



ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TÍTULO: La Influencia de las Redes Sociales, empleo y usos en las Operaciones de Información dentro del Nivel Operacional.

AUTOR: MY PABLO MAXIMILIANO AVALOS (EA)

TUTOR: TC ROBERTO CARI

AÑO: 2025

“Las ideas expuestas sólo representan la postura personal del autor, por lo que son de su absoluta responsabilidad, no reflejando en consecuencia la opinión de la Escuela Superior de Guerra Conjunta de la Facultad Militar Conjunta de la Universidad de la Defensa Nacional”

RESUMEN

En el contexto de los conflictos armados contemporáneos, las Operaciones de Información (OI) han adquirido un rol protagónico dentro del planeamiento operacional conjunto, especialmente en escenarios marcados por la presencia de los medios digitales. Entre los instrumentos de las OI, las redes sociales se han convertido en herramientas decisivas para modelar percepciones, influir en decisiones estratégicas, erosionar la voluntad del adversario y fortalecer la cohesión propia. Esta investigación aborda el empleo y la influencia de las redes sociales dentro del nivel operacional, con el propósito de analizar en qué medida estas plataformas pueden ser utilizadas como capacidades militares integradas en apoyo a las operaciones decisivas de una campaña.

Para ello, se examinarán doctrinas extranjeras y nacionales que conceptualizan el ambiente de la información, así como experiencias recientes en el uso de redes sociales particularmente en el caso de la guerra ruso-ucraniana para operaciones de propaganda, desinformación y movilización internacional (2014 - 2024). El estudio explorará los modos de empleo, efectos logrados y lecciones aprendidas desde la perspectiva del diseño operacional. Asimismo, se identificarán brechas doctrinarias en el marco normativo argentino, proponiendo líneas de acción para la incorporación formal de estas capacidades a la doctrina militar conjunta. Se considerarán, además, implicancias para la educación militar, el equipamiento y las coordinaciones cívico-militares necesarias para escenarios futuros.

El objetivo general es investigar el grado de contribución que puede ofrecer el empleo sistemático y planificado de las redes sociales en las OI dentro del nivel operacional. La hipótesis sostiene que su incorporación deliberada permite generar condiciones favorables en una campaña militar, tal como lo demuestran los resultados del conflicto ruso-ucraniano dentro del periodo seleccionado y que su integración en la doctrina nacional resulta imprescindible para enfrentar los desafíos de los entornos actuales y futuros.

PALABRAS CLAVE

Operaciones de Información – Redes Sociales – Influencia – Efectos – Nivel Operacional.

TABLA DE CONTENIDOS

Resumen	i
Palabras clave	i
Tabla de contenidos	ii
Lista de siglas y acrónimos.....	iii
Tabla de gráficos, cuadros e ilustraciones.....	iv
Introducción.....	1
Capítulo I - Las Operaciones de Información y el empleo de Redes Sociales.	5
1.1 Marco doctrinario internacional y regional	5
1.2 Ambientes de la información: dimensiones física, informativa y cognitiva	9
1.3. Redes sociales como herramienta operacional: características y capacidades	11
1.4. Aplicabilidad de las redes sociales en los niveles de la guerra.....	12
1.5. Riesgos, limitaciones y desafíos asociados	13
Capítulo II - La guerra Ruso-Ucraniana (2014-2024): operaciones de información y empleo de redes sociales en el nivel operacional.....	15
2.1. Contexto geopolítico y doctrinario previo al conflicto (2014 – 2024).....	15
2.2. Estrategia rusa de información y guerra cognitiva.....	16
2.3. Respuesta ucranianas: defensa informacional y guerra narrativa	18
2.4. Plataformas empleadas, actores y mecanismos de acción informacional	21
2.5. Efectos y comparación desde la perspectiva operacional.....	22
2.6. Lecciones aprendidas del caso analizado.	25
2.7. Aplicabilidad al ámbito de la defensa argentina.	26
Capítulo III - Implicancias y propuestas para el Instrumento Militar Argentino.....	27
3.1. Integración de las redes sociales en las Operaciones de Información conjuntas	27
3.2. Desafíos para la planificación y conducción conjunta	29
3.3. Propuesta de modelo operativo informacional para la defensa argentina	30
3.4. Evaluación prospectiva y requerimientos doctrinarios.....	32
Conclusiones generales.....	34
Bibliografía.....	36
Anexos	39

LISTA DE SIGLAS Y ACRÓNIMOS

Sigla / Acrónimo	Significado
OI	Operaciones de Información
RAND	Research and Development (Investigación y Desarrollo)
GCHQ	Government Communications Headquarters (Agencia de Inteligencia de Señales del Reino Unido)
Netwar	Guerra en red
NATO	North Atlantic Treaty Organization (Organización del Tratado del Atlántico Norte)
Strat Com COE	Strategic Communications Centre of Excellence (Centro de Excelencia en Comunicaciones Estratégicas)
JCOIE	Joint Concept for Operating in the Information Environment (Concepto Conjunto para Operar en el Entorno de Información)
JIOWC	Joint Information Operation Warfare Center (Centro de Operaciones de Información de Guerra Conjunta)
CDCiber	Centro de Defensa Cibernética
COTER	Comando de Operações Terrestres
IRC	Information Related Capabilities (Capacidades relacionadas con la información)
DFRLab	Digital Forensic Research Laboratory (Laboratorio de Investigación Forense Digital)
OODA	Observar, Orientar, Decidir y Actuar
OSINT	Open Source Intelligence (Inteligencia de Fuentes Abiertas)
CCOINF	Comando Conjunto de Operaciones Informacionales
FUCAME	Fuente, Unidad, Contexto, Audiencia, Medio y Efecto

TABLA DE GRÁFICOS, CUADROS E ILUSTRACIONES

Nº	Título	Tipo	Capítulo
Figura 1	Modelo operacional RAND Corporation para el uso de redes sociales.	Diagrama de flujo	I
Figura 2	Dimensiones del ambiente de la información.	Gráfico	I
Figura 3	Aplicabilidad de las redes sociales en los niveles de la guerra	Cuadro sinóptico	I
Figura 4	Estrategia informacional ucraniana (2014 – 2024).	Línea de Tiempo	II
Figura 5	Plataformas empleadas, actores y mecanismos de acción informacional	Cuadro	II
Figura 6	Zonas clave y operaciones informacionales.	Gráfico	II
Figura 7	Comparación desde la perspectiva operacional.	Cuadro	II
Figura 8	Modelo Ciclo Operativo Informacional	Gráfico circular	III
Figura 9	FUCAME de la plataforma Telegram.	Cuadro comparativo	A 1
Figura 10	FUCAME de la plataforma You Tube	Cuadro comparativo	A 1
Figura 11	Principales redes sociales empleadas en el dominio informacional	Cuadro sinóptico	A 2

INTRODUCCIÓN

En el marco de los conflictos armados contemporáneos, el dominio de la información dejó de ser un recurso eventual para convertirse en un dominio decisivo de la guerra adquiriendo una centralidad sin precedentes. En este escenario, el empleo de las redes sociales en las Operaciones de Información¹ (OI) constituye una herramienta fundamental para influir en la voluntad, percepción y comportamiento de actores relevantes, tanto en tiempos de paz como de conflicto. En particular, Moresi et al. (2023) sintetizan el cambio al afirmar: “la guerra actual demanda respuestas conjuntas, integradas y multi-agenciales de toda la sociedad, donde la información fluye libremente y los niveles de la guerra tienden a subsumirse” (p. 13).²

El presente trabajo parte de ese trasfondo para examinar la influencia de las redes sociales como herramienta de las OI en el nivel operacional y su proyección sobre el instrumento militar argentino, cuidando que el análisis no derive en tecnicismos sino en criterios útiles para el planeamiento conjunto.

De esta manera la pregunta de investigación se formula de modo sencillo y a la vez exigente: ¿en qué medida las redes sociales influyen en las OI del nivel operacional y cómo deberían ser incorporadas doctrinariamente el instrumento militar argentino? La hipótesis sostiene que estas plataformas constituyen un vector decisivo de la maniobra informativa y que su integración formal es indispensable para la Defensa Nacional.

Para ello dos advertencias conceptuales nos permiten delimitar el problema. “La guerra de la información debe ser entendida como un instrumento estratégico para controlar percepciones y desestabilizar sociedades adversarias” (Panarin, 2011, p. 43).³ Delimitada por

¹ Las Operaciones de Información son Acciones que implican el uso y manejo de la tecnología de la información y las comunicaciones, dentro de las dimensiones físicas, de información y cognitivas del ambiente de la información, en concierto con otras líneas de operaciones, para acceder, modificar, interrumpir, alterar o destruir la toma de decisiones del adversario, protegiendo, al mismo tiempo, las propias, según el Glosario de Términos de empleo militar para la Acción Militar Conjunta (2023).

² El ambiente informacional comprende tres dimensiones interdependientes: física (infraestructura y sistemas), informativa (contenido y flujos) y cognitiva (percepciones, emociones, moral).

³ Panarin, académico ruso, enlaza propaganda, geopolítica y control social; su enfoque resalta el empleo estratégico de medios y redes para efectos políticos.

la siguiente perspectiva de Rid (2020) “la desinformación es eficaz no por la mentira en sí misma, sino por su capacidad de erosionar la confianza pública en la verdad” (p. 92).⁴

Con este andamiaje, el objetivo general es analizar la influencia de las redes sociales como herramienta de las OI en el nivel operacional y proponer lineamientos para su incorporación doctrinaria. De él derivan propósitos específicos que orientan el hilo argumental: contrastar doctrinas de referencia, caracterizar el ambiente informacional, evaluar el caso ruso-ucraniano e identificar vacíos y capacidades necesarias en Argentina.

El marco teórico del trabajo de investigación integra tradición estratégica y producción reciente. Encontrándonos necesariamente con Sun Tzu quien nos sintetiza la siguiente afirmación duradera: “conocer y manipular la mente del adversario equivale a vencer sin combatir” (Cleary, 2003, p. 10).⁵ Podemos observar a inicios de este siglo Arquilla y Ronfeldt, desde la RAND Corporation (2001) anticipaban que “quienes dominen la información y la red dominarán el conflicto” (p. 25).⁶ Advirtiendo Thornton (2015) años después, que “los conflictos híbridos obligan a integrar sin fisuras lo militar y lo informacional para evitar desventajas estructurales” (p. 214). Para luego Omand (2020), exdirector del GCHQ, traducirnos todas estas afirmaciones diciendo que: “la confianza se ha convertido en la moneda estratégica del siglo XXI, más valiosa incluso que la superioridad tecnológica” (p. 61).⁷

Esta convergencia teórica respalda una premisa operativa: en el nivel operacional, las redes sociales pueden acelerar la masa de efectos informacionales sobre centros de gravedad cognitivos propios y ajenos, siempre que exista conducción, sincronización y límites legales y éticos explícitos.

En el plano doctrinario podemos confirmar y ordenar los siguientes hallazgos. Inicialmente la doctrina de Estados Unidos con su manual JP 3-13 (2012) define: “Las operaciones de información son el empleo integrado, durante las operaciones militares, de

⁴ Rid estudia campañas soviéticas y contemporáneas; centra el problema en la confianza social como objetivo y efecto de la desinformación.

⁵ Lectura contemporánea: la “mente del adversario” refiere hoy a audiencias segmentadas y mediadas por plataformas, no solo a comandantes enemigos.

⁶ RAND Corporation: centro de estudios estratégico; ‘netwar’ (guerra en red) como modelo para actores distribuidos que emplean redes para coordinar e influir.

⁷ GCHQ: Government Communications Headquarters, agencia de inteligencia de señales del Reino Unido; énfasis en resiliencia y verificación.

capacidades relacionadas con la información para influir, entorpecer, corromper o usurpar la toma de decisiones del adversario.” (p. I-2)⁸

En el marco regional, Brasil conceptualiza las OI como “esfuerzo permanente del Estado Mayor, integrándola con guerra electrónica, ciberdefensa, operaciones psicológicas, comunicación social y asuntos civiles” (Exército Brasileiro, 2020, p. 18).⁹ Asimismo Chile, en la DNC 3-7 (2014), las entiende como funciones destinadas a crear efectos en voluntad, comprensión y capacidades de audiencias hostiles, neutrales o favorables, en el marco de operaciones conjuntas y de Estado.¹⁰

En contraste, la Argentina carece de una doctrina conjunta consolidada que traduzca estas intuiciones en procesos, estructuras y capacidades permanentes; ello alimenta asimetrías frente a actores que ya integraron la dimensión informacional en su planeamiento.

El estudio de caso ruso-ucraniano (2014–2024) nos ofrece un laboratorio empírico. Por su parte Rusia combinó un control narrativo centralizado, operaciones cibernéticas y presión informativa a través de plataformas y medios estatales; en respuesta, Ucrania articuló una defensa informacional descentralizada con un fuerte rol de la sociedad civil y de los apoyos internacionales. Encontrándonos así a plataformas digitales como Telegram, X/Twitter y Tik Tok actuando como vectores para propaganda, movilización y diplomacia pública. Explotando sus facilidades tales como la rapidez y la segmentación para ampliar los efectos informacionales más allá del área de combate, impactando en la moral de combate y la legitimidad externa de los bandos.¹¹

El NATO Strat Com COE (2020), con sede en Riga, sistematiza estas dinámicas y señala que las operaciones de influencia en redes sociales se distinguen por “la combinación de velocidad, segmentación y masividad, transformando la percepción de las audiencias en un

⁸ Capacidades JP 3-13: operaciones psicológicas, guerra electrónica, operaciones cibernéticas, seguridad de operaciones y engaño militar (lista no exhaustiva).

