestructura de comunicación cuántica de escala nacional demuestran las ventajas de coordinación estatal directa, aunque con costos potenciales en términos de diversificación

14. Análisis bibliométrico realizado con datos de la plataforma Lens.org de Microsoft https://www.lens.org/
15. https://i-qcc.com/
16. https://www.enlacejudio.com/2022/07/19/israel-establecera-centro-de-computacion-cuantica/
17. https://qt.eu/

tecnológica y capacidad de innovación disruptiva.

Capacidades nacionales

Argentina posee una base de investigación cuántica emergente significativa. El CONICET desarrolla investigación en computación cuántica a través del Instituto de Física La Plata (IFLP). Paralelamente, la CNEA ha establecido proyectos específicos en el Centro Atómico Bariloche para desarrollar procesadores cuánticos con circuitos superconductores, mientras que la División Óptica Cuántica del DEILAP opera desde 2008 como laboratorio pionero en fenómenos ópticos cuánticos, trabajando con pares de fotones entrelazados y sistemas de Distribución Cuántica de Claves.

Las universidades nacionales complementan este ecosistema con iniciativas formativas y de investigación aplicada. La Universidad Nacional de La Plata forma parte activa de los esfuerzos universitarios coordinados con institutos del CONICET, mientras que la Universidad Nacional de Quilmes ha establecido programas específicos de desarrollo en computación cuántica. La Universidad de Buenos Aires ofrece cursos especializados de introducción a la computación cuántica, y Buenos Aires fue sede en julio de 2024 de la 21° Conferencia Internacional *"Quantum Physics and Logic"*, que reunió a más de 100 investigadores internacionales. Estas iniciativas, aunque limitadas en escala comparada con potencias cuánticas, demuestran capacidades existentes que podrían constituir la base para desarrollos más ambiciosos.

Conclusiones

Las capacidades existentes y los casos internacionales descriptos antes ilustran principios fundamentales aplicables al

GRÁFICO 5. EVOLUCIÓN DE TRABAJOS ACADÉMICOS

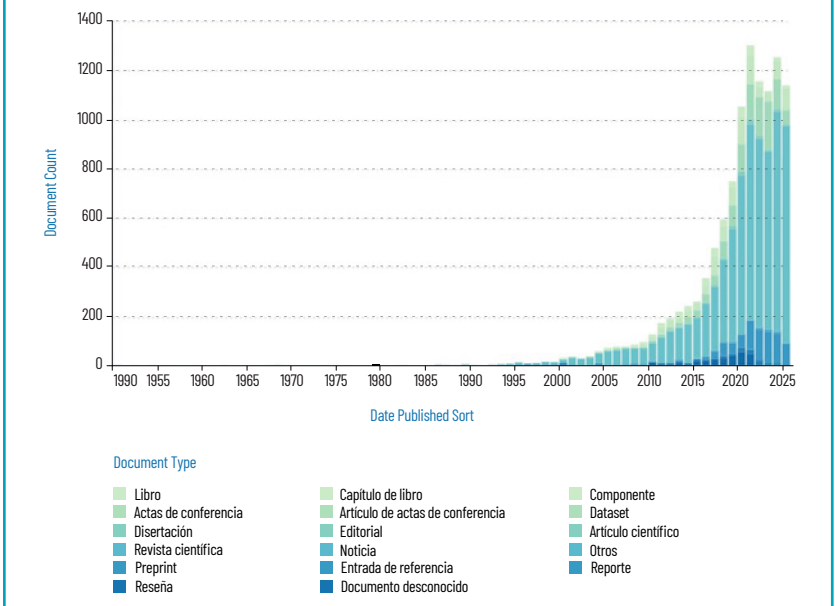
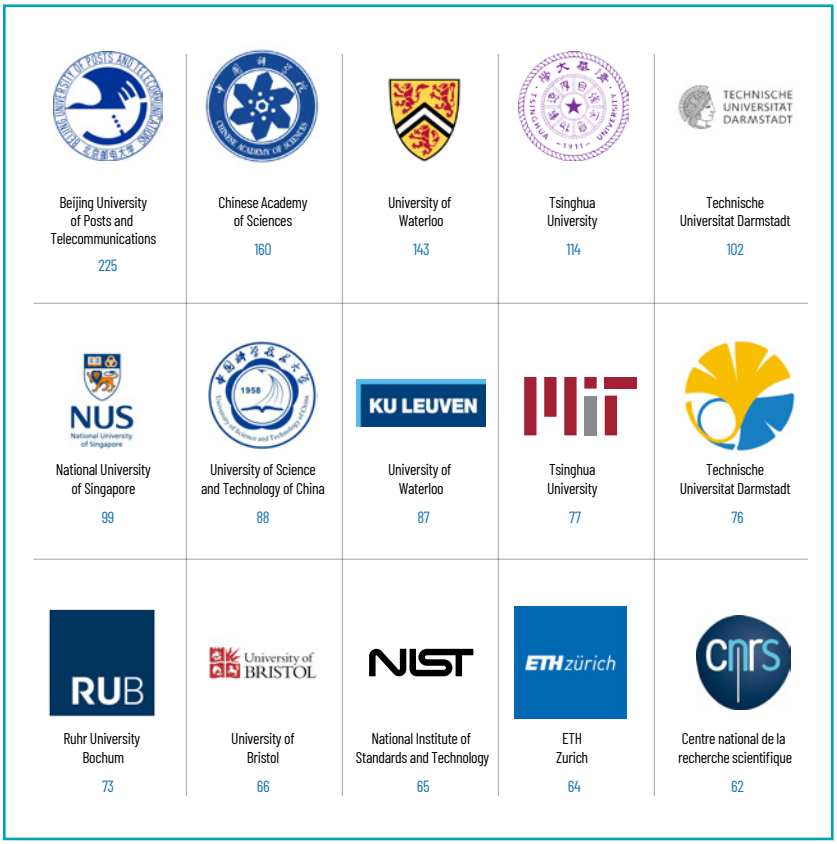


GRÁFICO 5. LOGOS DE LAS PRINCIPALES INSTITUCIONES



Fuente: Lens.org – query= "post-quantum cryptography"

contexto nacional. La coordinación efectiva entre sectores, la concentración estratégica de recursos en áreas de ventaja comparativa, y el desarrollo de marcos institucionales que faciliten la colaboración a largo plazo emergen como factores críticos de éxito. Es particularmente relevante la capacidad demostrada por estos modelos para mantener coherencia estratégica durante períodos gubernamentales múltiples, y asegurar continuidad en inversiones que requieren horizontes temporales extendidos para generar retornos tangibles.

La capacidad de respuesta efectiva ante amenazas cuánticas emergentes puede potenciarse sustancialmente mediante el fomento sistemático de investigación básica en la intersección crítica de inteligencia artificial y criptografía post-cuántica, creando nichos de expertise que complementen las capacidades globales existentes en lugar de replicar enfoques ya consolidados por las potencias dominantes.

Contar con un centro de excelencia en computación cuántica contribuiría a la transferencia de conocimiento entre universidades y el sector defensa en tecnologías emergentes que potencian el desarrollo de capacidades avanzadas.

Retener expertise crítico y acrecentar el número de especialistas en criptografía post-cuántica, a partir de la sinergia entre academia y gobierno sería factible con el diseño de programas de formación especializados, particularmente en la preparación de operadores de ciberdefensa capaces de gestionar sistemas híbridos complejos.

La incorporación sistemática del sector privado emerge como factor multiplicador crítico observado en todos los modelos exitosos. La generación de espacios de colaboración estructurada con la industria, especialmente con el ecosistema de empresas emergentes especializadas, puede aprovechar la dinámica y capacidad de inversión privada para acelerar procesos de desarrollo que tradicionalmente dependen exclusivamente de recursos públicos. Esta sinergia resulta particularmente relevante en el contexto de tecnologías cuánticas, donde los ciclos de innovación requieren tanto la estabilidad de financiamiento a largo plazo como la agilidad de respuesta ante oportunidades técnicas emergentes.

La transformación de capacidades técnicas en ventajas estratégicas requiere la convergencia de múltiples factores que median entre el desarrollo

La capacidad de respuesta efectiva ante amenazas cuánticas emergentes puede potenciarse sustancialmente mediante el fomento sistemático de investigación básica en la intersección crítica de inteligencia artificial y criptografía post-cuántica

científico y su aplicación geopolítica efectiva. Los factores económicos incluyen no solo la disponibilidad de recursos financieros, sino la capacidad de sustentar inversiones a largo plazo, desarrollar cadenas de suministro especializadas, y crear mercados domésticos que justifiquen la escala de producción. Los elementos institucionales abarcan marcos regulatorios apropiados, coordinación inter agencial efectiva, y la capacidad del sistema político para mantener coherencia estratégica durante múltiples ciclos gubernamentales. Los aspectos sociales involucran la formación de masa crítica de recursos humanos especializados, la creación de cultura organizacional que favorezca la innovación, y el desarrollo de redes de confianza entre academia, industria y gobierno que faciliten la transferencia efectiva de conocimiento y la colaboración a largo plazo.

La convergencia de la computación cuántica, inteligencia artificial y criptografía post-cuántica constituye una transformación tecnológica de alcances geopolíticos profundos y que redefine las bases sobre las cuales se construyen las ventajas competitivas entre naciones en el siglo XXI. La intersección de estos dominios críticos presenta una ventana única para el desarrollo de capacidades estratégicas diferenciadas, donde la supremacía no se define únicamente por el volumen de inversión, sino por la capacidad de integrar sinérgicamente estos campos emergentes en arquitecturas defensivas coherentes y adaptativas. De modo tal que permite la detección de amenazas en tiempo real mediante quantum machine learning, la optimización criptográfica adaptativa según amenazas emergentes y desarrollar sistemas de comunicación cuántica inmunes a intercepción clásica. Sin contar con capacidades propias, se acrecienta la asimetría informacional ante adversarios, los sistemas actuales entran en obsolescencia acelerada y se acrecienta la dependencia tecnológica de proveedores extranjeros.

BIBLIOGRAFÍA

Castryck, W. & Decru, T. (2022). An efficient key recovery attack on SIDH. *Advances in Cryptology - EUROCRYPT 2023*.

-

Chen, HZ., Li, MH., Wang, Y.Z. et al. Implementation of carrier-grade quantum communication networks over 10000 km. npj *Quantum* Inf 11, 137 (2025). https://doi.org/10.1038/s41534-025-01089-8. https://www.nature.com/articles/s41534-025-01089-8

-

Gidney, C. & Ekera, M. (2024). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Arxiv Quantum Physics*. Cornell University.

Google Quantum AI and Collaborators. Quantum error correction below the surface code threshold. *Nature 638*, 920–926 (2025). https://doi.org/10.1038/s41586-024-08449-y

-

IBM Research. (2024). Large-scale fault-tolerant quantum computing. *IBM Quantum Blog*. https://www.ibm.com/quantum/blog/large-scale-ftqc

-

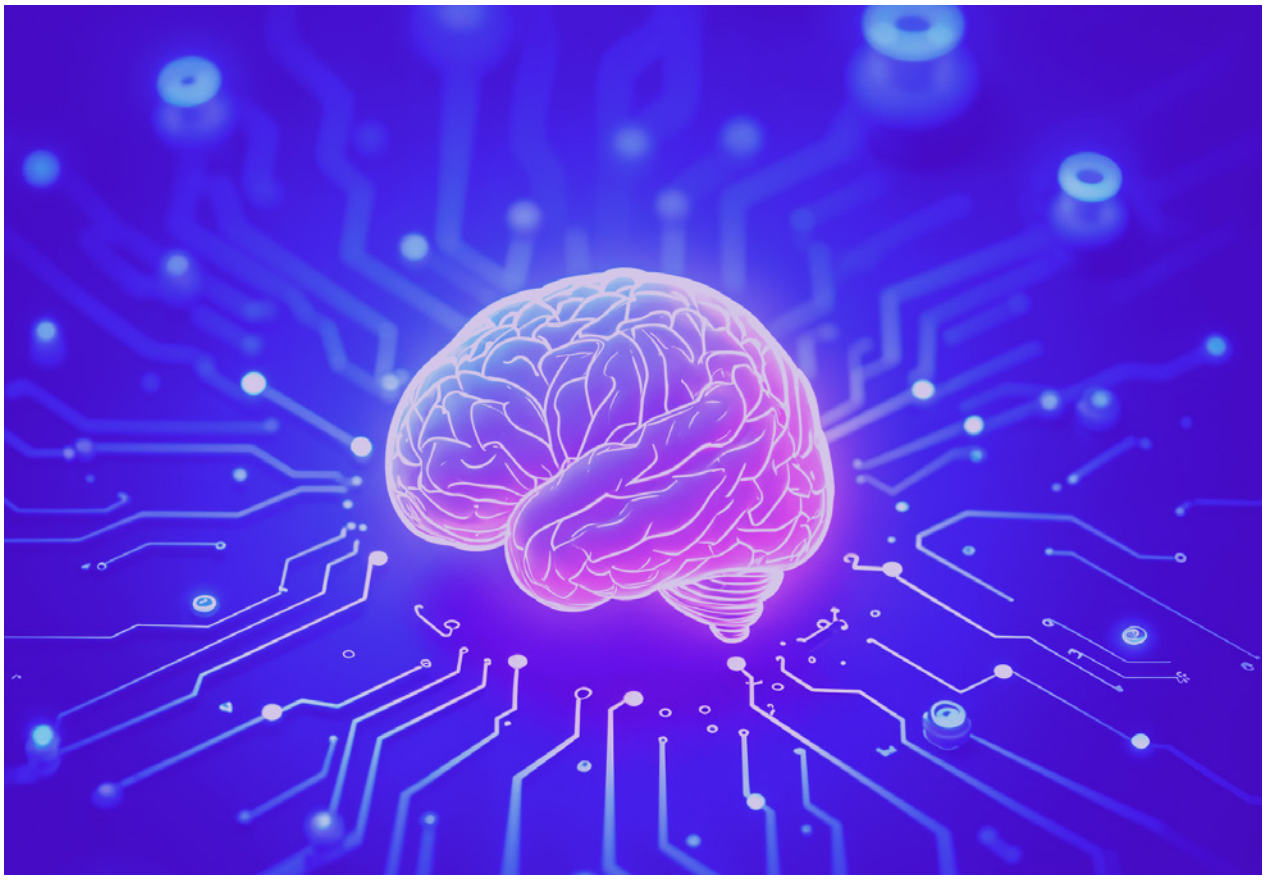
National Institute of Standards and Technology. (2024). NIST releases first 3 finalized post-quantum encryption standards. *NIST News*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

-

Ruane, J., Kiesow, E., Galatsanos, J., Dukatz, C., Blomquist, E., Shukla, P., "The Quantum Index Report 2025", MIT Initiative on the Digital Economy, Massachusetts Institute of Technology, Cambridge, MA, May 2025.

-

Sim, B., Park, A., & Han, D. (2022). Chosen-Ciphertext Clustering Attack on CRYSTALS-KYBER Using the Side-Channel Leakage of Barrett Reduction. IEEE Internet of Things Journal.



COSPAS-SARSAT, INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD

CONVERGENCIA TECNOLÓGICA PARA LA CIBERDEFENSA GLOBAL

Por BR (R) **GERARDO RUBÉN BIDEGAIN**

Palabras Clave:

> COSPAS-SARSAT
> Ciberseguridad Espacial
> Inteligencia Artificial
> MEOSAR
> Infraestructura Crítica
> Resiliencia operativa
> Cooperación internacional

1. Introducción

El Sistema Internacional **COSPAS-SARSAT (C/S)** constituye una de las expresiones más destacadas de cooperación tecnológica internacional, diseñado para detectar y localizar balizas de emergencia, como ser las ***"Emergency Position Indicating Radio Beacons" (EPIRBs);*** "Emergency Locator Transmitters" (ELTs) y ***"Personal Locator Beacons"*** (PLBs), que permiten salvar vidas en contextos marítimos, aéreos y terrestres respectivamente. Desde su concepción en 1982, el C/S ha operado como un instrumento humanitario crítico, pero su relevancia trasciende el mero rescate de vidas; se erige como *una infraestructura estratégica que integra múltiples plataformas satelitales, redes terrestres y sistemas de gestión de información*.

Es una iniciativa de cooperación internacional, de carácter humanitario y sin fines de lucro, que tiene como objetivo principal la detección y localización de balizas de emergencia para asistir en operaciones de "Search and Rescue" – "Búsqueda y Rescate" (SAR) en todo el mundo. Su nombre es un acrónimo de **"COSPAS"** (en ruso "Cosmicheskaya Sistema Poiska Avariynyh Sudovpara" - "Sistema Espacial para la Búsqueda de Buques en Peligro") y **"SARSAT"** (en inglés "Search And Rescue Satellite-Aided Trackingpara" - "Rastreo por Satélite para Búsqueda y Rescate").

Las balizas según el ámbito de uso se clasifican de la siguiente manera:

> **EPIRBs,** es una baliza de emergencia diseñada para **uso marítimo**. Se activa manualmente o automáticamente al entrar en contacto con el agua y envía una señal de socorro que ayuda a los servicios de rescate a localizar embarcaciones en peligro.
> **ELTs**, es una baliza de emergencia para **uso aeronáutico.** Se instala en aeronaves y se activa automáticamente con un impacto severo o manualmente por la tripulación. Su función es transmitir una señal de socorro que permite a los equipos SAR localizar el lugar de un accidente aéreo.
> **PLBs**, es una baliza de emergencia personal para **uso principalmente en tierra**, pero también su uso es posible en el mar o aire. Está diseñada para ser transportada por individuos y se activa manualmente.

2. Evolución histórica del COSPAS-SARSAT (1982–2025)

El Sistema C/S surgió en plena Guerra Fría como un proyecto de cooperación multilateral sin precedentes, involucrando a la Unión Soviética, Estados Unidos, Canadá y Francia. Su objetivo inicial fue la localización de personas en peligro mediante el uso de satélites **"Low Earth Orbit" (Satélites de Órbita Baja-LEO)** y **"Geostationary Equatorial Orbit"** (Satélites de Órbita Geoestacionaria-GEO), combinando capacidades de detección de señales de emergencia con Centros de Control Terrestre distribuidos internacionalmente.

Los satélites de **"Medium Earth Orbit" (Satélites de Órbita Terrestre Media - MEO)** fueron incorporados al Sistema C/S como parte de la evolución hacia el segmento **"Medium Earth Orbit Search and Rescue" (MEOSAR).** Este avance comenzó con pruebas y evaluaciones en la década de 2000, con la participación de constelaciones de satélites como:

> Galileo, es el sistema de navegación por satélite de la Unión Europea, diseñado para ofrecer posicionamiento global preciso y autónomo. La constelación está compuesta por satélites en órbita media y proporciona servicios tanto civiles como gubernamentales.
> GLONASS, es el sistema de navegación por satélite desarrollado por Rusia como alternativa al GPS. Operativo desde la década de 1990, ofrece servicios de posicionamiento y navegación a nivel global mediante una constelación de satélites en órbita terrestre media.
> GPS, es el sistema de navegación por satélite de EE.UU. Proporciona servicios de posicionamiento, navegación y sincronización a nivel mundial mediante una constelación de satélites en órbita terrestre media. Es ampliamente utilizado en aplicaciones civiles, comerciales y militares.

El Sistema MEOSAR estuvo operativo a partir del 13 de diciembre de 2016, cuando se inició la distribución operativa de datos de alertas de rescate. Posteriormente, el 25 de abril de 2023, el Consejo de COSPAS-SARSAT declaró la **"Capacidad Operativa Inicial" (IOC)** del sistema mencionado, consolidando su rol como la principal tecnología **para la localización de balizas de emergencia de 406 MHz.**

Esta incorporación ha permitido mejorar significativamente la precisión, rapidez y cobertura global en las operaciones SAR. Es un servicio satelital internacional destinado a detectar y localizar señales de socorro emitidas por balizas en situaciones de emergencia, facilitando operaciones SAR en tierra, mar o aire, al combinar las ventajas de los satélites LEO, ubicada entre

La creciente digitalización y la amenaza de ciberataques han convertido la integración de Inteligencia Artificial (IA) y Ciberseguridad Espacial (CE) en un elemento central para garantizar la resiliencia del sistema frente a amenazas contemporáneas.

los 160 y 2.000 km de altitud. Esta órbita es utilizada por satélites de observación, comunicaciones, investigación científica y estaciones espaciales debido a su baja latencia y proximidad a la Tierra y los GEO, se encuentra a unos 35.786 km sobre el ecuador. Los satélites en esta órbita giran a la misma velocidad que la Tierra, por lo que permanecen fijos sobre un punto del planeta. Es ideal para comunicaciones, meteorología y retransmisiones.

El sistema se consolidó mediante mejoras en la precisión de localización y expansión de su cobertura global. Entre los desarrollos más significativos se encuentran:

> La integración de satélites de nueva generación (LEO de órbita polar y GEO modernizados).
> La Implementación de protocolos de comunicación digital y cifrado avanzado.
> La extensión de la cooperación con organismos internacionales como la Unión Internacional de Telecomunicaciones (ITU); Organización de Aviación Civil Internacional (ICAO); Organización Marítima Internacional (IMO) y Agencia Espacial Europea (ESA).
> Los primeros estudios sobre el impacto de ciberamenazas y posibles escenarios de interferencia tecnológica, incluyendo vulnerabilidades de la cadena de suministro y ataques de día cero.