⁹ El Manual de Operações de Informação (Ejército de Brasil) enfatiza continuidad (paz-guerra) y protección de la voluntad propia como fin explícito.

¹⁰ DNC 3-7: Doctrina de Nivel Conjunto; especifica planificación, coordinación y evaluación como responsabilidades del EMCO chileno.

¹¹ El carácter 'trans-teatral' de los efectos informacionales explica por qué audiencias internacionales pueden transformarse en palancas logísticas y diplomáticas.

objetivo militar de alto valor”.¹² Ignorar este fenómeno no solo ampliaría vulnerabilidades operacionales y estratégicas, sino que también priva al país de un recurso que, bien empleado, puede convertirse en un multiplicador operacional.

La justificación de esta investigación, por lo tanto, es doble: anticipar riesgos en el dominio informacional y proponer criterios para su empleo responsable. El objetivo no es tecnificar la conducción, sino dotarla de un marco que armonice eficacia operacional con legitimidad y control civil.

Metodológicamente, se adoptó un enfoque cualitativo que combina revisión doctrinaria comparada (EE. UU., Brasil, Chile) y bibliografía especializada y luego el análisis de la inclusión de redes sociales como capacidades informacionales en el primer capítulo. Posteriormente el análisis del caso mencionado en el segundo capítulo, reconstruyendo los efectos del uso de redes sociales desde una perspectiva operacional. Llegando al desarrollo del tercer capítulo donde se derivará recomendaciones para capacidades, formación y procesos de planeamiento conjunto en el instrumento militar argentino.

Finalmente se exponen las conclusiones donde se validará la hipótesis que, en síntesis, se comprueba que incorporar las redes sociales al diseño operacional ya no es una opción eventual, sino una condición para competir con sentido en el ambiente informacional contemporáneo.¹³

¹² NATO Strategic Communications Centre of Excellence (Riga): centro de excelencia de la OTAN dedicado a investigación y doctrina sobre comunicación estratégica.

¹³ Consideraciones legales y éticas: respeto a DD. HH., protección de datos, proporcionalidad y transparencia en la comunicación institucional.

CAPÍTULO I

LAS OPERACIONES DE INFORMACIÓN Y EL EMPLEO DE REDES SOCIALES

1.1 Marco doctrinario internacional y regional.

El creciente protagonismo del entorno informacional en los conflictos del siglo XXI ha provocado una profunda transformación en la manera en que los Estados diseñan y conducen sus campañas militares. El entorno digital, en especial las redes sociales, se ha constituido en un dominio de confrontación directa, no solo por su capacidad de diseminación masiva de narrativas, sino por su potencial para modificar el comportamiento de actores estratégicos y públicos civiles. Por lo cual el estudio comparado de las OI permite observar una tendencia convergente: las mismas dejan de ser un apoyo eventual o esporádico y se integran como una capacidad conjunta, con conducción, evaluación y recursos permanentes. Es así que la diferencia entre países radica menos en las definiciones y más en el grado de institucionalización, coordinación interagencial y evaluación de efectos.

Es por ello que este capítulo examina los marcos doctrinarios internacionales y regionales sobre OI, describe las dimensiones del ambiente informacional, analiza las redes sociales como herramientas operacionales, su aplicabilidad y los riesgos inherentes a su uso militar.

1.1.1 Estados Unidos.

Las Fuerzas Armadas de los Estados Unidos fueron las primeras en definir un marco doctrinario sólido sobre OI. Definiendo el U.S. Department of Defense (Departamento de Defensa de los Estados Unidos), en su doctrina conjunta JP 3-13 (1998), que las OI constituyen “el empleo integrado, durante las operaciones militares, de capacidades relacionadas con la información [...] para influir, interrumpir, corromper o usurpar la toma de decisiones de adversarios y adversarios potenciales, protegiendo simultáneamente las propias” (p. I-2). Esta

definición dio origen a una visión sistémica en la que la información pasó a ocupar un lugar equivalente a otros instrumentos del poder militar.¹⁴

Esta conceptualización ha seguido evolucionando a través de los años y de las nuevas experiencias de guerra hacia un abordaje con un mayor énfasis en el dominio cognitivo, afirmando el mencionado Departamento que, las OI deben coordinarse estrechamente con el esfuerzo operacional, buscando alcanzar efectos sinérgicos mediante acciones no cinéticas que complementen las maniobras físicas. (U.S. Department of Defense, 2014)

En 2017, la doctrina conjunta estadounidense dio un paso aún mayor al reconocer la información como séptima función militar, otorgándole así un estatus semejante al de maniobra o logística (Joint Chiefs of Staff).¹⁵

Luego en 2018, el mismo organismo en su documento Joint Concept for Operating in the Information Environment (JCOIE) eleva esta conceptualización al exigir su integración multidominio y a una medición más rigurosa de sus efectos. Siendo las experiencias en Irak y Afganistán donde quedara demostrado que la superioridad cinética no se traduce automáticamente en superioridad estratégica si no se sincroniza con narrativas, percepciones y legitimidad locales e internacionales. Por lo cual, en la actualidad en apoyo a la ejecución, el Joint Information Operations Warfare Center (JIOWC) actúa como integrador y asesor del Estado Mayor Conjunto, articulando doctrina, capacitación y lecciones aprendidas.

En su constante evolución esta definición fue ampliada en el documento Information in Joint Operations (2022), que incorpora el dominio cognitivo como espacio de combate decisivo, haciendo hincapié en el rol de las redes sociales como herramientas de disuasión y manipulación narrativa en tiempo real.

Asimismo luego de analizar su doctrina y para hacer una analogía de estudios privados de fines del Siglo XX, nos referiremos a John Arquilla y David Ronfeldt que ya en 1996 nos advertían en su obra de The Advent of the Netwar sobre el surgimiento de una nueva forma de

¹⁴ La noción de Information Related Capabilities (IRC) en EE. UU. incluye capacidades psicológicas, de ciberdefensa, guerra electrónica, seguridad de la información y operaciones de influencia, todas integradas en un mismo proceso.

¹⁵ La inclusión de la “información” como séptima función conjunta representó un cambio cultural: ya no se trataba de un recurso auxiliar, sino de una capacidad estructural dentro del arte operacional.

confrontación: la netwar (guerra entre redes), ideológicas o criminales, donde el objetivo no es destruir al adversario, sino desorganizarlo psicológica y narrativamente.

Es así que podemos observar como corporaciones de estudios internacionales y estratégicos han avanzado en el desarrollo de esta temática, teniendo el caso en el informe The Role of Social Medium Military Operations donde se han desarrollado modelos operacionales que integran plataformas como Telegram, X (Twitter) y Tik Tok a campañas de contra información, vigilancia social, control de opinión pública y alteración de percepciones en el nivel táctico y operacional. (Rand Corporation, 2020).

Esa visión fue confirmada por el informe Handbook for Tactical Operations in the Information Environment, donde RAND propone fases operacionales reconocimiento, contrainformación, manipulación discursiva y explotación psicológica aplicables a campañas digitales (Schwille et al., 2021).

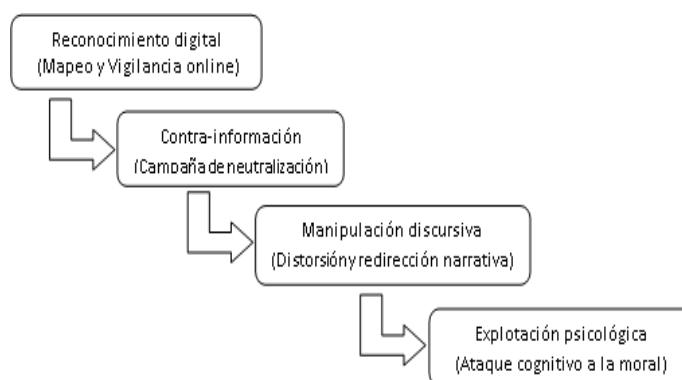


Figura 1 – Modelo operacional RAND Corporation para el uso de redes sociales.

1.1.2 Brasil y Chile.

En el plano regional, Brasil y Chile ofrecen perspectivas complementarias. Mientras que el Manual de Operações de Informação (2020) concibe las OI como un esfuerzo militar integral, centrado en la coordinación de las Capacidades Relacionadas con la Información (CRI), Chile opta por un enfoque más político-estratégico, donde la legitimidad frente a la sociedad es el elemento rector.

En el caso de Brasil, el Ministerio de Defensa aborda el tema estudiado a través de una aproximación sistémica en el Manual de Operações de Informação, conceptualizando a las OI como un esfuerzo permanente bajo conducción del Comando de Operações Terrestres (COTER). Definiendo a las OI como “la coordinación integrada de las CRI en apoyo a otras

operaciones o como parte del esfuerzo principal” (Ministério da Defesa, 2020, p. 15), con énfasis en operaciones psicológicas, ciberdefensa y guerra electrónica.

En ese marco, las redes sociales son reconocidas como herramientas clave para ejercer persuasión, reforzar la narrativa estratégica y desacreditar versiones hostiles en entornos complejos. Sosteniendo algunos autores que, su país ha dado pasos firmes en la integración de capacidades de ciberdefensa con operaciones cognitivas en redes sociales durante ejercicios y operaciones reales.

Como señalan Coelho y Almeida (2019), este modelo refleja la intención de consolidar un sistema de influencia digital dentro del arte operacional brasileño.¹⁶ Es así que la creación y expansión del Centro de Defensa Cibernética (CDCiber) refuerza esta dimensión técnica. Asimismo Ejercitaciones realizadas como el ejercicio Amazon Log 2017 han logrado mostrar coordinación multinacional en el entorno amazónico, donde la logística, la comunicación estratégica y la presencia digital condicionan la percepción regional.

Chile, en cambio, establece en su Doctrina de Nivel Conjunto (*DNC*) 3-7 Operaciones de Información que, la finalidad de estas es “integrar actividades de información para generar efectos en la voluntad, comprensión y capacidades del adversario” (Ministerio de Defensa de Chile, 2014, p. 8), con énfasis en la coordinación conjunta interagencial.

Investigadores como Soto (2017) muestran que las Fuerzas Armadas chilenas priorizaron el uso de redes sociales en situaciones de conflictividad interna, con un objetivo de contención social y legitimación institucional.¹⁷

1.1.3 Argentina.

Si bien Argentina reconoce el ambiente de la información en su Directiva de Planeamiento de la Defensa Nacional (2024), aún no existe una doctrina conjunta consolidada aprobada y específica sobre Operaciones de Información Conjunta, revelando así un estado incipiente dentro de su doctrina. Por lo cual el Glosario de términos de empleo militar para la

¹⁶ La doctrina brasileña interpreta a las OI como parte de la maniobra militar clásica, lo que contrasta con enfoques como el estadounidense, donde se privilegia la articulación civil-militar en escenarios conjuntos.

¹⁷ La doctrina chilena subraya la relación entre OI y democracia, estableciendo que la validez de la acción militar depende de la aceptación social y el control político civil].

acción militar conjunta (2023) solamente nos introduce hacia definiciones básicas, sin establecer procedimientos claros que traduzcan ese reconocimiento en estructuras y procesos.

En términos académicos, se destacan los aportes de Moresi et al. (2023), quienes establecen que las OI en Argentina deben ser entendidas como la “integración permanente y coordinada de capacidades informacionales, orientadas a producir efectos en la dimensión informativa y a otorgar ventajas al comandante del teatro de operaciones” (p. 158).

Este vacío doctrinario encuentra su antecedente histórico más evidente en la Guerra de Malvinas, donde el Informe Rattenbach advierte sobre “graves deficiencias en la Acción Psicológica: falta de organización centralizada, escasez de especialistas y ausencia de control sobre la información disponible” (Bayer, 2000, p. 212). Dichas falencias muestran que la carencia doctrinaria no es un fenómeno reciente, sino estructural.^{18 19}

Es así que investigaciones recientes de expertos evidencian estos vacíos doctrinarios y organizacionales que limitan la capacidad del instrumento militar para operar en campañas informacionales. Sosteniendo María Laura González (2016) que la ausencia de doctrina específica debilita la proyección de poder informacional del Estado argentino y advirtiendo Roberto Fernández (2018) en su libro Ciberseguridad y Redes Sociales en el Contexto Militar Argentino, de la necesidad de articular una visión estratégica nacional que contemple capacidades interagenciales y defensa narrativa frente a amenazas híbridas.

1.2 Ambientes de la información: dimensiones física, informativa y cognitiva.

El ambiente de la información es definido como “la totalidad de individuos, organizaciones y sistemas que recopilan, procesan, divulgan o actúan sobre la información” (U.S. D. o., Joint Publication 3 - 13 Information Operations, 2012, p. I-3). El cual puede dividirse en tres dimensiones —física, informativa y cognitiva— estas no solo deben entenderse como compartimentos aislados, sino como niveles interdependientes que

¹⁸ La doctrina argentina en OI permanece en fase inicial, con definiciones conceptuales pero sin un cuerpo estructural de aplicación operacional.

¹⁹ La Guerra de Malvinas constituye un hito negativo, ya que reveló que la ausencia de conducción centralizada de la información debilitando así la estrategia nacional en toda la campaña.

interactúan continuamente y que influyen de manera directa en el proceso de decisión militar. El manual FM 3-13 Information Operation (2003, p. V-1), clasifica:

La **dimensión física** incluye la infraestructura (satélites, servidores, antenas) que permite sostener los flujos de información.

La **dimensión informativa** se refiere a los datos, procesos y sistemas que permiten crear, almacenar y proteger la información.

La **dimensión cognitiva** constituye el centro de gravedad más delicado, pues abarca percepciones, valores y moral de las audiencias, donde se generan los efectos decisivos de influencia.