El Sistema C/S ha evolucionado hacia un sistema robusto y altamente interoperable, capaz de integrarse con otras plataformas de rescate y monitoreo internacional, constituyéndose como modelo de infraestructura crítica global. Su avance ha estado marcado por la modernización tecnológica y la expansión de su cobertura, consolidándose como una infraestructura crítica de importancia estratégica internacional. **La creciente digitalización y la amenaza de ciberataques han convertido la integración de Inteligencia Artificial (IA) y Ciberseguridad Espacial (CE) en un elemento central para garantizar la resiliencia del sistema frente a amenazas contemporáneas.**

3. Arquitectura técnica del sistema

El Sistema C/S se estructura en tres segmentos interdependientes:

1. **Segmento Espacial:** Satélites LEO, GEO y MEO equipados con receptores para señales de emergencia en 406 MHz.
2. **Segmento Terrestre:**
> **Local User Terminals (LUTs)**: Estaciones de recepción de las señales satelitales.
> **Mission Control Centers (MCCs):** procesan la información, realizan correlación de señales y envían alertas a los Centros de Coordinación Locales de Rescate.
3. **Segmento de Balizas (EPIRBs, ELTs, PLBs):**
> Dispositivos autónomos con capacidad de transmisión inmediata ante situaciones de emergencia.
> Incorporación de tecnologías de GPS para localización precisa.

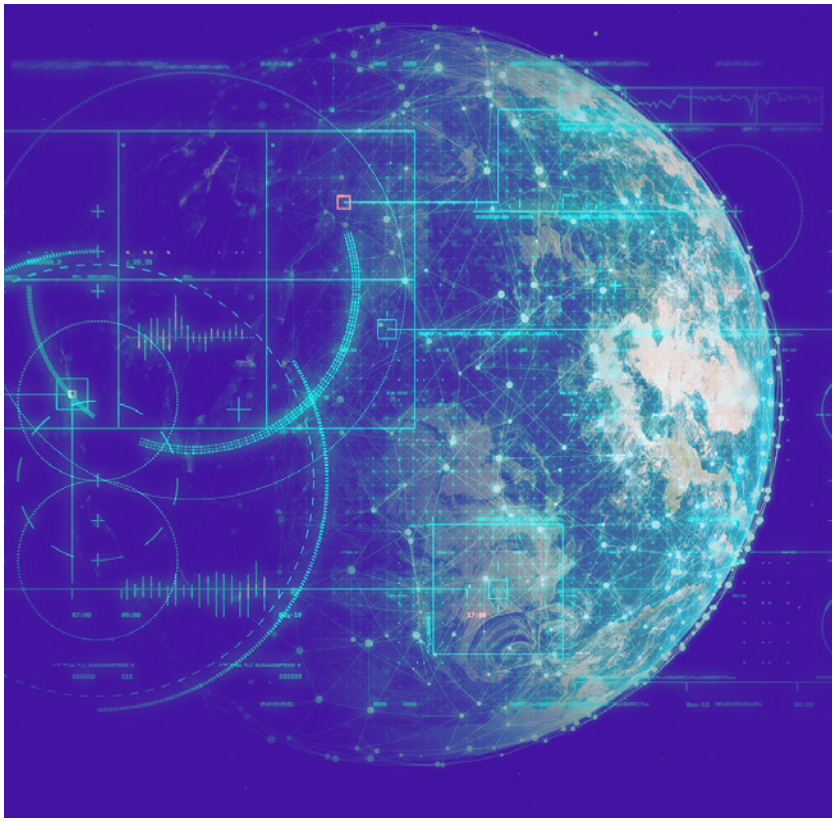
Este esquema técnico permite *alta disponibilidad, redundancia y resiliencia frente a fallos puntuales o ciberataques, aunque no está exento de vulnerabilidades emergentes.* Estos desarrollos permitieron que el Sistema C/S pasara de ser un *sistema de rescate humanitario básico a convertirse en una infraestructura estratégica de alto valor, cuya resiliencia y operatividad resultan fundamentales no solo para la seguridad humana, sino también para la estabilidad tecnológica y estratégica internacional.*

4. COSPAS-SARSAT como infraestructura crítica internacional

Más allá de su misión humanitaria, **el C/S se reconoce como una infraestructura crítica internacional, ya que impacta la seguridad marítima, aérea y terrestre de múltiples naciones y constituye un nodo vital en la interoperabilidad satelital global.** Por ello, es necesario **clasificar este sistema como prioridad estratégica,** estableciendo protocolos de monitoreo, planes de contingencia multinacionales y políticas de cooperación tecnológica internacional.

Junto con su misión humanitaria, el C/S asume funciones estratégicas que impactan la seguridad internacional, ya que:

> Garantiza la continuidad de operaciones de rescate global.



- Constituye un nodo crítico en la interoperabilidad satelital internacional.
- Su operación afecta directamente la seguridad de sistemas marítimos, aeronáuticos y terrestres de múltiples países.

En la era de la digitalización y la creciente complejidad de la ciberamenaza, la cual la podemos definir como *"toda acción, evento o posibilidad que busca vulnerar la seguridad de sistemas informáticos, redes o infraestructuras críticas mediante medios digitales, pudiendo implicar robo de información, sabotaje, interrupción de servicios o manipulación de datos".*

La convergencia de IA y CE, *"es el conjunto de medidas, políticas y tecnologías orientadas a proteger satélites, sistemas de control en tierra, enlaces de comunicación y servicios espaciales frente a ciberamenazas; siendo su objetivo garantizar la disponibilidad, integridad y confidencialidad de la información y las operaciones en el ámbito espacial"*, se vuelve un componente indispensable para garantizar la resiliencia del sistema.

Este trabajo intenta analizar la CE desde una perspectiva histórica, técnica y estratégica, abordando tanto las vulnerabilidades cibernéticas existentes como el potencial de la IA para mitigar riesgos. Asimismo, se proponen estrategias de protección orientadas a fortalecer la seguridad y sostenibilidad del entorno espacial, considerando las principales vulnerabilidades cibernéticas, el potencial de la IA y la formulación de estrategias de protección para fortalecer la seguridad del sistema en cuestión.

5. Vulnerabilidades y amenazas en el contexto de Ciberseguridad Espacial

El sistema enfrenta múltiples vulnerabilidades:

- **Spoofing:** señales falsas que pueden inducir a errores en la localización de emergencias.
- **Jamming:** interferencia intencionada de la frecuencia 406 MHz, degradando la recepción de señales.
- **Supply Chain:** Vulnerabilidad de cadena de suministro, que permiten comprometer sistemas críticos a través de proveedores o fallas aún no parcheadas.
- **Ataques de Día Cero:** es un ataque que explota una vulnerabilidad **desconocida** del software o hardware, que aún no ha sido detectada ni corregida por los desarrolladores.
- **Accesos no autorizados a los MCCs:** potencial manipulación de datos críticos.
- **Interdependencia tecnológica:** dependencia de satélites y redes externas que pueden ser vulnerables.

6. Aplicaciones de la Inteligencia Artificial en el Sistema SAR

La IA aporta mejoras significativas al sistema:

- **Clasificación automática de señales:** filtra falsas alarmas y prioriza rescates.
- **Mantenimiento predictivo:** anticipa fallos de hardware y optimiza la disponibilidad de satélites y estaciones terrestres.
- **Optimización logística:** planificación de rutas de respuesta y coordinación de equipos de rescate.
- **Predicción de incidentes y análisis de riesgos:** La IA permite anticipar escenarios complejos de emergencia, evaluar probabilidades de ocurrencia y vincular estos análisis con estrategias de Ciberseguridad, mejorando la resiliencia del sistema.

7. Inteligencia Artificial aplicada a la Ciberdefensa satelital

La IA se ha consolidado como una herramienta esencial en el

CV

BM (R) GERARDO RUBÉN BIDEGAIN

Brigadier Gerardo Rubén Bidegain, Licenciado en Sistemas Aéreos y Aeroespaciales y posgrados en Gestión para la Defensa Nacional y Producción de Información Estratégica. Especialista en Comunicaciones, con cargos en Dirección de Comunicaciones e Informática FAA, Presidencia de la Nación, Sistema COSPAS-SARSAT y J-VI C3 I GE. Participó en proyectos estratégicos, cumbres presidenciales y misiones internacionales, incluyendo Observador Militar ONU en Mozambique. Reconocimientos: Medalla ONU, premios institucionales y distinciones docentes.

ámbito de la Ciberdefensa, al potenciar las capacidades de detección, análisis y respuesta ante amenazas digitales. Su integración en sistemas de seguridad permite identificar patrones anómalos en tiempo real, automatizar respuestas ante incidentes y anticiparse a posibles ataques mediante técnicas predictivas. Estos avances mejoran significativamente la eficiencia de los equipos de seguridad y reducen el tiempo de reacción frente a incidentes.

En lugar de tratar estos beneficios en distintas secciones, es más efectivo presentar un enfoque integrado: *la IA no solo facilita la detección de intrusiones o la contención automatizada de amenazas, sino que también optimiza la gestión de riesgos y la asignación de recursos en entornos complejos.* De esta forma, su rol no se limita a la reacción, sino que se extiende a la prevención y adaptación continua frente a un panorama de amenazas en constante evolución.

La IA desempeña un rol clave en Ciberdefensa:

- **Detección de intrusiones (IDS) en satélites:** identifica comportamientos anómalos o no autorizados.
- **Respuesta automática a amenazas:** bloquea ataques y genera protocolos de mitigación en tiempo real.
- **Simulación de ciberataques:** permite anticipar vulnerabilidades emergentes y entrenar al personal en escenarios controlados.

Para fortalecer la resiliencia y capacidad estratégica del sistema, se proponen las siguientes líneas de acción para un observatorio de Ciberdefensa:

1. Fomentar alianzas internacionales de investigación permanente en Ciberseguridad espacial, inteligencia artificial y resiliencia operativa.
2. Fomentar alianzas internacionales con organismos como ITU, ESA, ICAO y la Secretaría de C/S para compartir información sobre amenazas y mejores prácticas.
3. Implementar un marco normativo nacional con criptografía post-cuántica, estándares de Ciberseguridad y protocolos de protección de infraestructura crítica.
4. Realizar ejercicios conjuntos de Ciberseguridad y SAR para entrenar personal y validar protocolos de respuesta ante contingencias.
5. Formar talentos multidisciplinarios, combinando expertos en IA, Ciberseguridad, ingeniería espacial y operaciones de rescate.

En el ámbito de la Ciberdefensa, la IA posibilita la detección temprana de intrusiones y anomalías en sistemas satelitales, la automatización de respuestas

frente a ataques y la simulación de escenarios complejos para el entrenamiento de personal especializado. La implementación de estas tecnologías permite anticipar amenazas, reducir tiempos de reacción y fortalecer la resiliencia de la infraestructura crítica.

La integración de IA con sistemas de monitoreo continuo y análisis predictivo constituye un componente esencial para la protección del C/S frente a ataques híbridos, interferencias estratégicas y manipulación de datos críticos. Asimismo, la IA facilita la elaboración de informes prospectivos y la planificación de estrategias de mitigación basadas en escenarios de riesgo.