Moresi et al. (2023) señalan que las redes sociales son consideradas capacidades claves en el dominio cognitivo, particularmente útiles durante las llamadas Fases Previas al Conflicto (Shaping Phase) (Fase de Modelado), donde la influencia sobre actores clave puede modificar el comportamiento adversario sin necesidad de hostilidades abiertas.

Este enfoque no es solo occidental. Tal como explica Vallejos (2018), la doctrina rusa actualizada, bajo el pensamiento de Gerasimov, integró de manera explícita las redes sociales en la dimensión cognitiva, utilizándolas para “la desestabilización, la erosión de la imagen o la movilización de masas”. (p. 4).^{20 21} Con ello, Rusia confirma que el verdadero campo de batalla contemporáneo es la mente del adversario.

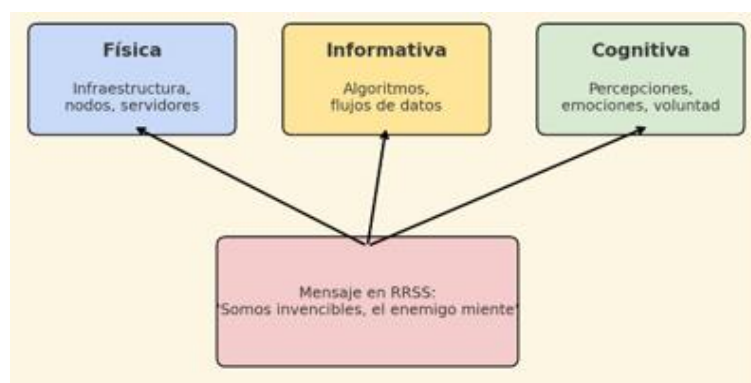


Figura 2 – Dimensiones del ambiente de la Información.

²⁰ La dimensión cognitiva se considera la más crítica, porque los efectos en las otras dos dependen en última instancia de la percepción humana.

²¹ El “control reflexivo” ruso consiste en manipular la percepción del adversario para que adopte decisiones convenientes al interés propio.

1.3 Redes sociales como herramienta operacional: características y capacidades.

Las redes sociales se consolidaron en las últimas dos décadas como un instrumento de alcance operacional. Su carácter bidireccional y su capacidad de difusión inmediata permiten afectar tanto a las tropas adversarias como a la opinión pública global. Demostrando así, según Rissoan (2011), que poseen características que las convierten en herramientas de valor operacional, permitiendo:

- Difusión inmediata y masiva de la información.
- Segmentación de audiencias mediante algoritmos.
- Retroalimentación en tiempo real.
- Dificultad para la trazabilidad o atribución de origen.

Estas cualidades permiten su uso en campañas de desinformación, operaciones psicológicas, manipulación narrativa, apoyo a maniobras y contención comunicacional de crisis. En apoyo a las operaciones militares, se las puede emplear tanto para influir sobre la opinión pública como para neutralizar acciones adversarias.

Jennifer Golbeck (2015) sostiene que estas plataformas constituyen espacios de interacción masiva donde la manipulación de narrativas se produce a escala inédita en la historia de la comunicación humana. En términos militares, su empleo no se limita a la propaganda, sino que también puede integrarse con funciones de inteligencia, contrainteligencia y operaciones psicológicas.

El uso de redes sociales en conflictos recientes muestra que fueron empleadas por ejemplo para desmoralizar fuerzas oponentes, cohesionar las propias y obtener apoyos internacionales (Omand, 2018). Estas capacidades las convierten en herramientas que trascienden lo táctico, atraviesan el nivel operacional y hasta alcanzan el nivel estratégico. No obstante, su eficacia depende de la sincronización con otras líneas de operación, como la ciberdefensa y la guerra electrónica.²²

²² La influencia de las redes sociales no puede entenderse de manera aislada; se potencia cuando se articula con otras capacidades informacionales, especialmente en ciberespacio.

Otro rasgo distintivo es su velocidad. Mientras que los medios tradicionales operan con ciclos de horas o días, las redes sociales lo hacen en segundos. Según el *NATO Strat Com COE* (2020), “la velocidad con que circula la información en redes sociales supera ampliamente los ciclos mediáticos tradicionales, lo que obliga a los planificadores a adoptar estructuras más flexibles y capacidades de respuesta en tiempo real” (p. 7).²³

1.4 Aplicabilidad de las redes sociales en los niveles de la guerra.

El empleo de redes sociales no se circunscribe a un solo nivel. En el nivel estratégico, permiten influir en percepciones internacionales y sostener narrativas que legitiman o deslegitiman conflictos (Rid, 2020).

En el nivel operacional, el empleo de las redes sociales y de las operaciones de información se orientó a afectar el centro de gravedad del adversario, entendido como el conjunto de capacidades que le otorgan cohesión y libertad de acción. Esta influencia se ejerce principalmente mediante operaciones psicológicas, campañas de desinformación y manipulación del entorno cognitivo, buscando debilitar la voluntad y la moral de combate del oponente (NATO StratCom COE, 2021; U.S. Joint Chiefs of Staff, 2018). En el nivel táctico, las mismas herramientas se aplican a la coordinación de fuerzas propias, la perturbación del mando y control enemigo y, en algunos casos, al engaño deliberado a través de operaciones de bandera falsa o simulacros informativos (RAND Corporation, 2020; Vallejos, 2024).

Esta versatilidad explica por qué Lucas Kello (2017) denomina a las redes sociales como armas no cinéticas de bajo costo y alto impacto. Sin embargo, su potencial depende de la integración en un diseño mayor de campaña. Así, la doctrina estadounidense JP 3-13 (2012) insiste en que las redes sociales deben concebirse como un medio más dentro del sistema de operaciones informacionales.²⁴

En Latinoamérica, diversas investigaciones coinciden en que las redes sociales desempeñan un papel relevante en la contención social y en el mantenimiento de la legitimidad

²³ Las redes sociales constituyen un espacio híbrido: son al mismo tiempo un sensor, un medio de transmisión y un vector de ataque informacional.

²⁴ Las redes sociales pueden considerarse “multiplicadores de fuerza no cinéticos”, siempre que se integren en el planeamiento conjunto.

democrática, al convertirse en instrumentos de influencia política y social en escenarios de tensión. Mitchelstein (2020) analiza cómo los usuarios latinoamericanos de redes sociales muestran altos niveles de compromiso democrático, pero también creciente desconfianza hacia las instituciones estatales, lo que potencia su papel como canales de movilización social. De modo complementario, Lupu et al. (2020) demostraron que en Brasil y México las plataformas digitales fueron decisivas para moldear narrativas políticas y sostener la legitimidad de los gobiernos en crisis. Sin embargo, en Argentina, estudios recientes advierten que, “pese al uso extendido de redes sociales para la comunicación institucional, aún no existe una doctrina de empleo operacional sistematizada que permita integrar estas herramientas dentro de un marco conjunto de operaciones de información” (Marañón, 2023, p. 3).²⁵

Nivel	Objetivo	Capacidades empleadas	Ejemplos Recientes
Estratégico	Influir en percepciones externas y sostener legitimidad nacional.	- Diplomacia digital - Comunicación estratégica - Campañas narrativas - Gestión de crisis	Campañas de legitimación (OTAN / Rusia, 2014-2022)
Operacional	Debilitar centros de gravedad y proteger la voluntad de combate propia.	- PSYOPS - Desinformación - Ciberdefensa - Operaciones Cognitivas - Contra información	Telegram y Twitter (Guerra ruso-ucraniana, 2022)
Táctico	Coordinar unidades, desorganizar el enemigo y generar micro-efectos locales.	- Mensajería instantánea - Operaciones de bandera falsa - Inteligencia social - Engaño Táctico	WhatsApp y canales cerrados (Siria e Irak, 2017-2019)

Figura 3 – Aplicabilidad de las redes sociales en los niveles de la guerra.

1.5 Riesgos, limitaciones y desafíos asociados.

Si bien las redes sociales ofrecen ventajas significativas, su empleo operacional conlleva riesgos considerables. Uno de ellos es la dificultad para verificar la autenticidad de la información, lo que puede exponer a las fuerzas propias a operaciones de engaño o desinformación (Rid, 2020). Asimismo, el uso de cuentas falsas, bots y trolls puede amplificar

²⁵ El desafío argentino es pasar de un empleo improvisado de redes a un uso institucionalizado dentro del arte operacional.

mensajes adversarios y generar saturación cognitiva en las audiencias. Otro desafío es el carácter difuso de la atribución. En el ciberespacio, resulta complejo identificar la autoría de un ataque informacional. Esto “genera incertidumbre estratégica, ya que dificulta la aplicación de represalias proporcionadas” (Kello, 2017, p. 97).²⁶

Además, Golbeck (2015) advierte que “cuando las personas creen que los organismos gubernamentales recolectan o manipulan datos sin supervisión, la confianza pública se erosiona y aumenta la resistencia” (p. 129). Esta erosión de la confianza social afecta directamente la legitimidad del accionar estatal, especialmente en contextos donde la información circula sin control ni trazabilidad.²⁷ Asimismo, enfatiza que “límites legales y éticos claros son esenciales para mantener la legitimidad institucional mientras se utilizan datos de redes sociales” (p. 130).

Finalmente, Golbeck (2015) advierte que “el monitoreo de redes sociales por parte de actores estatales puede percibirse fácilmente como vigilancia interna si no hay transparencia ni rendición de cuentas” (p. 131). Este riesgo convierte a la comunicación digital en un terreno sensible donde la confianza social puede transformarse en un objetivo estratégico tanto de defensa como de manipulación.²⁸

Este principio resulta aplicable a las Fuerzas Armadas cuando actúan en el dominio informacional, ya que delimita el marco de lo legítimo y protege la relación entre la sociedad y el instrumento militar.²⁹ El desafío, entonces, no solamente radica en si las redes deben ser utilizadas, sino también en cómo hacerlo dentro de un marco doctrinario claro, con controles normativos y con estructuras organizacionales capacitadas.

²⁶ La dificultad de atribuir responsabilidades convierte a las redes sociales en un campo ideal para la guerra híbrida y las operaciones en zona gris. (Kello, 2017)

²⁷ La autora analiza el impacto del uso institucional de redes sociales sobre la confianza ciudadana, señalando que la falta de transparencia puede generar percepciones de manipulación o vigilancia indebida.

²⁸ La autora relaciona la transparencia y la rendición de cuentas con la estabilidad democrática, destacando que su ausencia puede ser explotada en campañas de desinformación o guerra cognitiva.

²⁹ La observancia de marcos legales y éticos fortalece la legitimidad del poder militar y evita la percepción de intervención sobre la población civil.

CAPÍTULO II

LA GUERRA RUSO-UCRANIANA (2014-2024): OPERACIONES DE INFORMACIÓN Y EMPLEO DE REDES SOCIALES EN EL NIVEL OPERACIONAL

2.1 Contexto geopolítico y doctrinario previo al conflicto (2014-2024).

El conflicto entre Rusia y Ucrania no puede comprenderse sin atender al proceso de transformación doctrinaria que la Federación Rusa inició tras la disolución de la Unión Soviética. Desde comienzos del siglo XXI, Moscú identificó la pérdida de control informacional como una amenaza directa a su seguridad estratégica. En este sentido, el General Valeri Gerasímov (2013), Jefe del Estado Mayor ruso, sostuvo que “las reglas de la guerra han cambiado: el papel de los medios no militares para alcanzar objetivos políticos y estratégicos ha crecido y, en muchos casos, ha superado en eficacia al de las armas convencionales” (p. 2). Este principio, posteriormente interpretado en Occidente como la doctrina Gerasímov, describía un modelo de confrontación donde la información y la manipulación de percepciones constituían el núcleo de la maniobra estratégica.³⁰

El pensamiento militar ruso incorporó así los aportes de Igor Panarin y Sergei Komov, quienes desde la década de 1990 habían desarrollado la noción de guerra de información global. Mientras que Panarin (2006) definía esta modalidad como “la lucha por la dominación del espacio informacional mundial mediante el control de las conciencias y de los flujos de comunicación” (p. 74), Komov (2012), por su parte, profundizaba en la dimensión espiritual y cultural de la información, sosteniendo que la guerra moderna se libra “en la mente del adversario antes que en el terreno físico” (p. 41). Ambas visiones confluyeron en una estrategia estatal donde la propaganda, las operaciones psicológicas y la desinformación constituyen herramientas legítimas para erosionar la cohesión interna del oponente.³¹

³⁰ El concepto “doctrina Gerasímov” no fue formulado por el propio general, sino acuñado por analistas occidentales para sintetizar la integración rusa de instrumentos políticos, informacionales y militares en la guerra moderna.

³¹ En el pensamiento ruso, la “guerra de información” es concebida como un proceso permanente y no como una fase previa al conflicto, lo que le otorga carácter estratégico y no meramente táctico.

Mientras tanto, en el ámbito occidental, autores como David Omand y Thomas Rid advertían sobre el avance de un entorno caracterizado por la competencia informacional constante. Omand (2020) señalaba que las democracias deberían “integrar inteligencia, comunicación estratégica y ciberdefensa bajo una conducción centralizada para resistir la manipulación digital extranjera” (p. 67). En igual sentido, Rid (2020) sostenía que la desinformación no es simplemente “mentira política”, sino un “instrumento de influencia estratégica que busca moldear la realidad percibida” (p. 38). Estas reflexiones fueron confirmadas por los análisis del NATO Strat Com COE (2022) y de la RAND Corporation (2021), que desde 2015 advertían que Rusia combinaba la desinformación con operaciones militares convencionales para maximizar efectos sincrónicos en el plano político y cognitivo.³²

El escenario previo a 2022 se caracterizó así por una asimetría doctrinaria: mientras Rusia concebía la información como un arma estratégica total, las potencias occidentales la trataban principalmente como un dominio funcional de apoyo. Esta diferencia explica la ventaja inicial de Moscú en la construcción de narrativas y la manipulación perceptiva durante la anexión de Crimea en 2014, cuando logró instalar un relato de legitimidad popular y deslegitimar al gobierno de Kiev antes de iniciar acciones militares directas (NATO Strat Com COE, 2015). La expansión posterior del conflicto demostró que el control del entorno informacional es tan determinante como el control del terreno físico, consolidando la idea de que la guerra moderna se libra simultáneamente en los planos cinético y cognitivo.

2.2. Estrategia rusa de información y guerra cognitiva.

En el nivel operacional, la Federación Rusa integró las operaciones de información dentro de su concepción ampliada de la guerra híbrida, orientada a generar efectos directos en la voluntad, la moral y la percepción del adversario. Esta estrategia buscó no solo acompañar la maniobra militar, sino preparar el teatro de operaciones mediante la manipulación del entorno cognitivo, asegurando que las condiciones informacionales favorecieran la acción

³² La OTAN emplea el término “Information Environment Operations” para describir la integración de ciberdefensa, comunicación estratégica y operaciones psicológicas dentro del marco conjunto, equivalente funcional de las OI rusas.

posterior de las fuerzas convencionales. Según la RAND Corporation (2021), la ofensiva rusa combinó “acciones sincronizadas en el ciberespacio, la información pública y la percepción internacional” (p. 22) para alterar el equilibrio psicológico de Ucrania y sus aliados, demostrando un nivel de integración informacional sin precedentes.³³

La estrategia rusa se estructuró sobre tres ejes: propaganda estratégica, control reflexivo y dominación cognitiva. El primero de ellos, la propaganda, buscó modelar narrativas favorables dentro y fuera del país. Como explicó Igor Panarin (2006), la información “constituye el principal instrumento de poder, pues quien domina la interpretación de los hechos domina también la reacción de las masas” (p. 74). Esta premisa se operacionalizó mediante la generación de mensajes sincronizados desde medios estatales (RT, Sputnik), complementados por redes sociales y actores digitales afines, que actuaron como multiplicadores de contenido. El segundo eje, el control reflexivo, retomó la tradición soviética de inducir decisiones erróneas en el adversario mediante información parcial o ambigua. Valeri Gerasímov (2013) describió este enfoque al afirmar que “el objetivo es anticiparse al pensamiento enemigo, condicionando su acción a partir de percepciones que nosotros mismos creamos” (p. 3).³⁴

Finalmente, el tercer eje, la dominación cognitiva, sintetizó la convergencia entre las dimensiones informativa y psicológica. Sergei Komov (2012) sostenía que “la batalla contemporánea se libra en la conciencia colectiva: quien logra instalar su visión de la realidad obtiene la victoria antes de que comiencen los combates” (p. 41). Esta concepción fue aplicada en el conflicto ucraniano mediante campañas de desinformación destinadas a desmoralizar a las tropas enemigas, fracturar la cohesión nacional y generar desconfianza hacia las instituciones. Los informes del NATO Strat Com COE (2016) confirman que estas acciones tuvieron un propósito operacional definido: degradar el proceso decisorio ucraniano y disuadir la resistencia en áreas seleccionadas antes de la intervención militar directa.

³³ A nivel operacional, las OI rusas se planifican como parte de la maniobra conjunta, con objetivos definidos de desorganización del mando, ruptura comunicacional y erosión de la moral enemiga.

³⁴ El control reflexivo implica diseñar mensajes y acciones que orienten el proceso decisorio del adversario, llevándolo a adoptar comportamientos que favorezcan los intereses rusos.

Durante la invasión de 2022, esta estructura doctrinaria se tradujo en un sistema de mando informacional integrado al nivel de teatro. Las operaciones de información se coordinaron con las operaciones cibernéticas ofensivas y con las acciones de inteligencia militar. Según el Centro de Excelencia de Ciberdefensa de la OTAN (2022), la ofensiva digital previa al 24 de febrero “buscó paralizar infraestructuras críticas, sembrar pánico y reducir la capacidad de comunicación del gobierno ucraniano” (p. 7). Este patrón operativo demostró que las OI rusas ya no actuaban como un complemento táctico, sino como una línea de esfuerzo principal dentro del nivel operacional conjunto.

Por su parte, David Omand (2020) advierte que este modelo representa una amenaza directa para los sistemas democráticos, pues transforma la información en “un dominio de combate donde los límites entre lo civil y lo militar se desdibujan” (p. 118). Complementa esta visión Thomas Rid (2020) al afirmar que las operaciones rusas en Ucrania “marcaron el retorno de la desinformación estratégica como arma principal de guerra política” (p. 53). Ambas interpretaciones confirman que la maniobra rusa en el dominio informacional alcanzó efectos operacionales tangibles, degradando la cohesión social del adversario y generando una correlación de fuerzas favorable sin requerir victorias cinéticas iniciales.³⁵

En síntesis, la estrategia rusa de información se caracterizó por su planificación centralizada, su sincronización con otras funciones conjuntas (inteligencia, ciberdefensa, operaciones psicológicas) y su foco en la dimensión cognitiva del enemigo. El caso ucraniano confirmó la vigencia de la doctrina rusa que concibe la guerra no como un evento puntual, sino como un proceso continuo de confrontación política, económica e informacional, en el cual el control de la percepción precede a la acción militar.

2.3. Respuesta ucraniana: defensa informacional y guerra narrativa.

A diferencia de la estrategia rusa, la respuesta ucraniana en el dominio informacional se estructuró sobre la base de la defensa narrativa y la movilización internacional, orientadas a sostener la moral interna y garantizar el apoyo externo. Desde 2014, tras la anexión de Crimea,

³⁵ El nivel operacional constituye el espacio de articulación donde la influencia informacional se transforma en ventaja militar concreta, conectando los objetivos estratégicos con los efectos tácticos.

Kiev comprendió que el control del discurso público constituía un componente esencial del esfuerzo militar. Según el NATO Strat Com COE (2022), el gobierno ucraniano “pasó de ser objeto a actor del conflicto informacional, adoptando una política de comunicación estratégica destinada a contrarrestar la propaganda rusa y a fortalecer la legitimidad del Estado ante su población y la comunidad internacional” (p.19).³⁶ Frente a la comunidad internacional, Ucrania, a través de la Oficina de Comunicación Estratégica, se presentó como la nación agredida, articulando mensajes oficiales y coordinando una narrativa orientada a reforzar esa condición. Entre los ejes comunicacionales más recurrentes se destacaron afirmaciones tales como; ellos nos invadieron, el Donbás es históricamente nuestro y fue arrebatado, ya nos quitaron Crimea y ahora nos están bombardeando y ellos tiraron primero, entre otros.

En el nivel operacional, el mando ucraniano articuló las operaciones de información con las funciones de inteligencia, asuntos civiles y relaciones internacionales, siguiendo el modelo occidental de Strategic Communication (STRATCOM). Un documento del Centro para el Análisis de Políticas de Defensa de Kiev (2020) señaló que “la defensa informacional se convirtió en un componente de la maniobra conjunta, cuyo objetivo principal era preservar la cohesión moral del pueblo y de las fuerzas armadas” (p. 6). Esta defensa informacional se tradujo en una serie de operaciones narrativas que buscaron moldear la percepción de la guerra tanto dentro como fuera del país.

El liderazgo personal del presidente Volodímir Zelenski fue determinante en esta dinámica. Su presencia diaria en medios y redes sociales permitió mantener la moral de combate y proyectar la imagen de un Estado resiliente. Investigadores de la RAND Corporation (2022) señalan que la comunicación directa de Zelenski “logró neutralizar la desinformación rusa al humanizar la resistencia y enmarcar la defensa nacional como causa universal de libertad” (p. 11).³⁷

El aparato comunicacional ucraniano también se apoyó en alianzas informacionales con actores no estatales, incluyendo medios internacionales y comunidades digitales. Plataformas

³⁶ La comunicación estratégica se convirtió en Ucrania en un instrumento operacional, integrando los ámbitos político, militar y diplomático en un mismo esfuerzo de información.

³⁷ El liderazgo comunicacional de Zelenski funcionó como centro de gravedad moral, generando efectos operacionales al fortalecer la cohesión de las fuerzas y la voluntad popular de resistencia.

como Twitter, Telegram y TikTok se transformaron en multiplicadores de contenido, donde periodistas, voluntarios y ciudadanos difundieron evidencia de crímenes de guerra o éxitos militares en tiempo real. Thomas Rid (2020) subraya que “la transparencia y la descentralización de la información constituyen el antídoto más eficaz contra la manipulación” (p. 78). En este sentido, Ucrania utilizó la participación civil como recurso operacional, ampliando su capacidad de proyección narrativa sin depender exclusivamente del aparato estatal.

Los analistas del NATO Strat Com COE (2022) concluyen que esta estrategia generó un efecto multiplicador: la información difundida por redes sociales no solo fortaleció la moral interna, sino que movilizó apoyo político y militar internacional. La difusión planificada de imágenes de resistencia civil, el uso de símbolos nacionales y la construcción de una narrativa de víctima agredida legitimaron la recepción de ayuda occidental y consolidaron un frente comunicacional global favorable a Kiev.³⁸

Desde el punto de vista doctrinario, la defensa informacional ucraniana puede entenderse como una forma de operación conjunta en el dominio cognitivo, cuyo objetivo fue asegurar la continuidad del mando y control, preservar la voluntad nacional y proyectar resiliencia estratégica. En palabras de David Omand (2020), “la verdad verificada, difundida con rapidez y coherencia, es el arma más poderosa de las democracias ante la desinformación” (p. 141). Ucrania demostró que la información, gestionada con disciplina y sincronización a través de las redes sociales, puede transformarse en un vector operacional decisivo.

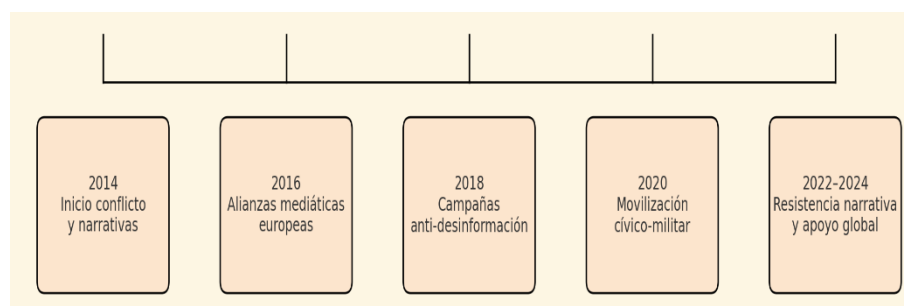


Figura 4 – Estrategia informacional ucraniana (2014 – 2024).

³⁸ La “guerra narrativa” ucraniana operó como línea de esfuerzo operacional complementaria a la maniobra militar, ampliando el espacio de batalla al ámbito diplomático y mediático.

2.4. Plataformas empleadas, actores y mecanismos de acción informacional.

Las OI desarrolladas durante la guerra ruso-ucraniana se articularon a través de una multiplicidad de plataformas digitales y estructuras mediáticas que operaron de forma sincronizada con los esfuerzos militares. En el caso ruso, el sistema comunicacional fue centralizado bajo la supervisión del Ministerio de Defensa y de agencias vinculadas al Servicio Federal de Seguridad (FSB) y a la Dirección Principal de Inteligencia (GRU). La red de medios estatales, encabezada por RT y Sputnik, funcionó como núcleo de propaganda estratégica, mientras que redes sociales como Telegram, VKontakte y Odnoklassniki canalizaron mensajes adaptados a distintos públicos. Según el NATO Strat Com COE (2022), estas plataformas permitieron “amplificar narrativas oficiales y difundir desinformación coordinada con campañas cibernéticas ofensivas” (p.26).³⁹

En contraste, el sistema ucraniano se caracterizó por una coordinación descentralizada basada en la flexibilidad y la participación ciudadana. La Oficina de Comunicación Estratégica del Ministerio de Defensa dirigió los mensajes oficiales y coordinó con los comandos conjuntos, mientras que las fuerzas en el terreno difundían información táctica a través de canales verificados en Telegram y Twitter. La sociedad civil, los medios independientes y la diáspora digital contribuyeron como multiplicadores narrativos. RAND Corporation (2022) señala que esta estructura “permitió sostener la continuidad del flujo informativo incluso durante la disrupción de redes convencionales” (p. 14), reforzando la resiliencia comunicacional del país.⁴⁰

Ambos bandos explotaron las plataformas globales –Twitter, VKontakte, Facebook, TikTok, YouTube y Telegram– para controlar la agenda informativa internacional. Sin embargo, sus objetivos eran diferentes: Rusia buscó deslegitimar a Kiev y dividir la opinión occidental, mientras que Ucrania priorizó la movilización emocional y la obtención de apoyo

³⁹ Las Operaciones de Información rusas siguieron un modelo de mando vertical: el nivel estratégico fija la narrativa, el operacional la sincroniza con la maniobra militar, y el táctico la ejecuta mediante actores digitales y medios afines.

⁴⁰ A diferencia del esquema ruso, el modelo ucraniano se apoyó en la adaptabilidad y la iniciativa individual, convirtiendo la información en un recurso de maniobra distribuida.

externo. Investigadores del Atlantic Council Digital Forensic Research Lab (DFRLab) (2023) detectaron redes coordinadas de cuentas automatizadas rusas que difundían mensajes repetitivos sobre desnazificación, mientras que activistas ucranianos generaban contenido viral que mostraba resistencia civil y daños infligidos al invasor. Esta competencia de narrativas transformó las redes sociales en un campo operacional de doble uso, donde el control del relato equivalía a controlar el espacio de maniobra.