8. Escenarios prospectivos y riesgos estratégicos

El contexto global actual indica que la proliferación de actores con capacidades cibernéticas avanzadas y la interdependencia tecnológica de infraestructuras interconectadas generan riesgos estratégicos complejos. La preparación ante estos escenarios requiere el desarrollo de estrategias multinacionales, el fortalecimiento de alianzas internacionales y la implementación de tecnologías avanzadas de Ciberdefensa.

El sistema enfrenta riesgos derivados de la militarización del espacio, la proliferación de actores con capacidades cibernéticas y el aumento de interdependencias tecnológicas:

- Conflictos híbridos con ataques cibernéticos sobre satélites LEO, GEO y MEO.
- Interferencia estratégica en operaciones SAR durante crisis humanitarias.
- Competencia internacional por control y acceso a frecuencias críticas.
- Riesgo de desinformación y manipulación de datos críticos en operaciones de rescate.

9. Sugerencias para fortalecer y proteger el Sistema COSPAS-SARSAT

Sugerencia 1: Clasificación de COSPAS-SARSAT como infraestructura crítica prioritaria: El Sistema C/S constituye una infraestructura esencial para la seguridad y salvamento internacional, operando en un marco multilateral que permite la detección y localización de personas, buques y aeronaves en situación de emergencia. Dada su relevancia estratégica, el sistema en cuestión debería ser clasificado como **"Infraestructura Crítica Prioritaria"**, reconociendo formalmente su vulnerabilidad frente a amenazas cibernéticas y físicas.

Esta clasificación implicaría la implementación de **"Protocolos de Monitoreo Continuo"** sobre todos los componentes críticos del sistema, incluyendo satélites, estaciones terrenas y enlaces de comunicaciones, con especial énfasis en la detección temprana de intrusiones, interferencias o anomalías operativas que puedan comprometer la integridad, disponibilidad o confiabilidad del servicio.

Asimismo, se sugiere el diseño y puesta en marcha de **"Planes de Contingencia Multinacionales"**, coordinados entre los Estados miembros de C/S, que contemplen escenarios de interrupción parcial o total del sistema. Dichos planes podrían incluir:

1. **Procedimientos de respaldo y redundancia:** Establecer rutas alternativas de comunicación, capacidades de retransmisión y satélites de reemplazo en caso de fallo.
1. **Cooperación internacional y protocolos de alerta:** Definir mecanismos de comunicación rápida entre centros de control de diferentes países para garantizar una respuesta coordinada ante emergencias.
1. **Pruebas y simulacros periódicos:** Realizar ejercicios regulares que validen la efectividad de los procedimientos de contingencia y el tiempo de respuesta frente a incidentes cibernéticos o físicos.
1. **Evaluación y actualización continua:** Mantener un registro dinámico de vulnerabilidades, amenazas emergentes y mejores prácticas internacionales, asegurando que la protección del sistema evolucione al ritmo de los avances tecnológicos y tácticas de ataque.

La adopción permitiría adoptar reforzar la **resiliencia operativa del Sistema C/S**, asegurando que continúe cumpliendo su misión crítica de salvar vidas y brindar servicios de alerta de emergencia a nivel global, incluso ante incidentes de Ciberseguridad de alta complejidad o conflictos internacionales.

Sugerencia 2: Mapear vulnerabilidades y diseñar planes de mitigación cibernética: Dada la creciente sofisticación de las amenazas cibernéticas, es imprescindible que el Sistema C/S cuente con un **"Programa Integral de Identificación de Vulnerabilidades"** y **"Mitigación de Riesgos"**, garantizando la continuidad y confiabilidad de sus operaciones críticas. Para ello, se propone implementar las siguientes acciones:

1. **Mapeo exhaustivo de vulnerabilidades:** Realizar un inventario detallado de todos los componentes del sistema (satélites, estaciones terrenas, enlaces de comunicación, servidores y software de gestión), identificando posibles puntos de ataque, debilidades en protocolos de comunicación y riesgos asociados a terceros proveedores. Este mapeo debe actualizarse periódicamente, considerando nuevas tecnologías y amenazas emergentes.
2. **Pruebas de penetración cibernética controladas bajo**

estándares internacionales: Ejecutar simulaciones de ataques bajo entornos controlados para evaluar la resiliencia del sistema frente a intrusiones, ransomware, interferencias satelitales o manipulación de datos críticos. Los resultados de estas pruebas deben servir para priorizar acciones correctivas y fortalecer los mecanismos de defensa.

3. **Redundancia tecnológica:** Implementar **sistemas paralelos y rutas de comunicación** alternativas que garanticen la continuidad operativa ante fallas de hardware, interrupciones de enlace o ataques dirigidos. Esto incluye servidores de respaldo, enlaces satelitales duplicados y mecanismos automáticos de conmutación ante fallos.
4. **Planes de mitigación integrales:** Con base en el mapeo de vulnerabilidades y las pruebas de penetración, se deben desarrollar **procedimientos de respuesta y recuperación,** incluyendo la priorización de activos críticos, protocolos de comunicación de incidentes y ejercicios de simulación de escenarios de contingencia.

La adopción de estas medidas permitiría que el Sistema C/S mantenga una **postura defensiva proactiva,** reduciendo significativamente el riesgo de interrupciones operativas y asegurando que el sistema pueda continuar ofreciendo servicios esenciales de alerta y rescate en situaciones de emergencia a nivel global.

Sugerencia 3: Fortalecer la cooperación internacional y el intercambio seguro de información. El Sistema C/S opera bajo un esquema multinacional, donde la coordinación entre estados miembros es esencial para garantizar la efectividad de las operaciones SAR. En este contexto, se podría establecer medidas que aseguren tanto la colaboración como la protección de información crítica frente a amenazas cibernéticas y operativas, de acuerdo al siguiente detalle:

1. **Protocolos estandarizados de intercambio de información con autenticación robusta y cifrado:** Desarrollar y adoptar procedimientos uniformes que permitan la transferencia segura de datos de emergencias entre Centros de Control, estaciones terrenas y agencias SAR. Esto incluye el uso de protocolos de autenticación robustos y firmas digitales para validar la integridad de la información.
2. **Acuerdos de cooperación multinacional: Formalizar "Memorandos de Entendimiento y Convenios Operativos"** que definan roles, responsabilidades y mecanismos de alerta temprana entre los estados miembros, asegurando una respuesta coordinada ante incidentes y la disponibilidad de recursos compartidos.
3. **Redes de comunicación resilientes y segregadas:** Implementar canales de comunicación redundantes y segmentados que minimicen el riesgo de interrupciones o interferencias externas, garantizando que la información crítica pueda fluir incluso en escenarios de ataque cibernético o fallas técnicas.
4. **Capacitación conjunta y ejercicios de interoperabilidad:** Organizar simulacros regulares y programas de formación multinacional que entrenen al personal en la operación conjunta del sistema, manejo seguro de información y respuesta ante incidentes, fortaleciendo la confianza y la coordinación entre países.
5. **Monitoreo y auditoría continua:** Establecer mecanismos de seguimiento permanente para evaluar la efectividad de la cooperación internacional y detectar posibles brechas de seguridad o fallos operativos, incorporando mejoras continuas basadas en lecciones aprendidas y estándares internacionales de ciberseguridad.

En el ámbito de la Ciberdefensa, la IA posibilita la detección temprana de intrusiones y anomalías en sistemas satelitales, la automatización de respuestas frente a ataques y la simulación de escenarios complejos para el entrenamiento de personal especializado.

La implementación de estas medidas fortalecería la **resiliencia global del Sistema C/S**, asegurando que los flujos de información crítica sean confiables y que la cooperación multinacional se mantenga eficiente incluso frente a amenazas cibernéticas sofisticadas, ataques dirigidos o interrupciones operativas.

Sugerencia 4: Implementar programas de capacitación y concientización en Ciberseguridad para personal clave. La protección del Sistema C/S no recae exclusivamente en medidas tecnológicas, sino también en el factor humano, considerado uno de los eslabones más críticos en la seguridad de infraestructuras estratégicas. Por ello, se recomienda establecer un "Programa Integral de Formación" y concientización en Ciberseguridad dirigido al personal operativo, técnico y de gestión involucrado en la operación del sistema, a través de:

1. **Capacitación especializada:** Desarrollar cursos y talleres avanzados que aborden **amenazas cibernéticas emergentes, protocolos de seguridad, respuesta a incidentes y manejo de sistemas críticos,** adaptados al nivel de responsabilidad de cada rol dentro de la organización.
2. **Simulaciones de incidentes y ejercicios prácticos: Implementar ejercicios regulares de ciberataques simulados** que permitan al personal practicar la detección, mitigación y recuperación ante incidentes, fortaleciendo la reacción ante escenarios reales y mejorando la coordinación interdepartamental.
3. **Programas de concientización continua:** Establecer campañas permanentes que refuercen la cultura de seguridad, fomentando hábitos como el uso de contraseñas seguras, identificación de correos sospechosos, manejo seguro de dispositivos y protocolos de comunicación seguros.
4. **Evaluación y certificación del personal:** Incorporar mecanismos de **evaluación periódica** de conocimientos y competencias en Ciberseguridad, así como certificaciones reconocidas internacionalmente, garantizando que el personal mantenga un nivel adecuado de preparación frente a riesgos emergentes.
5. **Actualización ante nuevas amenazas:** Adaptar los contenidos y metodologías de capacitación de forma continua, considerando **avances tecnológicos, vulnerabilidades detectadas y nuevas tácticas de ataque,** para asegurar que el personal esté siempre preparado para enfrentar desafíos contemporáneos.

La implementación de esta recomendación permitirá que el Sistema C/S cuente con una **fuerza humana altamente capacitada y consciente de los riesgos,** reduciendo significativamente la probabilidad de errores operativos o brechas de seguridad.

Sugerencia 5: Desarrollar infraestructura tecnológica de última generación y sistemas de resiliencia operativa. Para garantizar la continuidad y confiabilidad del Sistema C/S ante fallas técnicas, desastres naturales o ataques cibernéticos, es imprescindible invertir en infraestructura tecnológica avanzada y mecanismos de resiliencia operativa que minimicen la interrupción del servicio y protejan los activos críticos, mediante:

1. **La Modernización de Estaciones Terrenas:** Actualizar equipos de recepción, transmisión y procesamiento de señales, incorporando tecnologías de alto desempeño, sistemas de monitoreo automatizados que detecten anomalías en tiempo real y la actualización constante de software y hardware para reforzar la Ciberseguridad.
2. **Redundancia integral de sistemas**: Implementar **duplicación de enlaces de comunicación y servidores críticos,** de manera que ante cualquier fallo o ataque se

active automáticamente un sistema de respaldo sin pérdida de funcionalidad.

3. **Sistemas de recuperación ante desastres**: Establecer centros de respaldo geográficamente distribuidos, con capacidad de asumir operaciones completas en caso de interrupción de los centros principales, asegurando que la disponibilidad del servicio no se vea comprometida.
4. **Tecnologías de Ciberdefensa incorporadas: Integrar soluciones avanzadas de detección de intrusiones, análisis de tráfico anómalo y protección de "endpoints"**, que operen en paralelo con los sistemas de control del servicio, garantizando la defensa proactiva frente a amenazas cibernéticas sofisticadas.
5. **Monitoreo Predictivo y Mantenimiento Preventivo:** Desarrollar herramientas de **análisis predictivo basadas en IA** que permita anticipar fallas, optimizar recursos y reducir el tiempo de inactividad.