Desde la perspectiva doctrinaria, puede afirmarse que la información se convirtió en una función operacional transversal, capaz de alterar la correlación de fuerzas sin recurrir a enfrentamientos cinéticos. La coordinación entre actores estatales, civiles y tecnológicos demuestra que el entorno informacional contemporáneo trasciende los límites tradicionales de la guerra. En palabras de David Omand (2020), “la guerra moderna se libra tanto en la nube como en el terreno; quien controla la narrativa controla la acción” (p. 145). El estudio del caso ruso-ucraniano revela, en consecuencia, que la dominación cognitiva y la velocidad de difusión se consolidaron como nuevos factores de poder en el nivel operacional. (Ver Anexo 1)

Plataforma	Uso ruso	Uso ucraniano
Telegram	Canales pro-Kremlin, difusión de fake news	Información militar directa, alertas civiles
Vkontakte	Coordinación de desinformación regional	Defensa narrativa en Donbás
Twitter/X	Desinformación automatizada, hashtags manipulados	Testimonios ciudadanos, diplomacia digital
TikTok	Videos editados para generar pánico	Viralización de relatos de resistencia
YouTube	Propaganda y relatos conspirativos	Conferencias de prensa, denuncias de crímenes

Figura 5 - Plataformas empleadas, actores y mecanismos de acción informacional.

2.5. Efectos y comparación desde la perspectiva operacional.

El análisis de los resultados operacionales del conflicto demuestra que las redes sociales se convirtieron en uno de los principales multiplicadores de poder informacional, generando efectos que trascendieron el plano comunicacional para influir directamente en la conducción de operaciones. Según la RAND Corporation (2022), el empleo de redes como Twitter, Telegram y Tik Tok “modificó la correlación de fuerzas al permitir a los actores estatales y no estatales obtener ventajas cognitivas sobre el adversario” (p. 22). Estas plataformas no solo

sirvieron para difundir información, sino también para recolectarla, analizarla y transformarla en inteligencia operacional en tiempo real.⁴¹

En el caso ruso, las redes sociales fueron utilizadas para anticipar reacciones enemigas, difundir narrativas y desorganizar la moral ucraniana, en estrecha coordinación con sus operaciones cibernéticas y psicológicas. Un informe del NATO Strat Com COE (2022) señala que Moscú “empleó Telegram como centro de comando informacional, integrando cuentas oficiales, troles y medios afines para maximizar la velocidad y la coherencia de los mensajes” (p. 31). La campaña de desinformación sobre la supuesta rendición ucraniana de Kiev, lanzada durante las primeras 48 horas de la invasión, ejemplifica esta sinergia: su objetivo era generar confusión, afectar la voluntad de combate y condicionar el proceso decisorio del adversario.⁴²

Por su parte, Ucrania demostró que las redes sociales pueden operar como armas defensivas y ofensivas no cinéticas. La estrategia del Centro de Comunicación Estratégica y la acción directa del presidente Volodímir Zelenski transformaron plataformas como Twitter y Tik Tok en medios de conducción política y psicológica. La difusión constante de mensajes desde la capital sitiada reforzó la moral nacional y proyectó una imagen de liderazgo activo. Según el Atlantic Council Digital Forensic Research Lab (DFRLab) (2023), la interacción digital directa de Zelenski “produjo un efecto sinérgico entre la percepción popular y la maniobra militar, reduciendo el impacto psicológico de los ataques iniciales rusos” (p. 12). Este fenómeno evidenció que la narrativa puede convertirse en un factor operacional decisivo cuando es empleada con sincronización y coherencia estratégica.⁴³

Además, las redes sociales operaron como instrumentos de inteligencia colectiva. Miles de usuarios ucranianos y ciudadanos internacionales colaboraron en la geolocalización de movimientos rusos mediante publicaciones, imágenes y videos, generando una red espontánea de recolección de datos (crowdsourced intelligence). Este proceso permitió optimizar los ciclos de decisión en el nivel operacional, al proporcionar información casi en tiempo real al mando

⁴¹El empleo de redes sociales en el nivel operacional proporcionó inteligencia abierta (OSINT) de alto valor táctico y permitió sincronizar decisiones sobre objetivos de campaña.

⁴²El efecto operacional de la desinformación rusa se midió en la ralentización del mando ucraniano y en la pérdida temporal de cohesión en las primeras líneas.

⁴³El liderazgo comunicacional ucraniano funcionó como un centro de gravedad moral, cuyo sostenimiento dependió del uso constante y disciplinado de redes sociales.

militar. El NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2022) observó que la interacción entre la población civil y los planificadores militares “redujo los tiempos de respuesta y amplificó la conciencia situacional del campo de batalla” (p. 9). Así, el entorno digital se transformó en un campo de maniobra compartido, donde cada usuario representó un nodo activo dentro del sistema informacional conjunto.⁴⁴

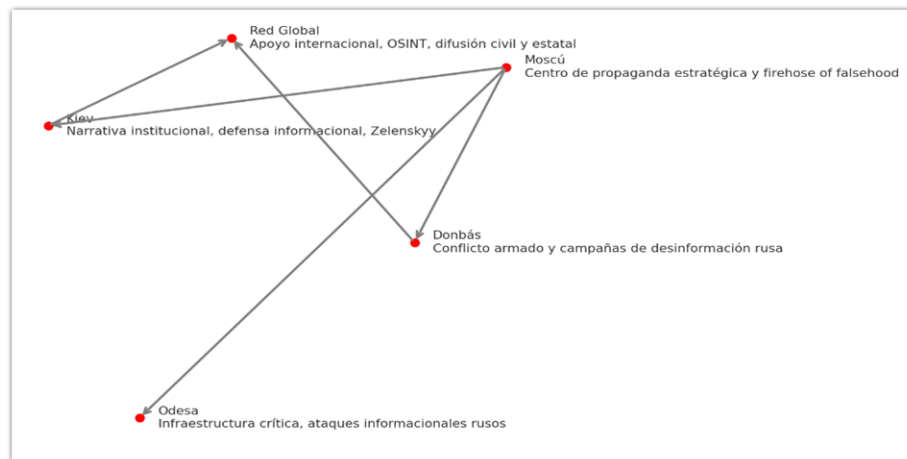


Figura 6 - Zonas clave y operaciones informacionales.

Desde la perspectiva de la evaluación de efectos, el empleo de redes sociales logró alterar la dimensión cognitiva del conflicto. Para David Omand (2020), la información difundida en redes puede “desactivar o potenciar voluntades colectivas”, y en el caso ucraniano, “operó como catalizador de cohesión social y legitimidad internacional” (p. 148). En términos operacionales, los efectos se reflejaron en tres logros concretos: la preservación de la moral nacional, la neutralización parcial de la desinformación rusa y la movilización del apoyo externo. Como concluye Thomas Rid (2020), esta guerra “demostró que la victoria en la esfera informacional precede y condiciona la victoria en el campo de batalla” (p. 89).

⁴⁴ La integración de información civil abierta (OSINT) con inteligencia militar tradicional constituye uno de los mayores avances en la conducción operacional moderna.

Fuente	Actor estatal (GRU)	Actores civiles/estatales
Mensaje	Narrativa unificada	Narrativas múltiples
Objetivo	Propaganda externa	Legitimidad democrática
Plataformas	Redes pro-régimen	Redes mixtas
Control	Alto centralismo	Alta adaptabilidad

Figura 7 – Comparación desde la perspectiva operacional.

2.6. Lecciones aprendidas del caso analizado.

La guerra ruso-ucraniana evidenció que las redes sociales constituyen un componente decisivo del poder informacional en el nivel operacional, al permitir generar efectos inmediatos sobre la moral, la cohesión y la percepción estratégica del adversario. En contextos donde la confrontación directa resulta limitada o inaceptable, las redes operan como un multiplicador no cinético, capaz de modificar comportamientos colectivos y alterar la correlación de fuerzas sin recurrir a la violencia. Según la RAND Corporation (2022), “el dominio informacional ha adquirido un valor operacional equivalente al fuego o a la maniobra” (p. 33), ya que sus resultados impactan directamente en la libertad de acción de las fuerzas.⁴⁵

Para las Fuerzas Armadas argentinas, este caso confirma la necesidad de integrar de manera sistemática las redes sociales dentro del planeamiento conjunto, tanto en su dimensión ofensiva (influencia externa) como defensiva (protección de la narrativa nacional). La experiencia ucraniana demuestra que la información puede emplearse como línea de esfuerzo coordinada, capaz de reforzar la legitimidad de la acción militar y sostener el apoyo social. David Omand (2020) advierte que “la credibilidad y la coherencia del mensaje son elementos de combate tanto como el poder de fuego” (p. 152), lo cual exige estructuras doctrinarias que

⁴⁵ En la actualidad, las operaciones informacionales constituyen un instrumento legítimo para alcanzar efectos operacionales sin desgaste material, a través de la manipulación de percepciones.

unifiquen comunicación estratégica, inteligencia y operaciones psicológicas bajo una conducción centralizada.⁴⁶

2.7. Aplicabilidad al ámbito de la defensa argentina.

La aplicación nacional de las lecciones aprendidas -del caso analizado en la sección anterior- requiere, la creación de un Comando Conjunto de Operaciones Informacionales con capacidad de planificar, coordinar y evaluar los efectos cognitivos y sociales derivados del uso de redes digitales. Dicho comando debería integrar especialistas en comunicación, ciberdefensa, inteligencia y asuntos civiles, siguiendo el modelo de coordinación observado en Ucrania. El NATO StratCom COE (2022) señala que “la integración de los flujos informacionales en todos los niveles de conducción incrementa la efectividad de la maniobra militar” (p. 42). Este principio podría adaptarse al contexto argentino, fortaleciendo la conducción operacional y la protección de los centros de gravedad cognitivos de la sociedad.

Finalmente, las redes sociales deben entenderse como una herramienta de proyección estratégica para las democracias modernas. Su empleo controlado permite aumentar la capacidad disuasiva del Estado, proteger la legitimidad de sus instituciones y anticipar amenazas híbridas. Como sostiene Thomas Rid (2020), “la desinformación no desaparece; se combate con organización, disciplina y verdad verificada” (p. 284). El desafío argentino consiste, por tanto, en transformar el aprendizaje observado en Ucrania en doctrina nacional, que contemple la información como un dominio operativo, la red como un campo de batalla, y la verdad como un recurso operacional y estratégico de la defensa.

⁴⁶ El planeamiento operacional debe contemplar el dominio informacional como espacio de maniobra, incorporando el control y la defensa de las narrativas propias.

Capítulo III

IMPLICANCIAS Y PROPUESTAS PARA EL INSTRUMENTO MILITAR ARGENTINO

3.1 Integración de las redes sociales en las Operaciones de Información conjuntas.

La evolución del entorno operativo contemporáneo ha obligado a reconocer a las redes sociales como un elemento esencial del poder informacional. Su masividad, inmediatez y capacidad de segmentación han convertido estos espacios digitales en verdaderas plataformas de maniobra cognitiva, donde la información puede emplearse para lograr efectos decisivos en el nivel operacional. En palabras de Lucas Kello (2017), “las redes sociales actúan como armas no cinéticas de bajo costo y alto impacto, capaces de producir desorganización estratégica en cuestión de minutos” (p. 95). Este fenómeno confirma que el dominio informacional ya no es accesorio, sino un componente orgánico de la maniobra conjunta, en el cual las operaciones psicológicas, la inteligencia y la comunicación estratégica convergen para garantizar la libertad de acción del comandante operacional.⁴⁷

La integración de las redes sociales dentro de las OI conjuntas requiere una doctrina que combine el control del flujo informativo con la capacidad de generar efectos cognitivos planificados. Según la RAND Corporation (2022), la superioridad informacional se obtiene “cuando la comunicación, la percepción y la acción se sincronizan dentro del ciclo operacional” (p. 27). De manera concordante, Moresi et al. (2023) señalan que la conducción operacional moderna “debe articular los efectos cinéticos y no cinéticos mediante la manipulación del entorno cognitivo del adversario” (p. 164). Este principio coincide con el enfoque del NATO StratCom COE (2022, p. 15), que define el éxito operacional como la capacidad de “dominar la narrativa y limitar la capacidad de respuesta del enemigo” (p. 15). En este marco, las redes

⁴⁷ El nivel operacional constituye el espacio donde la información, gestionada con precisión, puede traducirse en ventaja táctica y estratégica simultáneamente.

sociales operan como vectores de influencia simultánea, capaces de degradar centros de gravedad morales y fortalecer la cohesión de las propias fuerzas.⁴⁸

A diferencia de los medios tradicionales, las redes sociales introducen un factor de velocidad y retroalimentación constante que modifica los procesos de mando y control. Jennifer Golbeck (2015) advierte que “la interacción digital a gran escala altera los ciclos de decisión, forzando a los planificadores a operar en horizontes temporales más cortos” (p. 129). En consecuencia, la conducción de OI conjuntas debe incorporar estructuras de monitoreo permanente (OSINT) y equipos especializados capaces de detectar tendencias y responder en tiempo real. David Omand (2020) complementa esta idea al sostener que “la ventaja informacional no se logra con más datos, sino con mayor rapidez en su interpretación” (p. 150). El desafío consiste, entonces, en integrar las redes sociales a los procesos operacionales mediante sistemas de análisis, orientación y respuesta, garantizando coherencia entre los objetivos militares y las condiciones cognitivas del entorno.⁴⁹

Finalmente, la doctrina conjunta argentina debería avanzar hacia la formalización de un sistema integrado de operaciones informacionales, donde las redes sociales se gestionen como parte de la maniobra conjunta. De Spiegeleire et al. (2017) advierten que los Estados que “no institucionalicen la dimensión informacional en su estructura operacional quedarán rezagados ante actores más ágiles y descentralizados” (p. 13). Esta afirmación adquiere relevancia en el contexto nacional, donde autores como Vallejos (2018) proponen consolidar un modelo de “operaciones cognitivo-informacionales” bajo un comando conjunto especializado (p. 32). En síntesis, la integración de las redes sociales dentro de las OI conjuntas permitirá a las Fuerzas Armadas argentinas proyectar poder informacional, proteger su narrativa estratégica y generar efectos operacionales medibles en el ámbito regional e internacional. (Ver Anexo 2)

⁴⁸ La información difundida en redes puede tener un efecto operacional análogo al fuego de apoyo, actuando sobre la moral y la voluntad de combate.