La implementación de estas medidas asegurará que el Sistema C/S mantenga **alta disponibilidad y confiabilidad operativa,** fortaleciendo su capacidad para cumplir su misión crítica de alerta y rescate en emergencias, incluso frente a escenarios de alto riesgo tecnológico o ciberataques complejos.

Sugerencia 6: Implementar un sistema de monitoreo y evaluación continua del desempeño y la seguridad. La resiliencia y eficiencia del Sistema C/S dependen de un **seguimiento constante de su operación y de la seguridad de sus componentes críticos.** Por ello, se recomienda establecer un "Sistema integral de monitoreo y evaluación continua", que permita detectar fallas, vulnerabilidades y oportunidades de mejora de manera proactiva, mediante el:

1. **Monitoreo en tiempo real:** Integrar **plataformas centralizadas de supervisión** que recojan datos de satélites, estaciones terrenas y enlaces de comunicación, permitiendo la detección inmediata de anomalías operativas, ciberataques o fallas técnicas.
2. **Indicadores de desempeño y seguridad:** Definir métricas específicas para evaluar la **disponibilidad del servicio, tiempos de respuesta, eficacia de los protocolos de contingencia y nivel de protección cibernética,** asegurando un análisis cuantitativo del funcionamiento del sistema.
3. **Alertas y notificaciones automatizadas:** Configurar sistemas que generen **alertas tempranas** ante desviaciones críticas, vulnerabilidades detectadas o amenazas emergentes, permitiendo la activación inmediata de planes de mitigación y contingencia.
4. **Auditorías periódicas y revisiones de seguridad:** Realizar evaluaciones formales y auditorías externas para validar la eficacia de los controles implementados, la robustez de la infraestructura tecnológica y la preparación del personal frente a incidentes, incluyendo simulacros de ciberataques. Estos **simulacros de ciberataques** deben ser ejercicios controlados que **imiten ataques reales a sistemas informáticos o redes críticas,** con el objetivo de probar la capacidad de respuesta, detectar vulnerabilidades, entrenar al personal y validar los protocolos de seguridad sin afectar la operación real del sistema. Son ejercicios controlados que imitan ataques reales a sistemas informáticos o redes críticas,

con el objetivo de probar la capacidad de respuesta, detectar vulnerabilidades, entrenar al personal y validar los protocolos de seguridad sin afectar la operación real del sistema.

5. **Retroalimentación y mejora continua:** Implementar un ciclo sistemático de análisis y ajuste, donde los resultados de monitoreo, simulacros y auditorías alimenten mejoras operativas, tecnológicas y de Ciberseguridad, garantizando que el sistema evolucione frente a nuevas amenazas y requerimientos.

La adopción de estas medidas permitirá que el Sistema C/S mantenga una **operación confiable, segura y resilientes,** garantizando que la infraestructura crítica esté siempre disponible para cumplir su misión de alerta y rescate internacional, incluso en escenarios complejos o bajo presión de amenazas cibernéticas.

10. Conclusiones

El Sistema Internacional C/S se erige como una de las infraestructuras críticas más relevantes a nivel global, articulando cooperación tecnológica, humanitaria y estratégica entre múltiples países y organismos internacionales. Su evolución desde 1982 hasta la consolidación del MEOSAR transformó un dispositivo de salvamento en una red de alcance planetario, capaz de sostener operaciones SAR de manera inmediata, precisa y coordinada.

En el escenario actual, marcado por la digitalización, la interdependencia tecnológica y la creciente sofisticación de las ciberamenazas, la mera modernización tecnológica resulta insuficiente. **La protección del C/S requiere integrar la IA y la Ciberseguridad Espacial como ejes transversales, no solo para garantizar la continuidad operativa, sino también para preservar la confianza internacional en el sistema.**

La IA ofrece ventajas disruptivas en el filtrado de falsas alarmas, mantenimiento predictivo, optimización logística y detección de intrusiones, constituyéndose en una herramienta indispensable para anticipar vulnerabilidades y responder en tiempo real frente a incidentes complejos. De igual modo, la cooperación multinacional, la estandarización de protocolos y la capacitación permanente del personal se consolidan como pilares de la resiliencia operativa.

Las sugerencias planteadas —clasificación del Sistema C/S como infraestructura crítica prioritaria, mapeo exhaustivo de vulnerabilidades, cooperación internacional reforzada, formación especializada, inversión en infraestructura de última generación y monitoreo continuo— delinean un marco estratégico integral para la protección y sostenimiento del sistema.

El análisis prospectivo indica que la militarización del espacio, los conflictos híbridos y la competencia por el control de frecuencias críticas configuran riesgos cada vez más tangibles. En este contexto, la resiliencia del Sistema C/S no debe depender únicamente de tecnologías avanzadas, sino de una gobernanza multinacional robusta, flexible y adaptativa, capaz de articular respuestas conjuntas frente a amenazas globales.

En definitiva, el futuro del Sistema C/S depende de su capacidad para adaptarse al nuevo paradigma de seguridad tecnológica. La convergencia entre IA y Ciberseguridad Espacial constituye una necesidad estratégica, fortaleciendo la continuidad de operaciones de rescate, preservando la estabilidad de la infraestructura crítica y garantizando que el sistema cumpla su misión humanitaria y estratégica en un entorno global crecientemente desafiante.

BIBLIOGRAFÍA

COSPAS-SARSAT Secretariat. (s.f.). *System Overview and Operations Manual.* Recuperado de https://www.sarsat.noaa.gov/cospas-sarsat-system-overview/

-

International Telecommunication Union (ITU). (2024). *Radio Regulations.* Recuperado de https://www.itu.int/pub/R-REG-RR

-

European Space Agency (ESA). (2024). *How ESA ensures cybersecurity in space.* Recuperado de https://www.esa.int/About_Us/Cyber_resilience_at_ESA/How_ESA_ensures_cybersecurity_in_space

-

International Civil Aviation Organization (ICAO). (2018). *Safety Management Manual* (Doc 9859). Recuperado de https://aviassist.org/icao-safety-management-manual/-

Freedman, L. (2013). *Strategy: A History.* Oxford University Press.

-

International Maritime Organization (IMO). (2019). *Global Maritime Distress and Safety System (GMDSS) Manual.* Recuperado de https://www.imo.org/en/OurWork/Safety/Pages/IMO-circulars-related-to-the- GMDSS.aspx

-

United Nations Office for Outer Space Affairs (UNOOSA). (2021). *Guidelines for the Long-term Sustainability of Outer Space Activities.* Recuperado de https://www.unoosa.org/documents/pdf/PromotingSpaceSustainability/Publication_Final_English_June2021.pdf

¿TERCERIZACIÓN DE LA PAZ?

ANÁLISIS DE LAS OPERACIONES DE PAZ A MANOS DE EMPRESAS PRIVADAS.

Por **GD (R) CARLOS PÉREZ AQUINO**

Palabras Clave:
> Tercerización de la paz
> Empresas militares privadas
> Seguridad Internacional
> Derecho Internacional Humanitario
> Operaciones de paz

Resumen
En el presente artículo se analiza el fenómeno de la eventual tercerización de las operaciones de paz a través del uso de empresas militares y de seguridad privadas (PMSC por su sigla en inglés), y se exploran sus implicancias estratégicas, jurídicas y éticas en el contexto de los conflictos contemporáneos. A partir de una revisión de casos relevantes, se examina la evolución del papel de las PMSC, su impacto en el Derecho Internacional Humanitario (DIH) enfocado en las operaciones de paz, así como los desafíos que plantea su regulación. Se concluye que, si bien estas empresas ofrecen capacidades especializadas que pueden resultar efectivas para los Estados y organismos internacionales, su utilización presenta riesgos significativos para la transparencia, la rendición de cuentas y la protección de los derechos humanos.

A 80 años de la creación de la Organización de las Naciones Unidas observamos que el sublime propósito de los pueblos de las Naciones Unidas de *"preservar a las generaciones venideras del flagelo de la guerra que dos veces durante nuestra vida ha infligido a la Humanidad sufrimientos indecibles"* (ONU, 1945) parece no haberse logrado. La violencia sigue presente y los mecanismos de la seguridad global que debían evitar o al menos limitar el sufrimiento humano se encuentran severamente cuestionados. Las complejidades de los conflictos actuales plantean dudas sobre la eficacia de la herramienta por las que la ONU se ha hecho merecedora del Premio Nobel de la Paz: *las Operaciones de Paz.*

Además, se ha planteado que la burocracia de la ONU dificulta su empleo eficiente, y se han comparado los gastos incurridos en una determinada situación por parte de las tropas de la ONU, con las de las tropas rentadas a compañías privadas. La participación de este tipo de "contratistas" en Haití abre interrogantes sobre los resultados que se pueden obtener, cuando la ONU ya se desplegó allí reiteradas veces sin soluciones.

Es por eso que debemos señalar el avance de las organizaciones regionales e incluso de Compañías Privadas de Seguridad y Militares en roles que tradicionalmente estaban reservados a la ONU. Las denominadas "operaciones paralelas" o las operaciones de paz multilaterales, así denominadas por el Instituto internacional de investigación de la Paz de

Estocolmo (SIPRI por sus siglas en inglés), son formas alternativas a las operaciones.

Se vive hoy en un mundo marcado por la vigencia de la geopolítica y la complejización de las guerras convencionales e hibridas, con un rol predominante de la tecnología, que obliga a replantearse las técnicas, tácticas y el planeamiento operacional y estratégico. Es en este entorno en el que el fenómeno de "tercerización de la guerra" ha cobrado protagonismo como herramienta estratégica y táctica en el escenario internacional. Aunque esta no es una novedad, su recurrencia y expansión en el siglo XXI la convierten en un rasgo característico de la conflictividad moderna.

Hacia la primera década del siglo XXI, las empresas militares privadas y de seguridad ya habían pasado de ser subcontratistas menores a ser corporaciones que representaban la mitad del personal desplegado en Irak. Esta evolución es materia de estudio, dada su omnipresencia en los conflictos contemporáneos. Un punto de inflexión en este proceso se produjo cuando la consecución de objetivos deseables en distintos escenarios –como el ya mencionado de Irak, y el de Afganistán– fue permitida por las capacidades especializadas de las PMSC, y no por ejércitos soberanos; y luego, cuando las PMSC fueron capaces de ofrecer un rendimiento que ningún otro tipo de organización podía lograr, se constituyeron como una industria independiente de la que empezaron a depender distintas autoridades, como las estadounidenses y británicas (Baum y McGahan, 2011).

El empleo de estos contratistas –que no está exento de cuestionamientos por su estatus legal, su falta de "rendición de cuentas" en el sentido más amplio, la opacidad de sus vínculos y los excesos verificados en su empleo–, también alcanza de diversas maneras la esfera de las operaciones de paz, por lo que debemos mirar atentamente a estos actores que ya están presentes en casi todos los escenarios de conflicto contemporáneos.

Viejas prácticas, nuevas formas

Desde la Guerra Fría, las guerras proxy con el empleo de PMSC han sido instrumentos de política exterior que permiten a los Estados influir en conflictos ajenos sin exponerse directamente. Lo que era una táctica ocasional ha mutado en una práctica extendida. Hoy, en conflictos como los de Ucrania, Siria, Yemen y varias regiones africanas, la participación indirecta de potencias globales y regionales mediante insurgencias aliadas locales, milicias o contratistas privados se ha vuelto la norma.

Pero **¿qué tareas realizan las PMSC?** Las PMSC ofrecen servicios de combate y seguridad a sus

Los países africanos, incapaces de combatir por sí solos el terrorismo, y ante el aparente fracaso de la ONU y los ejércitos europeos desplegados de forma directa, tuvieron que buscar otras soluciones. A esto debemos agregar un clima antioccidental el los años recientes, producto del abandono de occidente a varios Estados africanos.

clientes a cambio de un pago por dichos servicios. Existen dos tipos de propiedad en las corporaciones militares privadas: *privadas o semi-gubernamentales.* Si bien las empresas militares privadas proporcionan guardias armados a organizaciones gubernamentales y no gubernamentales en el país de origen, existe una tendencia a contratar contratistas militares privados y enviarlos a misiones en el extranjero.

Presencia como gestores de paz/ seguridad, algunos ejemplos

Los ejemplos del empleo de estas empresas son variados y es una práctica antigua que se ha *aggiornado.* Se verifica una presencia muy significativa en ambientes particulares, donde llevan a cabo operaciones conjuntas con fuerzas regulares en algunos escenarios, mientras que en otros trabajan casi de manera autónoma. A continuación, se exponen varios ejemplos.

A menudo se cita el ejemplo de la empresa sudafricana –ya disuelta– Executive Outcomes (EO). Esta tuvo un contrado en Angola para la protección de pozos petrolíferos, lo que la posicionó frente a los gobiernos africanos. A continuación, tuvo un contrato con el gobierno de Sierra Leona con la finalidad de detener al Frente Revolucionario Unido (FRU). Al respecto, Arévalo (2019) dice que: *"Aunque sus procedimientos resultaran criticables en muchos aspectos, EO se mostró muy eficaz: por 35 millones de dólares, logró derrotar en 21 meses al FRU, sin tener nunca sobre el terreno más de 300 hombres y sufriendo solamente 6 muertes entre sus filas. Un éxito si tenemos en cuenta que la misión de la ONU en este mismo país, enviada tras el golpe de estado de 1997, costó 47 millones en ocho meses y hubo de abandonarlo cuando las fuerzas del FRU se acercaron de nuevo a la capital. EO demostró que las PMC son una opción barata para solucionar problemas que los ejércitos regulares no pueden afrontar".*

Está claro que tanto los Estados, como la ONU e incluso las ONGs, son incapaces de ejecutar determinadas tareas relacionadas con la defensa o la seguridad, por lo que apelan de manera creciente a estos recursos, como veremos más adelante. Lo que se señala es que la apelación a estos contratistas se lleva a cabo muchas veces cuando los Estados consideran que los recursos "oficiales" son insuficientes para el cumplimiento de una tarea.

Sean McFate (2019) relata en primera persona un requerimiento de una misión que tanto la CIA como las FFEE habían descartado, ya que *"si un equipo de la CIA o de operaciones especiales se metiera en problemas, el gobierno de los EEUU tendría que hacer algo: organizar un salvamento, pagar un gran rescate, o hacerlo público. Pero no es así con los contratistas"*. La tarea en cuestión era preservar la vida del presidente de Burundi que había sido amenazada por las FNL (Fuerzas Nacionales de Liberación, integradas por extremistas Hutus), ya que su muerte podría desencadenar, muy probablemente, un genocidio. Esta misión, calificada como "imposible", fue puesta en manos de McFate, que organizó su equipo y relata: *"unas semanas más tarde, el FNL atacó y hubo una batalla nocturna en las calles de Bujumbura, la capital de Burundi. El presidente sobrevivió y el FNL se retiró de regreso al Congo. Evitamos el genocidio".*

Los países africanos, incapaces de combatir por sí solos el terrorismo, y ante el aparente fracaso de la ONU y los ejércitos europeos desplegados de forma directa, tuvieron que buscar otras soluciones. A esto debemos agregar un clima antioccidental el los años recientes, producto del abandono de occidente a varios Estados africanos.

Un ejemplo de esto es el caso de Mali, donde el grupo ruso Wagner está presente desde 2021, tras un golpe militar para ayudar a combatir a los grupos terroristas, en reemplazo de las tropas francesas y las fuerzas de paz internacionales. Sin embargo, el ejército maliense y los mercenarios rusos tuvieron dificultades para frenar la violencia en el país, y ambos han sido

acusados de atacar civiles. Luego de tres años y medio combatiendo la insurgencia y el terrorismo islámico, la empresa dejó el país (Banchereau, 2025). Desde 2017 Wagner ha tenido una presencia significativa en África, donde brinda apoyo militar y de seguridad a varios gobiernos a cambio de acceso a recursos naturales y ubicaciones estratégicas. Algunos de los países en los que Wagner ha operado incluyen a la República Centroafricana, Sudán, Libia, Malí, Níger y Mozambique. Recientemente, las actividades de Wagner en África han sido reemplazadas por el nuevo *Africa Corps,* bajo el control directo del Ministerio de Defensa ruso.

Indudablemente se trata de un fenómeno cuyas dimensiones eran difíciles de imaginar a fines del siglo pasado, pero que tal como se ha expuesto, tienen una enorme vigencia en la lucha geopolítica actual.

Marco legal de las PMSC

Compañías como las célebres Wagner o *Blackwater,* actúan en una delgada línea entre lo legal y lo ilegal, es por eso que la proliferación de estos actores plantea interrogantes éticos y jurídicos sobre el control del uso de la fuerza.

Es necesario, a priori, tratar de determinar cuál es su estatus jurídico. El DIH (Derecho Internacional Humanitario) contempla la presencia y la protección de tres categorías de participantes en los conflictos armados: combatientes, no combatientes y civiles que acompañan la fuerza, y los que prestan apoyo sin participar en las hostilidades; entonces se puede entender que el DIH protege a los contratistas de las PMSC cuando actúan como civiles, pero pierden esa protección si participan directamente en las hostilidades. Además, no gozan del estatus de combatiente ni de prisionero de guerra, salvo que, con carácter excepcional, estén integrados oficialmente en las Fuerzas Armadas de una de las partes en conflicto.

El Documento de Montreux – firmado en 2008, y cuya finalidad es recordar las obligaciones jurídicas internacionales para los Estados que se involucran con PMSC–, ha generado diversas opiniones en la comunidad internacional, académica y de derechos humanos, en relación con su valor y efectividad para regular a las empresas militares y de seguridad privadas. A pesar de que se le reconoce, ser el primero en abordar el problema que generó la primera respuesta multilateral, y haber sentado las bases para el Código Internacional de Conducta para Proveedores de Servicios de Seguridad Privada (ICoC por sus siglas en inglés) y otras regulaciones más concretas dentro del sector; se destaca por otro lado que su carácter no vinculante y altamente dependiente de la voluntad política de los Estados proporciona una muy limitada protección a los derechos humanos y no impone ningún tipo de rendición de cuentas a las PMSC. A su vez, el documento evita pronunciarse claramente sobre si las PMSC pueden o no participar directamente en hostilidades, lo cual abre una zona gris en el DIH.

El ya mencionado ICoC es un documento no vinculante, en el cual las empresas adheridas voluntariamente aceptan cumplir con ciertos estándares éticos y operativos. Al firmarlo, estas empresas se someten a la supervisión del ICoCA (Asociación Internacional de Código de Conducta), una organización con múltiples actores. El ICoC es un instrumento *soft law* con fuerte valor ético, creciente reconocimiento internacional y potencial para mejorar las prácticas del sector, pero su impacto real depende del contexto político y contractual en el que se aplique.

En definitiva, la falta de legislación vinculante en el plano internacional y las serias limitaciones para aplicar el derecho que puede tener un Estado en el que operan las PMSC, generan una laguna legal difícil de solucionar.

Las OMP ¿tercerizadas?

La tercerización de la guerra plantea una seria amenaza a los esfuerzos de pacificación duradera. La multiplicación de actores con agendas fragmentadas, la opacidad de sus vínculos y la falta de control estatal sobre la violencia dificultan enormemente la resolución de los conflictos. La paz, como la guerra, también podría estar siendo tercerizada, y no siempre a favor de los pueblos que la necesitan.

Pero **¿qué pasa si la paz es tercerizada?** Ya a mediados de los 90, y como resultado de los fracasos en Somalia y Ruanda, la idea de "privatizar la paz" rondaba en la ONU. Si bien el secretario

general por aquel entonces, Koffi Annan, rechazaba las ideas con el planteo de que quizás el mundo no debía estar preparado para privatizar la paz (Annan, 1998. Citado por Fitzsimons, 2014), el ejemplo de la eficacia de EO en Sierra Leona, y la falta de tropas disponibles para enfrentar este tipo de situaciones, llevaba a pensar seriamente esta alternativa.

Hoy la presencia de grupos terroristas como Boko Haram, el Estado Islámico en África Occidental (ISWAP), el JNIM (*Jama'at Nasr al-islam wal Muslimin*) y *Al-Murabitun*, entre otros, potencia las necesidades de seguridad y compromiso a los responsables de ejecutarla. Cuando ese compromiso es limitado o inexistente, recurrir a los contratistas no plantea muchas objeciones.

La ONU, a través del UNDSS *(United Nations Safe and Security)* emitió las Directivas para el empleo de los Servicios de Seguridad Armada por parte de Compañías Privadas de Seguridad en 2012. Este establece las responsabilidades respecto a la seguridad y protección del personal de la ONU del gobierno anfitrión. Cuando esta responsabilidad no es asumida se puede recurrir a servicios de seguridad proporcionados por Estados miembros o parte del sistema de seguridad de la ONU.

"De manera excepcional, para cumplir sus obligaciones, el Sistema de Gestión de la Seguridad de las Naciones Unidas podrá recurrir a empresas privadas para prestar servicios de seguridad armada cuando las condiciones de amenaza y las necesidades del programa lo justifiquen. El principio fundamental que orienta cuándo utilizar los servicios de seguridad armados de una empresa de seguridad privada es que estos pueden considerarse solamente cuando no es posible proporcionar seguridad armada adecuada y apropiada por parte del gobierno anfitrión, de los Estados miembros alternativos o de recursos internos del sistema de las Naciones Unidas, como los Servicios de Seguridad y Vigilancia o los oficiales de seguridad contratados directamente por una misión o por conducto de otra organización del Sistema de Gestión de la Seguridad de las Naciones Unidas" (UNDSS, 2012).