⁴⁹ El ciclo informacional operacional debe incluir la observación, orientación, decisión y acción, replicando la lógica del ciclo OODA en el dominio informacional.

3.2 Desafíos para la planificación y conducción conjunta.

La incorporación de las redes sociales en las OI conjuntas plantea desafíos significativos para la planificación y conducción operacional. En primer lugar, surge la dificultad de mantener el control doctrinario sobre una herramienta que, por naturaleza, es descentralizada, dinámica y de alcance global. Jennifer Golbeck (2015) advierte que “las redes sociales poseen una lógica de viralidad que escapa a las jerarquías tradicionales de control” (p. 132), lo cual puede generar efectos no deseados o contradictorios con los objetivos de la operación. En contextos militares, esta imprevisibilidad obliga a establecer mecanismos de coordinación, monitoreo y evaluación de efectos para evitar la dispersión del mensaje o la vulneración de la narrativa institucional.⁵⁰

Otro desafío es la delgada frontera entre la acción informativa legítima y la manipulación indebida. David Omand (2020) plantea que “la eficacia en el dominio informativo depende de la disciplina ética en el uso de la verdad” (p. 152). Las Fuerzas Armadas deben equilibrar la necesidad de influir en el adversario con la preservación de la legitimidad democrática y el respeto al derecho internacional. En el caso argentino, esto implica ajustar las operaciones informativas a los marcos normativos vigentes y garantizar que las acciones de comunicación estratégica no vulneren derechos fundamentales. Moresi et al. (2023) sostienen que “el empleo ético de la información es condición indispensable para la sostenibilidad de la acción militar en sociedades democráticas” (p. 170).⁵¹

Asimismo, la dependencia tecnológica constituye un riesgo operacional creciente. Las plataformas de redes sociales son en su mayoría privadas y extranjeras, lo que limita la soberanía informativa de los Estados. Según Lucas Kello (2017), “el control de la infraestructura digital equivale al control de la percepción global” (p. 99). Esta afirmación cobra especial relevancia para la defensa nacional, ya que una interrupción en los servicios o un cambio en las políticas de las plataformas puede afectar la continuidad de las operaciones. En consecuencia, la conducción conjunta debe prever planes de contingencia informativa, diversificar canales de difusión y fortalecer las capacidades nacionales de ciberdefensa. De

⁵⁰ El control operacional de la información digital debe basarse en la trazabilidad del mensaje y en la responsabilidad de mando.

⁵¹ La transparencia y el respeto al marco jurídico constituyen la base moral de las OI en contextos democráticos.

Spiegeleire et al. (2017) destacan que “la resiliencia informacional se logra mediante redundancia, autonomía tecnológica y adiestramiento en ciberseguridad” (p. 15).⁵²

Por último, la planificación de OI en redes sociales enfrenta el desafío del análisis de efectos cognitivos. A diferencia de los resultados físicos o cuantificables, los efectos sobre la percepción, la moral o la cohesión social son difíciles de medir y evaluar. Eric V. Larson (2021) señala que “la evaluación de operaciones informacionales requiere métricas flexibles, basadas en indicadores de influencia y cambios de comportamiento” (p. 12). En el nivel operacional, esto implica desarrollar metodologías conjuntas para identificar indicadores tempranos de éxito o fracaso, empleando análisis de sentimiento, seguimiento narrativo y monitoreo del impacto público. La evaluación precisa de estos efectos permitirá a los comandantes ajustar el esfuerzo informacional y garantizar la coherencia entre los objetivos estratégicos y los resultados alcanzados.

3.3 Propuesta de modelo operativo informacional para la defensa argentina.

La experiencia internacional analizada evidencia que las OI constituyen un instrumento decisivo de la maniobra conjunta moderna. En este sentido, las Fuerzas Armadas argentinas deben evolucionar hacia una estructura que integre doctrinariamente las redes sociales, la ciberdefensa y la comunicación estratégica bajo un mando unificado. Tal como advierten Moresi et al. (2023), “la información debe ser tratada como una capacidad operacional y no como un apoyo accesorio” (p. 181). El objetivo es generar un sistema de conducción capaz de planificar, ejecutar y evaluar efectos cognitivos, tanto en el plano nacional como regional, mediante el empleo disciplinado de redes digitales.⁵³

El modelo operativo propuesto se basa en tres principios doctrinarios: centralización de la conducción, sincronización de funciones y flexibilidad adaptativa. Según la RAND Corporation (2022), la integración efectiva de las capacidades informacionales “requiere una arquitectura conjunta que unifique inteligencia, ciberdefensa y comunicación en una misma

⁵² La soberanía informacional depende tanto de la infraestructura tecnológica como de la capacidad humana para gestionar el entorno digital.

⁵³ El modelo operativo informacional conjunto propone transformar el dominio informativo en un espacio de maniobra autónomo, sujeto a la conducción centralizada.

línea de esfuerzo” (p. 34). En esta línea, el NATO Strat Com COE (2022) enfatiza que la eficacia de las OI radica en “la interoperabilidad entre organismos civiles y militares, bajo un comando estratégico-operacional unificado” (p. 42). En el contexto argentino, ello implicaría la creación de un Comando Conjunto de Operaciones Informacionales (CCOINF) dependiente del Estado Mayor Conjunto de las FFAA, con facultades para planificar y conducir acciones en el dominio informacional. (Ver Anexo 3)

En el nivel operacional, este Comando tendría a su cargo tres áreas funcionales:

1. **Monitoreo y análisis informacional (OSINT y Ciberinteligencia)**, orientado a detectar narrativas hostiles y evaluar vulnerabilidades cognitivas.
2. **Planeamiento y ejecución de operaciones informacionales**, orientado a la comunicación estratégica, contra información y campañas digitales.
3. **Evaluación de efectos cognitivos y de percepción**, para generar indicadores medibles de influencia y cohesión social.

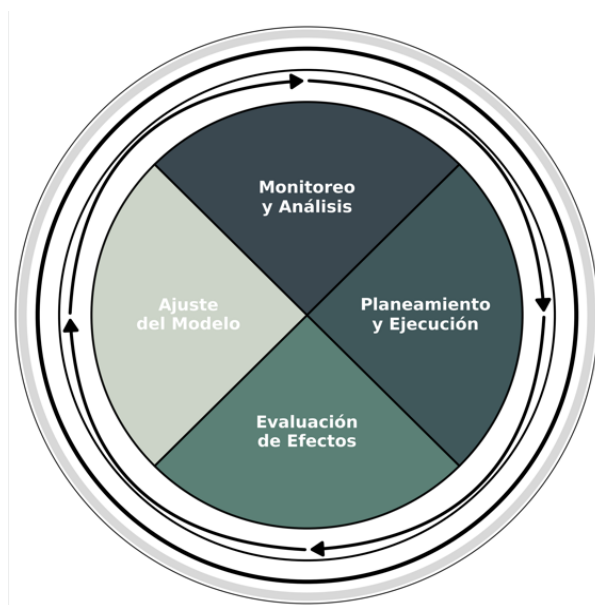


Figura 8 – Modelo Ciclo Operativo Informacional.

De Spiegeleire et al. (2017) afirman que “la capacidad de traducir la información en poder operacional depende de la existencia de estructuras permanentes de análisis y respuesta” (p. 18). Este enfoque permitiría a la Argentina disponer de una capacidad sostenida de acción

informativa, con medios civiles y militares interoperables, bajo conducción conjunta y control político-estratégico-operacional.⁵⁴

Por último, la consolidación del modelo propuesto requiere formación doctrinaria, adiestramiento conjunto y desarrollo tecnológico nacional. Omand (2020) sostiene que “el verdadero poder informativo reside en la preparación del personal y en la cultura de análisis que guía sus decisiones” (p. 154). Para ello, resulta indispensable incorporar módulos de guerra cognitiva y operaciones en redes en los programas de formación de los institutos de defensa. Asimismo, la coordinación con universidades y centros de innovación nacionales permitirá fortalecer la investigación aplicada al dominio informativo. El propósito final de este modelo no es solo responder ante amenazas, sino proyectar influencia, proteger la narrativa nacional y asegurar la libertad de acción cognitiva del Estado argentino en el siglo XXI.

3.4 Evaluación prospectiva y requerimientos doctrinarios.

La progresiva incorporación del dominio informativo en la planificación operacional exige una doctrina nacional integral que consolide los aprendizajes obtenidos y proyecte la acción conjunta hacia el futuro. La experiencia comparada —especialmente el caso ucraniano— demostró que las redes sociales no son solo un medio de comunicación, sino una herramienta de poder nacional que influye directamente sobre la cohesión social, la legitimidad institucional y la libertad de acción de las fuerzas. Thomas Rid (2020) afirma que “la información es ahora un espacio permanente de confrontación estratégica, donde los Estados compiten por moldear la percepción antes que por ocupar el terreno” (p. 287). Este nuevo paradigma obliga a redefinir la doctrina argentina, incorporando la información y el uso de las redes sociales como capacidades esenciales del nivel operacional conjunto.⁵⁵

En el corto plazo, el desafío principal es la formalización doctrinaria. Las Fuerzas Armadas deben incorporar la dimensión informativa en sus manuales de planeamiento, ejercicios conjuntos y currículas de formación. Según la RAND Corporation (2022), “los

⁵⁴ La interoperabilidad civil-militar en el dominio informativo es esencial para garantizar legitimidad y continuidad institucional.

⁵⁵ La información, tratada como un recurso operacional, requiere conducción, estructura, adiestramiento y evaluación igual que cualquier otra función militar.

Estados que institucionalizan la información como dominio de maniobra obtienen ventajas duraderas en la toma de decisiones” (p. 38). De manera coincidente, Moresi et al. (2023) plantean que “la actualización doctrinaria debe acompañar la transformación tecnológica, sin perder el marco ético y jurídico que caracteriza a las fuerzas democráticas” (p. 191). En este sentido, la doctrina argentina debería establecer principios rectores para el empleo de redes sociales en operaciones informacionales: legitimidad, veracidad, proporcionalidad y sincronización con los objetivos estratégicos nacionales.

A mediano plazo, resulta imprescindible fortalecer las capacidades humanas y tecnológicas. David Omand (2020) sostiene que “el capital intelectual de las fuerzas es el verdadero multiplicador de poder informacional” (p. 156). Para ello, se requiere la formación de oficiales analistas del dominio informacional, capacitados en inteligencia abierta, ciberseguridad, psicología militar y gestión de narrativas. Asimismo, la cooperación con universidades y centros de innovación permitirá desarrollar herramientas nacionales de análisis de redes, simulación de escenarios cognitivos y detección de desinformación. Golbeck (2015) enfatiza que la comprensión del comportamiento digital “es condición para la defensa efectiva en el ciberespacio social” (p. 131).⁵⁶

Finalmente, en el largo plazo, la consolidación del modelo operativo informacional argentino dependerá de la creación de una cultura de defensa informacional, basada en la coordinación interagencial y en la conciencia social del valor estratégico de la información. De Spiegeleire et al. (2017) advierten que “la resiliencia cognitiva nacional es la nueva forma de disuasión” (p. 22). En el contexto latinoamericano, autores como Rojas (2021) y Soto (2019) coinciden en que la protección de la narrativa institucional es clave para mantener la estabilidad democrática frente a amenazas híbridas. La Argentina deberá, por tanto, avanzar hacia una doctrina conjunta que combine tecnología, ética y adaptabilidad, consolidando su presencia en el dominio informacional regional.⁵⁷

⁵⁶ El adiestramiento y la investigación aplicada constituyen los pilares del poder informacional nacional.

⁵⁷ La defensa de la narrativa nacional constituye una forma moderna de soberanía.

CONCLUSIONES GENERALES

El desarrollo de la presente investigación permitió comprobar que las redes sociales han adquirido una función determinante dentro de las OI, especialmente en el nivel operacional, donde su empleo puede modificar la correlación de fuerzas sin recurrir a la acción cinética. El caso analizado evidenció que el dominio informacional constituye un espacio de confrontación continua, en el cual los Estados buscan controlar percepciones, desorganizar la cohesión del adversario y sostener su propia legitimidad. Esta constatación permitió validar plenamente la hipótesis inicial: el empleo planificado de redes sociales influye de manera directa sobre la eficacia de las operaciones conjuntas, al integrarse como herramienta de inteligencia, influencia y coordinación narrativa en el campo de batalla cognitivo.

El análisis doctrinario comparado confirmó que tanto las potencias occidentales (Estados Unidos, OTAN, Reino Unido) como los marcos doctrinarios emergentes (Rusia, China) conciben la información como un instrumento de poder operacional. Las aportaciones de autores como Omand (2020), Rid (2020), Kello (2017), Panarin (2006) y Komov (2012) demostraron que el dominio informacional se ha transformado en una capacidad multidimensional que combina comunicación estratégica, ciberdefensa e inteligencia psicológica. El caso ucraniano ilustró, de modo paradigmático, la transición hacia una guerra cognitiva, donde las redes sociales funcionaron como multiplicadores de influencia, vectores de legitimación política y plataformas de articulación entre fuerzas militares, sociedad civil y audiencias internacionales. La investigación verificó que el poder informacional no reside en la cantidad de datos disponibles, sino en la velocidad, coherencia y credibilidad con que estos se emplean para generar efectos en la mente del adversario.

Desde la perspectiva argentina, se concluyó que las Fuerzas Armadas deben avanzar hacia una doctrina nacional del dominio informacional que formalice la integración de las redes sociales dentro del planeamiento conjunto. La creación de un Comando Conjunto de Operaciones Informacionales (CCOINF) permitiría centralizar la planificación y conducción de las OI, fortalecer la coordinación interagencial y consolidar la protección de la narrativa institucional. También, la investigación confirmó la necesidad de incorporar la dimensión ética y jurídica al empleo informacional, garantizando que las operaciones digitales se conduzcan bajo principios de legitimidad, proporcionalidad y transparencia. La profesionalización del personal militar en inteligencia abierta, ciberdefensa y comunicación estratégica resultó

identificada como condición indispensable para alcanzar la madurez doctrinaria en este nuevo dominio de la guerra.

Asimismo, se identificó que la profesionalización del personal militar, si bien indispensable, no resulta suficiente sin una articulación estrecha con actores civiles. En un ecosistema comunicacional dominado por influencers, creadores de contenido y comunidades digitales con agendas propias, se vuelve necesario establecer mecanismos de coordinación y orientación mediante herramientas normativas flexibles —como un Manual de Buenas Prácticas de Comunicación Social en Ambientes Digitales— que definan márgenes claros de conducta, estilo y oportunidades narrativas, sin imponer criterios taxativos ni coartar la libertad de expresión. Este instrumento permitiría orientar la acción de quienes poseen capacidad real de influencia, alineándolos con los objetivos informacionales nacionales y evitando que sus intereses individuales interfieran en la coherencia de la campaña. En tal sentido, la figura del community manager institucional del Comando Conjunto de Operaciones Informacionales se proyecta como la autoridad técnica responsable de convocarlos, capacitarlos, coordinar su desempeño y dirigirlos con profesionalismo, generando una red civil-militar de comunicadores estratégicos capaz de actuar de manera sincronizada, ética y eficaz en apoyo a la maniobra informacional conjunta.

Finalmente, se concluyó que el futuro de la acción militar conjunta también dependerá de la capacidad nacional para proyectar poder informacional y defender la soberanía cognitiva del Estado. La integración doctrinaria de las redes sociales en el nivel operacional permitirá a la Argentina adaptarse a los nuevos escenarios de conflicto híbrido y a las formas emergentes de disuasión no cinética. Como señalaron Moresi et al. (2023), “la defensa del siglo XXI se libra en la mente tanto como en el terreno” (p. 198). Por ello, el desafío final radica en consolidar una cultura de defensa informacional que articule tecnología, doctrina, ética y conciencia nacional. La información —administrada con rigor profesional— debe concebirse no solo como un recurso, sino como una capacidad estratégica y operacional integral destinada a preservar la libertad de acción, la legitimidad institucional y la estabilidad democrática de la Nación.

BIBLIOGRAFÍA

- Access Now . (2022). *Digital Rights in Occupied Ukraine*.
- Army, D. o. (2003). *FM 3 - 13 Information Operations*. Washington: Army of EE. UU.
- Arquilla, J. &. (1993). *Cyberwar is coming!* California: RAND Corporation.
- Arquilla, J. &. (1999). *The Advent of Netwar*. California: RAND Corporation.
- Atlantic Council. (2022). *Russia's Global Disinformation Ecosystem*.
- Bellingcat. (2022–2024). *War Crime Investigations*.
- Brasileiro, E. (2020). *Manual de Operações de Informação*. Brasília: Estado-Maior do Exército.
- CCDCOE, N. (2022). *Cyber Operations in the Ukraine Conflict: Preliminary Analysis*. Tallin: Cooperative Cyber Defence Centre of Excellence.
- Chile, M. d. (2014). *Operaciones de Información*. Santiago de Chile: Ministerio de Defensa Nacional de Chile.
- COE, N. S. (2016). *Analysis of Russia's Information Campaign against Ukraine*. Riga, Letonia: NATO Centre of Excellence for Strategic Communications.
- COE, N. S. (2022). *Russia's Information Warfare in the Ukraine Conflict*. Riga. Letonia: NATO Centre of Excellence for Strategic Communications.
- Coelho, C. F. (2019). *Segurança da Informação e Redes Sociais no Contexto Militar Brasileiro*. Brasil.
- Corporation, R. (2020). *The firehose of falsehood: Russian propaganda and disinformation in the 21st century*. Santa Monica, CA: RAND Corporation.
- Corporation, R. (2020). *The Role of Social Medium Military Operations*. Santa Monica, CA: RAND Corporation.
- Corporation, R. (2021). *The Role of Information in Twenty-First-Century Warfare*. Santa Monica, CA: RAND Project AIR FORCE. Obtenido de https://www.rand.org/pubs/research_reports/RRA379-1.html
- Corporation, R. (2022). *Countering Russian Information Operations in Ukraine*. Santa Monica, CA: RAND Project AIR FORCE.
- DataReportal. (2024). *Digital 2024 Global Overview Report*. San Francisco, California: We Are Social & Meltwater.
- De Spiegeleire, S. S. (2017). *The rise of cyber-subversion: Global strategic trends and implications*. Den Haag, Países Bajos: The Hague Centre for Strategic Studies.
- Ejército Argentino. (2015). *ROB 00-01 Comunicación Social Aplicativa al Combate (COSACO)*. Argentina.
- Estado Mayor Conjunto de las Fuerzas Armadas. (s.f.). *Glosario de Términos para la Acción Militar Conjunta (PC 00 02) 2023*. Buenos Aires: Ministerio de Defensa.
- Excellence, C. o. (2020). *The Speed of Influence*. Riga, Latvia: NATO Strategic Communications.

- Excellence, N. S. (2015). *Analysis of Russia's Information Campaign Against Ukraine*. Riga: NATO Strat Com COE.
- Excellence, N. S. (2021). *Social media as a tool of hybrid warfare*. Riga, Letonia: NATO StratCom COE.
- Frontiers in Psychology. (2023). *Zelenskyy's leadership and emotional influence through social media*.
- García-Pelayo, C. v. (2002). *De la guerra*. Buenos Aires: Editorial Libertador.
- General Gerasimov, V. V. (27 de Febrero de 2013). Ценность науки в предвидении [El valor de la ciencia en la previsión]. *Voyenno-Promyshlenny Kuryer (Военно-промышленный курьер, abreviado VPK)*., edición n.º 8(476).
- Golbeck, J. (2015). *Introduction to Social Media Investigation: a Hands-on Approach*. United States: Syngress Media.
- Gonzalez, M. L. (2016). *El uso de las Redes Sociales en la Estrategia Militar Argentina*. Buenos Aires.
- Gouliev, Z. (2025). *NLP Analysis of Twitter*. Obtenido de propaganda.ArXiv.org
- Iskoujina, Z. G. (2024). *Social media as an information warfare tool*. New Media & Society.
- Kello, L. (2017). *The Virtual Weapon and International Order*. New Haven, Connecticut: Yale University Press.
- Kiev, C. p. (2020). *Information Defense Policy of Ukraine*. Kiev: CAPD Press.
- Komov, S. (2012). *Dukhovnye aspekty informatsionnoy voyny [Aspectos espirituales de la guerra de la información]*. Moscú: Academia de Ciencias Militares.
- Lab, A. C. (2023). *War in the Digital Domain: Ukraine and the New Front of Information Operations*. Washington D. C.: Atlantic Council.
- Laboratory, D. F. (2023). *War in the Digital Domain: Ukraine and the New Front of Information Operations*. Washington D. C.: Atlantic Council.
- Lupu, N., Ramirez Bustamante, M. V., & Zechmeister, E. J. (2020). Social media disruption: Messaging mistrust in Latin America. (J. H. Press, Ed.) *Journal of Democracy*, 31(3), 160-171. Obtenido de <https://doi.org/10.1353/jod.2020.0043>
- Marañón, A. (14 de July de 2023). How have information operations affected the integrity of democratic elections in Latin America? *Lawfare*. Obtenido de https://www.lawfaremedia.org/article/how-have-information-operations-affected-integrity-democratic-elections-latin-america?utm_source=chatgpt.com
- Mitchelstein, E. (2020). Social media and democracy in Latin America. *Social Media + Society (Vol. 6 n° 4)*, 1-12. Obtenido de <https://doi.org/10.1177/2056305120984452>
- Moresi Alejandro et al. (2023). *Operaciones en el ambiente de la información*. Buenos Aires: Estado Mayor Conjunto de las Fuerzas Armadas.
- Omand David, P. M. (2018). *Principled Pying: The Ethics of Secret Intelligence*. Oxford Inglaterra: Oxford University Press.

- Omand, D. (2020). *How Spies Think: Ten Lessons in Intelligence*. Londres: Penguin Books.
- Panarin, I. (2006). *Informatsionnaya voyna i geopolitika [La guerra de la información y la geopolítica]*. Moscú: GEKS Publisher.
- Panarin, I. (2011). *La guerra de la información y la geopolítica*. Moscú: MGIMO.
- R., F. (2018). *Ciberseguridad y Redes Sociales en el Contexto Militar Argentino*. Buenos Aires.
- RAND Corporation (Schwille, M. e. (2021). *Handbook for Tactical Operations in the Information Environment*. Santa Monica, California: RAND Corporation.
- RAND, Corporation. (2023). *Ukrainian Resilience to Russian Disinformation*. EE. UU.
- Rissoan, R. (2011). *La redes sociales: Facebook, Twitter, LinkedIn, Viadeo en el mundo profesional*. Madrid: ENI.
- Rojas, H. (2021). *Operaciones de información y contención social en América Latina*. Santiago de Chile: Instituto de Estudios Estratégicos de la Defensa Nacional.
- Soto, M. F. (2019). *La Influencia de las Redes Sociales en las Operaciones*. Santiago de Chile, Chile.
- Staff, C. o. (2017). *Septima Función Militar*. Estados Unidos: Departamento de Defensa de los Estados Unidos.
- Staff, U. J. (2018). *Joint Publication 3-13: Information Operations*. Washington, D.C.: Department of Defense.
- The Washington Post. (2023). Ukrainian Digital Resistance.
- Thomas, R. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Nueva York: Farrar, Straus and Giroux.
- Thomas, R. (2020). *Desinformación: La guerra política moderna*. Londres: Hurst & Company.
- Thornton, R. (2015). The Changing Nature of Modern Warfare: Responding to Hybrid Threats. *The RUSI Journal*, vol. 160, n.º 5, 214.
- Tzu, S. (2003). *El arte de la guerra, traducción de Thomas Cleary*. Madrid: Alianza Editorial.
- U.S., D. o. (1998). *Joint Publications 3-13: Information Operations*. Estados Unidos.
- U.S., D. o. (2012). *Joint Publication 3 - 13 Information Operations*. Estados Unidos.
- U.S., D. o. (2014). *Joint Publication 3 - 13: Information Operations*. Estados Unidos.
- U.S., D. o. (2022). *Information in Joint Operations*. Estados Unidos.
- Vallejos, G. (2018). La Doctrina Gerasimov vs las operaciones de Información: Inteligencia en primera línea. *Instituto Internacional de Estudios en Seguridad Global*, 4-12.
- Vallejos, G. D. (2018). La guerra de la información: Operaciones de información y operaciones de influencia. *Revista Visión Conjunta / ESGC*.
- Vallejos, G. D. (2024). Operaciones de bandera falsa y desinformación en el ciberespacio. *Visión Conjunta (31)*, 54-67.

Anexo 1

ANÁLISIS FUCAME DEL EMPLEO DE REDES SOCIALES EN EL CONFLICTO

1. Introducción

El presente anexo desarrolla un análisis comparado del empleo de las principales plataformas digitales utilizadas durante el conflicto ruso-ucraniano, aplicando la metodología FUCAME (Fuente, Unidad, Contexto, Audiencia, Medio y Efecto), de uso extendido en el análisis de propaganda y operaciones psicológicas contemporáneas (Vallejos, 2018). En el marco de las OI, las redes sociales funcionaron como vectores de influencia en la dimensión cognitiva, complementando acciones cibernéticas, psicológicas y mediáticas descritas por la doctrina occidental y rusa (Moresi et al., 2023; Vallejos, 2018).

En este contexto, el método FUCAME permite describir de manera sistemática cómo cada red social fue explotada por los distintos actores para producir efectos en el nivel operacional, afectando la moral de combate, la legitimidad internacional y la cohesión social del adversario, en línea con la concepción de la información como función conjunta y como factor de poder (JP 3-13, 2012; Omand, 2020).

2. El método FUCAME

Se estructura en seis componentes:

- **Fuente** (¿Quién habla?)
Corresponde al emisor del mensaje: actor estatal, organismo militar, agencia de inteligencia, medio estatal, grupo de trolls, bot automatizado, influencer o cuenta civil. La identificación de la fuente es esencial para evaluar credibilidad, capacidad de coordinación y alineamiento con objetivos estratégicos (NATO StratCom COE, 2016; Vallejos, 2018).
- **Unidad** (Contenido) (¿Qué dice?)
Refiere al mensaje concreto: texto, imagen, video, meme, mapa, consignas, hashtags o narrativas marco (Rid, 2020). El análisis se centra en los temas recurrentes, en las emociones invocadas (miedo, orgullo, odio, heroísmo) y en el grado de alineamiento con los objetivos de la campaña informativa.