En trabajos académicos se debate sobre sobre la "privatización de la paz". Los argumentos a favor y en contra permiten ver con claridad la existencia de necesidades en las operaciones de paz, y que las alternativas para solucionarlas son claramente imperfectas. Pero entonces, ¿podemos plantearnos cuales son los límites de esta imperfección? La exposición de argumentos puede ayudarnos a aproximar una respuesta.

Al respecto, Fitzsimons (2014) plantea que las PMSC deben ser consideradas como "segunda mejor opción como fuerza de mantenimiento de la paz cuando los estados no están dispuestos a

aportar con prontitud suficientes tropas de calidad suficiente para dotar de personal a las operaciones de paz de la ONU". A continuación, se presentan tres argumentos:

En primer lugar, las PMSC tienen una capacidad demostrada para ser utilizadas en las operaciones de paz de la ONU. En segundo lugar, existen salvedades a las críticas de los opositores a las PMSC que hacen que sea inadmisible descartarlas como segunda mejor fuerza de mantenimiento de la paz. En tercer lugar, existen claros beneficios en el uso de las PMSC, especialmente cuando los Estados no están dispuestos a aportar con prontitud suficientes tropas de calidad suficiente para dotar de personal a las operaciones de paz de la ONU.

Plantea también la superposición de tareas desarrolladas por tropas de la ONU y la PMSC, tales como el despliegue de Dyncorp en Kosovo, el apoyo logístico proporcionados por Defence System Limited en Timor Oriental, la contratación de Kroll Associates para la provisión de inteligencia en Angola, entre otros casos que contribuyen a entender que, según ella, las PMSC suman al éxito de las Operaciones de Paz.

Se defiende su participación en Operaciones de Paz argumentando en **primer lugar**, que las empresas militares privadas pueden ayudar a compensar las deficiencias cualitativas en las operaciones de paz de la ONU, ya que están mejor organizadas, entrenadas y equipadas que las fuerzas de paz de la ONU. La práctica de las Naciones Unidas en las operaciones de paz multinacionales se enfrenta a dificultades, como la falta de equipo común, sistemas de comunicación incompatibles, experiencias operativas y doctrinas diversas, y diferentes idiomas.

El **segundo beneficio** es que las empresas militares privadas pueden ayudar a compensar las respuestas tardías a las crisis, ya que pueden desplegarse con mayor rapidez que las fuerzas de paz de la ONU. Esta ha enfatizado repetidamente la importancia del despliegue rápido para frenar eficazmente los conflictos, reducir la escalada de las crisis y prevenir atrocidades masivas. Sin embargo, persisten tasas de despliegue lentas, y las fuerzas de paz de la ONU tardan entre tres meses y un año en desplegarse. En comparación, la EO inició operaciones en Angola y Sierra Leona al mes de su contratación (Spearin). La empresa militar privada afirma que podría haber enviado personal a Ruanda en 14 días, al que se unirían 1500 refuerzos en semanas (Bures). De igual manera, se afirma que las empresas militares privadas podrían desplegar personal para apoyar la operación de paz de la ONU en el Congo en un plazo de 30 a 90 días.

El **tercer beneficio** planteado es que las PMSC son más rentables. La comparación de los costos de la operación de paz de la EO en Sierra Leona con los de la ONU resulta ilustrativa. Esto fue explicado "ut supra". En este trabajo detallan los costos mensuales de esta PMSC que fueron de 1,19 millones de dólares estadounidenses, mientras que los de la ONU fueron de 19,4 millones de dólares estadounidenses. Los costos por personal de la EO fueron de 71.429 dólares estadounidenses, mientras que los de la ONU fueron de 108.756 dólares estadounidenses. Además, la operación de la ONU fue más larga, de mayor envergadura y menos efectiva. La operación de la ONU duró 74 meses, mientras que la de la EO duró menos de 24 meses. A pesar de desplegar 11.797 efectivos de mantenimiento de la paz, la operación de la ONU no cumplió con su mandato de desarmar, desmovilizar y reintegrar a los combatientes. De hecho, hubo varios incidentes en los que efectivos de mantenimiento de la paz de la ONU fueron desarmados. Por el contrario, el EO desplegó solo 350 efectivos. Recuperaron eficazmente el control de zonas estratégicas y debilitaron la posición militar del Frente Revolucionario Unido hasta tal punto que la facción rebelde se vio obligada a firmar un acuerdo de paz con el gobierno. En resumen, existen claros beneficios en el uso de las PMC, en particular cuando los Estados no están dispuestos a aportar con prontitud suficientes tropas de calidad para dotar de personal a las operaciones de paz de la ONU (Fitzsimons, 2014).

Otro enfoque presenta un rol complementario de las PMSC a las tropas de la ONU, sin emplearlas como *"peacekeepers"* de primera línea (Østensen). Plantea, **en principio,** su empleo en misiones de seguridad, así como otros servicios especializados como asesoramiento, entrenamiento, desminado, logística, etc. En **segunda instancia** deja claro que, a pesar que ya se plantea su empleo para suplir la inacción de los Estados Miembros, no se aprecia probable su empleo en operaciones de magnitud. Su composición diversa limita severamente un empleo de esas características. En **tercera instancia** se verifica que, en las operaciones de paz, los contratos, muchas veces, no pasan por la gestión de la ONU. Estos contratos pueden ser gestionados directamente por Estados Miembros o terceros.

El empleo extenso de la PMSC en numerosas misiones en el África en el ámbito de la ONU se comprueba en UNICEF, el Programa Mundial de Alimentos, ACNUR (Alto Comisionado de las Naciones Unidas para los Refugiados), (UNDP) Naciones Unidas para el Desarrollo, entre otros, lo cual demuestra la necesidad de atender tareas que no es posible realizar con medios de la ONU o de los Estados miembros.

Un caso paradigmático ya mencionado es el de los sucesivos fracasos de la ONU y de la comunidad internacional en su

CV

GD (R) CARLOS PÉREZ AQUINO

General de División (R) del Ejército Argentino. Actualmente de desarrolla en la actividad académica como profesor y en el asesoramiento en materia de Defensa y Manejo de Crisis. Se desempeñó cuatro años como comandante operacional de las FFAA, como Jefe de Estado Mayor en la Fuerza de Paz "Cruz del Sur", y en las misiones de paz UNCIFYP (Chipre) y MINUSTAH (Haití).

conjunto en **Haití**. Los despliegues de la ONU fueron ONUVEH – Misión de Observadores de la ONU para verificar elecciones en Haití (1990–1991),MINUHA – Misión de la ONU en Haití (1993–1996), MINUH – Misión de la ONU en Haití (1996–2000), MIPONUH – Misión de la Policía Civil de la ONU en Haití (1997–2000), MICAH – Misión Internacional Civil de Apoyo en Haití (2000–2001), MINUSTAH – Misión de Estabilización de la ONU en Haití (2004–2017), la más extensa, reemplazada por MINUJUSTH – Misión de Apoyo a la Justicia en Haití (2017–2019), que sustituyó a MINUSTAH con un enfoque en instituciones judiciales y derechos humanos y la BINUH – Oficina Integrada de la ONU en Haití (2019–presente). Todo este esfuerzo de la ONU no logró solucionar la situación de caos permanente de este país. Se obtuvieron éxitos operacionales que debían haber sido acompañados por un apoyo de nivel estratégico de la comunidad internacional para reconstruir el tejido social y la estructura administrativa imprescindible para funcionar como estado nación, pero nada de eso pasó.

Hoy Kenia lidera la Misión Multinacional de Apoyo a la Seguridad (MSS) en Haití, autorizada por el Consejo de Seguridad de la ONU, para ayudar a la Policía Nacional de Haití (PNH) a combatir la violencia de pandillas. La misión, si bien no es una operación de la ONU, ha recibido apoyo de diversos países y organizaciones regionales. Si bien inicialmente estaba prevista para 2500 efectivos, **la misión ha enfrentado dificultades para asegurar la contribución completa de policías y aún no ha logrado resultados significativos** en la lucha contra la inseguridad generalizada.

Ante esa imposibilidad de ordenar el país el gobierno de Haití recurrió a Vectus Global, cuyo propietario el ya mencionado Erik Prince quien está reforzando la presencia de su empresa de seguridad privada en Haití, desplegando a cientos de combatientes de Estados Unidos, Europa y El Salvador para combatir a las pandillas que controlan gran parte del país (Callanan & Yee, 2025). "Vectus Global, de Prince, activa a*llí desde marzo 2025, afirma estar trabajando bajo un acuerdo de 10 años con el gobierno haitiano, que incluye un rol en la recaudación de impuestos. Esta medida, que incluye el uso de francotiradores, helicópteros y drones, se produce después de que las pandillas derrocaran al gobierno en febrero, provocando el caos continuo en Puerto Príncipe (Associated Press, 2025).*

Indudablemente la falta de compromiso de la comunidad internacional en la resolución de conflictos impone la necesidad de apelar a estos recursos en los roles más diversos. La pregunta: si bien hoy las PMSC cubren roles secundarios ¿es posible que, ante la falta de aporte de los

No es una anomalía: es el signo de un orden en el que la tercerización se confunde con la gobernanza. El outsourcing, entonces, es la confesión de que la ONU no funciona, de que las ONG son incómodas y de que lo urgente requiere algo más parecido a un "proyecto" que a un tratado.

estados miembros de la ONU, estas organizaciones asuman las tareas centrales de las fuerzas de paz? Indudablemente el caso de Haití es paradigmático. Habrá que seguir de cerca los resultados, pero demostraría una alternativa poco convencional que deberá probar ser efectiva. Hay voces que hablan de eficacia y otras de riesgos severos en la violación de DDHH, falta de regulación normativa sólida y de rendición de cuentas.

La ONU publica en su página oficial *la resolución del CSONU de octubre de 2025 acaba de autorizar el establecimiento de una nueva fuerza internacional en Haití. No se trata de una misión de paz al como las que desplegara previamente, sino de una fuerza de represión para combatir a las bandas. Una medida considerada como necesaria pero insuficiente, ya que no atiende cuestiones como la ayuda humanitaria, el desarrollo y la reforma de la gobernanza del país. Aún no está claro qué países la integrarán, ni quienes facilitarán su financiamiento".* La misma ONU plantea su escepticismo ante una resolución que enfrentará, seguramente, serios problemas para su implementación.

Otra manifestación de la tercerización es la *Gaza Humanitarian Foundation* (GHF) diseñada en octubre de 2024 para distribuir ayuda humanitaria con la custodia de tropas israelíes y contratistas norteamericanos. En este diseño participó el *Boston Consulting Group* (BCG) que trabajó en el modelado de reconstrucción de posguerra cuantificando la "relocalización" de 500.000 palestinos. En pocas palabras, una expulsión masiva (Merke 2025).