- **Contexto** (¿Cuándo / dónde?)
Considera la situación en que el mensaje es emitido: ofensiva o retroceso militar, sanciones económicas, votaciones en organismos internacionales, ataques a infraestructuras críticas, crisis de refugiados, entre otros (RAND, 2021). El mismo contenido puede producir efectos distintos si se inserta en un contexto de éxito o fracaso operacional.
- **Audiencia** (¿A quién?)
Identifica el público objetivo: tropas propias, combatientes enemigos, población civil, minorías étnicas, opinión pública internacional, aliados, indecisos, etc. La doctrina de OI insiste en segmentar audiencias y adaptar mensajes a perfiles específicos dentro de la dimensión cognitiva (JP 3-13, 2012; Moresi et al., 2023).
- **Medio** (¿Por dónde?)
Define el canal o plataforma de difusión: Telegram, Twitter/X, Facebook, TikTok, YouTube, VKontakte, Odnoklassniki, entre otros. Cada medio tiene lógicas algorítmicas, alcances y estilos comunicacionales diferenciados, por lo que su selección es una decisión operacional, no meramente técnica (RAND, 2021).
- **Efecto** (¿Para qué?)
Analiza el impacto buscado y el logrado: desmoralizar, desorganizar, cohesionar, intimidar, movilizar apoyos externos o saturar el espacio informacional. En términos operacionales, los efectos se vinculan con la alteración de la voluntad, la comprensión o las capacidades del adversario (Moresi et al., 2023; Omand, 2020).

La combinación de estos seis elementos permite reconstruir campañas de información completas, identificar patrones de coordinación entre actores y evaluar la integración entre OI, operaciones cibernéticas y acciones cinéticas, tal como se observa en el caso ruso-ucraniano (NATO StratCom COE, 2016; Atlantic Council DFRLab, 2023).

3. Análisis FUCAME por redes sociales

A continuación, se presenta un análisis sintético de dos plataformas, destacando el empleo realizado por Rusia y Ucrania. El objetivo es ofrecer un esquema de lectura operacional que pueda ser replicado en otros conflictos.

Elemento	Empleo ruso	Empleo ucraniano
Fuente	Ministerio de Defensa, canales prorrusos, bloggers militares vinculados a estructuras estatales y grupos armados	Oficina de Comunicación Estratégica del Ministerio de Defensa, Fuerzas Armadas, unidades tácticas, OSINT voluntaria
Unidad	Reportes de “éxitos” rusos, mapas manipulados, justificativos ideológicos, amenazas y desinformación sobre avances	Comunicados operacionales verificados, imágenes de resistencia, destrucción de material enemigo, advertencias a la población
Contexto	Ofensivas en Donbás, anexiones, ataques a infraestructuras	Defensa de Kiev, contraofensivas regionales, ataques de misiles
Audiencia	Población rusa, combatientes separatistas, simpatizantes externos	Ciudadanía ucraniana, fuerzas propias, aliados y diáspora
Medio	Canales de alto número de suscriptores y redes de reenvío coordinado	Canales oficiales verificados y canales de unidades identificadas
Efecto	Intimidación, construcción de sensación de inevitabilidad de la victoria, saturación de la narrativa oficial rusa	Refuerzo de la resiliencia, confianza en las fuerzas armadas, legitimación internacional de la defensa ucraniana

Figura 9 - FUCAME de la plataforma Telegram.⁵⁸

Elemento	Empleo ruso	Empleo ucraniano
Fuente	Medios estatales, canales de análisis afines al Kremlin	Ministerio de Defensa, documentalistas independientes, OSINT
Unidad	Documentales justificando la operación militar, revisionismo histórico, debates sesgados	Evidencia audiovisual de crímenes de guerra, explicaciones de operaciones, conferencias de prensa
Contexto	Anexiones, debates sobre legitimidad de la operación	Liberación de localidades, hallazgo de fosas y destrucción de infraestructuras
Audiencia	Público global interesado en análisis “en profundidad”	Opinión pública informada, medios y analistas
Medio	Videos largos, producciones con estética de noticiero	Series documentales breves, piezas explicativas
Efecto	Búsqueda de legitimidad histórica e intelectual	Consolidación de la percepción de víctima y reforzamiento del apoyo internacional

Figura 10 - FUCAME de la plataforma You Tube.⁵⁹

⁵⁸ Principal plataforma de guerra en tiempo real en el teatro ucraniano, gracias a sus canales masivos, reenvío rápido de contenidos y relativa tolerancia al anonimato (Atlantic Council DFRLab, 2023; RAND, 2021).

⁵⁹ Fue el espacio para narrativas de mayor profundidad, documentales y análisis extensos. (RAND, 2021; Vallejos, 2018).

Anexo 2

TIPOLOGÍA DOCTRINARIA Y ANÁLISIS OPERACIONAL DE REDES SOCIALES EN LAS OPERACIONES DE INFORMACIÓN CONJUNTAS

Las redes sociales han pasado de ser simples espacios de interacción civil a convertirse en plataformas de maniobra informacional en los conflictos contemporáneos.⁶⁰ Su potencial radica en la capacidad de amplificar mensajes, segmentar audiencias y generar reacciones emocionales inmediatas, lo que las convierte en instrumentos estratégicos en el nivel operacional. Según la RAND Corporation (2022), “las redes sociales constituyen el sistema nervioso de la guerra informacional moderna” (p. 24). Estas plataformas permiten simultáneamente recolectar inteligencia, diseminar narrativas y coordinar acciones psicológicas.⁶¹

Desde un enfoque doctrinario, las **OI** desarrolladas en redes sociales se clasifican en tres categorías funcionales:

1. **Ofensivas de influencia**, orientadas a degradar la moral del adversario, alterar su percepción o dividir su cohesión social.
2. **Defensivas informacionales**, destinadas a proteger la narrativa nacional y contrarrestar la desinformación.
3. **De apoyo a la maniobra**, que emplean redes para coordinar fuerzas, difundir información institucional o recabar datos en tiempo real.

Red Social	Usuarios activos (millones)	Grupo etario predominante	Facilidades Operacionales	Aplicabilidad doctrinaria
Facebook	2.960	25-54 años	Gran alcance global, permite segmentar audiencias y construir comunidades.	Difusión institucional, campañas de legitimación y monitoreo social.
Twitter / X	556	18-44 años	Alta velocidad y viralidad, ideal para comunicación	Difusión de mensajes operacionales,

⁶⁰ Moresi (2023) sostiene que “la maniobra informacional eficaz depende de la selección adecuada del canal digital y del conocimiento de su público objetivo” (p. 184). Este principio justifica el análisis comparativo de las principales plataformas utilizadas en el ámbito operacional contemporáneo.

⁶¹ El valor operacional de las redes sociales reside en su doble uso: herramienta de influencia y sensor del entorno cognitivo.

			estratégica y propaganda inmediata.	contranarrativas y crisis informativas.
Instagram	2.000	18–34 años	Comunicación visual, alta emotividad, fuerte impacto en públicos jóvenes.	Proyección de imagen institucional y campañas psicológicas positivas.
TikTok	1.560	16–30 años	Formato breve y creativo, permite manipular emociones y narrativas mediante audiovisual.	Operaciones de influencia cognitiva, propaganda emocional, detección de tendencias.
Telegram	800	20–45 años	Grupos cerrados, anonimato y velocidad de difusión.	Canal de mando informacional (Rusia) y comunicación de resistencia (Ucrania).
YouTube	2.500	18–49 años	Larga permanencia, contenido audiovisual extenso y educativo.	Campañas de legitimación, propaganda estratégica y documentación informativa

Figura 11 - Principales redes sociales empleadas en el dominio informacional (Datos estimativos, fuente: DataReportal 2024; NATO StratCom COE 2023; RAND 2022)

Cada plataforma presenta ventajas y vulnerabilidades distintas. Facebook y YouTube son útiles para campañas de legitimación institucional y control narrativo a gran escala; Twitter/X destaca por su rapidez, pero es altamente volátil y sensible a la manipulación algorítmica; TikTok posee el mayor impacto emocional sobre públicos jóvenes, aunque su control extranjero genera riesgo de seguridad; Telegram ofrece anonimato y control de grupos cerrados, lo que lo convierte en herramienta predilecta de operaciones rusas; LinkedIn, aunque menos masiva, es relevante para influir en comunidades profesionales y decisores. Según Golbeck (2015), “cada red social constituye un ecosistema conductual donde las percepciones pueden ser modeladas a través de micro-interacciones” (p. 128).⁶²

El análisis comparado permite concluir que la efectividad operacional del empleo de redes sociales depende de tres factores:

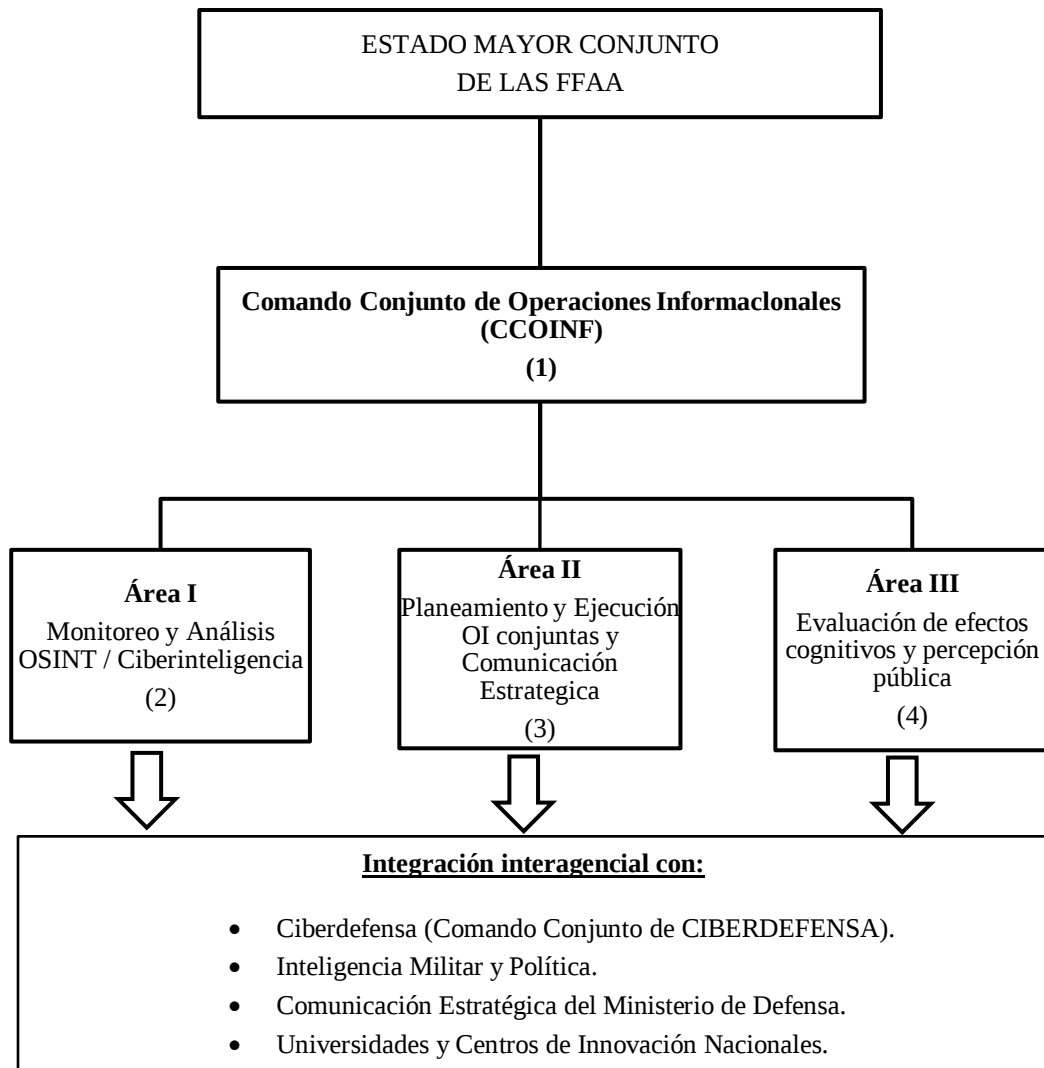
⁶² El dominio informacional requiere conocer la naturaleza y psicología de cada red social, adaptando el mensaje al público y la plataforma.

- a) la **selección del canal** según el público objetivo y el contexto cultural.
- b) la **coherencia narrativa** con los objetivos estratégicos.
- c) la **capacidad de sincronización interagencial** (militar, política, civil y tecnológica).

En el plano nacional, esta tipología ofrece una base para la futura doctrina argentina de Operaciones Informacionales Conjuntas, integrando medios civiles y militares bajo conducción conjunta. Como advierte De Spiegeleire, Skinner y Sweijs (2017), “la superioridad informacional no proviene de la cantidad de mensajes, sino de la coherencia y credibilidad con que son ejecutados” (p. 21).

Anexo 3

DISEÑO ACADÉMICO COMANDO CONJUNTO DE OPERACIONES INFORMACIONALES



(1) Con facultades para planificar y conducir acciones en el dominio informacional.

(2) Orientado a detectar narrativas hostiles y evaluar vulnerabilidades cognitivas.

(3) Incluyendo comunicación estratégica, contra información y campañas digitales.

(4) Con indicadores medibles de influencia y cohesión social.