En el artículo referido, Federico Merke señala que: *No es una anomalía: es el signo de un orden en el que la tercerización se confunde con la gobernanza. El outsourcing, entonces, es la confesión de que la ONU no funciona, de que las ONG son incómodas y de que lo urgente requiere algo más parecido a un "proyecto" que a un tratado. Pero el precio es alto. Al delegar funciones humanitarias a una firma privada, se diluyen principios elementales: neutralidad, imparcialidad, independencia. Se refuerza, además, la percepción de que la ayuda ya no es un gesto moral, sino una extensión del poder duro. El escándalo no dice tanto sobre Gaza como sobre nuestro tiempo: uno en el que el humanitarismo puede ser tratado como un "deliverable" y el orden global como un "cliente".*

¿Qué opina la ONU?

La Asamblea General de las Naciones Unidas (AGONU) ha abordado ampliamente el uso y la regulación de las PMSC, en particular en lo que respecta a los derechos humanos y la rendición de cuentas. La Asamblea ha reconocido la creciente dependencia de las PMSC por parte de los Estados y las organizaciones internacionales, incluida la propia ONU, y ha enfatizado la necesidad de una regulación sólida para prevenir los abusos de los derechos humanos y garantizar la rendición de cuentas por las violaciones.

De todos modos, persisten las preocupaciones y desafíos por la potencial violación de los DDHH por parte de estas organizaciones, teniendo en cuenta, en particular, la falta marco legal y rendición de cuentas. Por otra parte, se teme un impacto en la Operaciones de Paz que socave la imparcialidad y eficiencia de dichas operaciones. La privatización de la seguridad afecta el control de la seguridad a que los organismos públicos están sometidos.

Es importante tener en cuenta que, si bien la AGONU se expide sobre sus preocupaciones sobre el empleo de las PMSC y se emite una Directiva, la ONU es una suma de organizaciones reunidas por la Carta y una bandera tornándose difícil determinar una posición consistente respecto a las contrataciones de un recurso sumamente presente en la organización como son las PMSC. Es muy probable que veamos posturas contradictorias, de acuerdo a la organización que examinemos. Se puede decir que la posición de la ONU es multifacética.

A modo de conclusión

Las sociedades occidentales "post-heroicas" (Luttwark, 1996), que pretenden minimizar el riesgo humano, político y económico han favorecido la proliferación de organizaciones de estas

características tanto en los Estados Nación, como en la propia ONU, como hemos visto.

Por lo que debemos asumir que la presencia de la PMSC en casi todos los conflictos es una realidad con la que debemos convivir. Su empleo, muchas veces imprescindible, debe ser regulado y los límites de su empleo deben ser fijados con claridad. En la tercerización, se diluyen principios elementales: neutralidad, imparcialidad, independencia.

Habrá que seguir con atención el accionar y los resultados de la PMSC "Vectus" en Haití. Fuera de la ONU y bajo contrato directo del estado nación, posiblemente nos permita analizar esta herramienta en una situación en que los recursos de la ONU no pudieron solucionar.

Sin dudas la falta de un marco legal sólido y vinculante genera lógicas preocupaciones por la falta de rendición de cuentas, violaciones a los DDHH y su empleo en una "zona gris" plagada de lagunas legales con riesgo de impunidad y la opacidad en las contrataciones. La actividad desarrollada por la ONU y el CICR es sumamente loable, aunque se aprecia de difícil aplicación.

En síntesis, la tercerización de la paz mediante PMSC es una variante en los conflictos modernos. Su empleo puede ofrecer ventajas operacionales, pero implica riesgos jurídicos, éticos y políticos que requieren una regulación más robusta y mecanismos de control efectivos. Es necesario reforzar la supervisión internacional y la transparencia en la contratación para asegurar que su actuación se ajuste a los principios del DIH y los Derechos Humanos. ▮

BIBLIOGRAFÍA

Annan, Kofi (26 de junio, 1998) *"On Intervention"*, discurso dictado en la Fundación Ditchley. (Citado por Lauren Grace Fitzsimons).

-

Baum, Joel A.C; McGahan, Anita (2011). *Outsourcing War: The Co-Evolution of Transactions, Capabilities and Performance in the Private Military Industry*. Rotman School of Management, University of Toronto, 2011

-

Bures, Oldřich. *"Private Military Companies"*, p. 539. (Citado por Lauren Grace Fitzsimons).

-

Callanan, Riley; Yee, Lizzy (2025). *"What we're watching: Haiti turns to foreign fighters, China's economy slumps, protests flare-up in Serbia". GZERO Media.*

-

Comité Internacional de la Cruz Roja (1949) *Convenios de Ginebra de 1949 y Protocolos Adicionales. Artículo 43, "Fuerzas Armadas" y Artículo 51 "Protección de la población civil"*. Ginebra, Suiza.

-

Comité Internacional de la Cruz Roja (2012) *Implementación del Derecho Internacional Humanitario a nivel nacional. Manual. Ginebra, Suiza.*

-

Coto, Dánica (agosto, 2025). "fundador de Blackwater enviará cerca de 200 personas a Haití para sofocar violencia de pandillas. *Associated Press News*. Disponible en: https://apnews.com/article/haiti-violencia-seguridad-pandillas-42062b2581d0413548182e79f0a714c5

-

Fitzsimons, Lauren Grace (2014). *Should Private Military Companies be use in UN Peace Operations? Publicado en e-international relations*. Disponible en: https://www.e-ir.info/2015/11/17/should-private-military-companies-be-used-in-un-peace-operations/

-

Luttwak, Edward N. (1996). "A Post-Heroic Military Policy". *Foreign Affairs*, vol. 75, nº 4, pp. 33-44.

-

Manejo de sistemas de seguridad de la ONU. (2012) *"Security Management Operations Manual Guidelines on the Use of Armed Security Services from Private Security Companies".*

-

Merke, Federico (agosto, 2025). "El experimento humanitario de una consultora corporativa en Gaza que salió mal". *Cenital.com*, disponible en: https://cenital.com/el-experimento-humanitario-de-una-consultora-en-gaza-que-salio-mal/

-

Misión Permanente de Suiza ante las Naciones Unidas (2008). *Documento de Montreux*. Consultado en 2025.

-

Noticias ONU (octubre, 2025). "¿Qué es la nueva fuerza respaldada por la ONU en Haití? Disponible en: https://news.un.org/es/story/2025/10/1540516

-

Østensen, Åse Gilje (2011). *UN Use of Private Military and Security Companies. Practices and Policies*. Chapter: "The United Nations and MNSCs: An overview", pp. 11-18. Geneva Centre for the Democratic Control of Armed Forces.

-

Organización de las Naciones Unidas (1945). *Carta de las Naciones Unidas, Preámbulo.* www.un.org Consultado en 2025.

-

Spearin, Christopher (2022). *"UN peacekeeping and Chinese Private Security Companies: assessing demand factors for China", Defense & Security Analysis, Taylor & Francis Journals*, vol. 38(1). (Citado por Lauren Grace Fitzsimons).

-

Ruiz Arévalo, Javier (2010). "¿Contratistas o mercenarios?" *En Revista Defensa* nº 382. Disponible en: https://www.defensa.com/en-abierto/contratistas-o-mercenarios

-

United States Military Academy Modern War Institute (2019) *Sean McFate on The New Rules of War.* Disponible en: https://mwi.westpoint.edu/mwi-video-sean-mcfate-new-rules-war/

-

Banchereau, Mark (6 de junio, 2025). *"Wagner Group leaving Mali after heavy losses but Russia's Africa Corps to remain". Associated Press News.* Disponible en: Russia's Africa Corps to remain in Mali despite Wagner mercenaries exit | AP News

REPOSITORIO DIGITAL INSTITUCIONAL

Para acceder a la producción científica de docentes, investigadores, alumnos, egresados y colaboradores que integran las comunidades repositorio institucional de las Fuerzas Armadas (en español e inglés), ingrese en: **http//www.cefadigital.edu.ar**

NORMAS DE PRESENTACIÓN DE COLABORACIONES PARA LA REVISTA *VISIÓN CONJUNTA*

Para la selección y análisis de los trabajos a considerar para su publicación:

> Comité de Referato: Su función es garantizar la calidad de los trabajos presentados.
> Comité Editorial: Su función es resguardar la línea editorial institucional, la pertinencia y utilidad de su publicación en el ámbito educativo de las tres Sedes Educativas que integran la FMC.

La Secretaría de Extensión y Comunicación seleccionará los artículos propuestos por las instancias evaluadoras previas.

El material publicado en formato analógico y/o digital, queda amparado por la Ley de Propiedad Intelectual Nro. 11723. Todos los derechos están reservados y los contenidos son de propiedad de la FMC y Estado Mayor Conjunto de las Fuerzas Armadas, sin perjuicio de los derechos morales de los autores. Las citas y uso de imágenes obrantes en el dominio privado, deben ser debidamente autorizadas, y en todos los casos con mención completa de la fuente.

Estructura del artículo

> Título
> Nombre y apellido del autor, acompañado por un breve currículo de, aproximadamente, 700 caracteres.
> Resumen: 200 a 300 palabras en idioma español.
> Palabras clave: máximo 4.

Requerimientos

> Los artículos podrán ser de opinión, resultados de investigación, traducciones y recensiones, comentarios u otras fuentes de consulta.
> Tendrán una extensión máxima de 35.000 caracteres con espacio, en página A4, interlineado sencillo.
> Numeración en cada página.
> Artículo realizado en Word, letra arial, tamaño de fuente 11 para todo el texto, en una sola columna.
> Cursivas (itálica o bastardilla) se utilizarán sólo para palabras de otro idioma. Las citas textuales deben ser realizadas entre comillas o con sangría, de modo de poder diferenciar lo expuesto por autor del texto respecto del citado, con mención completa de la fuente a pie de página.
> Las abreviaturas, siglas o acrónimos, deben ser aclararlas en oportunidad de su primer uso.
> Inclusión de gráficos, mapas o material histórico se permitirán solo dos (2) por artículo y se citará la fuente correspondiente. Los gráficos deben estar en idioma español.
> Las citas y notas se incluirán al pie de página.

Toda la correspondencia relacionada con publicaciones de la Editorial Universitaria de la Facultad Militar Conjunta (FMC), será dirigida a la Secretaría de Extensión y Comunicación:

Av. Luis María Campos 480, PB , Edificio Videla, C1426BOP, Ciudad Autónoma de Buenos Aires

publicaciones@fmc.undef.edu.ar

FMC

Facultad Militar Conjunta

MISIÓN

Formar y capacitar profesionales nacionales y extranjeros, militares y civiles, con un alto nivel académico y comprometidos con la formación continua, a través de carreras de grado, carreras y cursos de posgrado en el campo de la Estrategia Operacional, de la Estrategia Militar, de la Producción y Gestión de la Información/Inteligencia en el Nivel Táctico, Operacional y Estratégico Militar, de la Ciberdefensa y Operaciones Militares Cibernéticas, y de todas las ramas del saber relacionadas con ellas, que permitan mantener el ritmo de evolución de los conocimientos científico-tecnológicos y desarrollar actividades de investigación y extensión.