ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TÍTULO: IMPACTOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN ANTE UNA AMENAZA HÍBRIDA EN LA QUE DEBA ACTUAR EL INSTRUMENTO MILITAR.

AUTOR: MY I JUAN ESTEBAN PEDERNERA.

TUTOR: CR (R) “VGM” EDUARDO LUIS DOVAL.

AÑO: 2025.

1. RESUMEN

El presente Trabajo Final Integrador aborda una línea de investigación que articula dos dimensiones centrales de los conflictos contemporáneos, las Tecnologías de la Información y la Comunicación y la guerra híbrida. Ambas han demostrado poseer un impacto decisivo en la configuración, conducción y resolución de los conflictos armados del siglo XXI, modificando de manera sustancial la forma en que los Estados emplean el poder militar y otros instrumentos del poder nacional. Lejos de constituir fenómenos aislados, las Tecnologías de la Información y la Comunicación y la guerra híbrida constituyen en la actualidad un binomio inseparable, cuya comprensión resulta indispensable para el planeamiento, la conducción y la adaptación del Instrumento Militar frente a amenazas sumamente complejas, multidimensionales y signadas por un constante dinamismo.

En primer lugar, las TIC han experimentado en las últimas décadas un desarrollo exponencial que ha permitido su progresiva inserción efectiva en todos los ámbitos de la actividad humana, introduciéndose de manera notoria en los diferentes conflictos armados del siglo XXI.

En segundo lugar, el concepto de guerra híbrida, cuya conceptualización no posee aún una definición única y consensuada, ha surgido como una concepción analítica destinada a explicar la convergencia de tácticas, técnicas y procedimientos convencionales y no convencionales, integrados en un mismo teatro de operaciones.

La articulación entre TIC y guerra híbrida constituye, por lo tanto, un factor determinante para el análisis de conflictos recientes como Afganistán, Iraq y la guerra entre Rusia y Ucrania. Estos casos, ampliamente documentados y estudiados por la doctrina occidental, permiten observar cómo las TIC han consolidado su función como multiplicador de fuerzas, facilitando la difusión de propaganda, el reclutamiento virtual, la comunicación efectiva, la obtención de inteligencia a partir de fuentes abiertas, la manipulación de la información y el desarrollo de capacidades en el ciberespacio.

El objetivo general de este trabajo consiste en extraer aprendizajes derivados del empleo de las TIC en las guerras híbridas recientes, con el fin de identificar qué elementos podrían ser utilizados por las Fuerzas Armadas argentinas para neutralizar amenazas futuras y aprovechar oportunidades en un eventual escenario híbrido.

Finalmente, los resultados esperados permitirán no solo contribuir al campo disciplinar de la conducción operacional, sino también aportar elementos conceptuales y prácticos que fortalezcan el pensamiento estratégico militar argentino.

1.1. Palabras clave

Tecnologías de la información y la comunicación - Guerra híbrida - Amenaza híbrida - Conflictos armados - Amenazas y oportunidades - Impactos - Pensamiento estratégico.

CONTENIDOS

1. RESUMEN I

1.1. Palabras clave II

2. INTRODUCCIÓN 1

3. CAPÍTULO I: LA AMENAZA HÍBRIDA EN EL SIGLO XXI 9

3.1. Conceptualización de la amenaza híbrida 9

3.2. Comparación doctrinaria entre Occidente y Oriente 16

3.3. Análisis comparado de casos: Afganistán, Iraq y Rusia-Ucrania 18

4. CAPÍTULO II: IMPACTOS DE LAS TIC EN EL INSTRUMENTO MILITAR FRENTE A AMENAZAS HÍBRIDAS 23

4.1. Vulnerabilidades del Instrumento Militar potenciadas por las TIC 23

4.2. Oportunidades generadas por las TIC para el Instrumento Militar 26

4.3. Requerimientos para la adaptación del Instrumento Militar 26

4.4. Capacidades necesarias para operar en escenarios híbridos 27

5. CONCLUSIONES 31

6. BIBLIOGRAFÍA 37

2. INTRODUCCIÓN

En las últimas décadas, el acelerado desarrollo de las Tecnologías de la Información y la Comunicación (TIC) ha transformado significativamente la naturaleza de los conflictos armados, generando un entorno operacional caracterizado por la superposición de acciones militares, políticas, económicas, psicológicas y tecnológicas.

Este entorno, propio de la denominada guerra híbrida, redefine los límites clásicos entre paz y conflicto, obliga a los Estados a replantear sus sistemas tradicionales de defensa y a incorporar nuevas capacidades orientadas al dominio de la información, la superioridad cognitiva y la protección de infraestructuras críticas.

Las TIC han alterado no solo la velocidad de transmisión y el caudal de la información, sino también la forma en que los actores estatales y no estatales emplean este recurso para alcanzar objetivos estratégicos. La capacidad de manipular la información, vulnerar infraestructuras críticas, operar en el ciberespacio, interferir en procesos decisorios y erosionar la cohesión y el orden social constituye un instrumento táctico y operacional de considerable impacto.

Para los Estados, esto supone un escenario en el que la seguridad nacional ya no depende exclusivamente de las capacidades militares, sino también de su habilidad para gestionar, proteger y emplear información en entornos cada vez más complejos, volátiles e inciertos.

La proliferación de las mencionadas TIC abrió el camino a nuevas modalidades de confrontación que desafían las estructuras clásicas de la guerra. Una de las expresiones más visibles de esta transformación es la llamada “guerra híbrida”, un tipo de conflicto que combina la acción militar convencional con tácticas irregulares, acciones cinéticas y no cinéticas, operaciones encubiertas, campañas de desinformación, operaciones psicológicas, ciberoperaciones, manipulación de redes sociales y de otros medios de comunicación masiva, tensiones sociales y económicas, y el empleo estratégico de actores no estatales.

La característica distintiva de este tipo de guerra es su capacidad para operar deliberadamente en espacios grises, donde las fronteras entre paz y conflicto se desdibujan y donde la atribución de responsabilidades se vuelve difusa. Galeotti (2016), Hammes (2004), Hoffman (2007) y Locatelli (2019) sostienen que este tipo de enfrentamiento busca erosionar

las capacidades del adversario sin desencadenar una acción militar directa y abierta, aprovechando vulnerabilidades institucionales, socioeconómicas, tecnológicas e informacionales.

Resulta indispensable reconocer que, en el contexto de una amenaza híbrida, el campo de batalla excede lo físico y adquiere una dimensión principalmente informacional y cognitiva. También implica aceptar que la velocidad en la transmisión de la información, la diversidad de actores autónomos en el ciberespacio y la capacidad de manipulación requieren una adaptación profunda del Instrumento Militar, tanto en su estructura como en su cultura organizacional.

En este marco, el Instrumento Militar adquiere un rol protagónico, no sólo como brazo brazo armado de una nación, sino como actor estratégico capaz de operar, disuadir y responder en escenarios multidimensionales donde la información se convierte en un recurso decisivo de poder para un Estado. Esta transformación en la concepción del Instrumento Militar exige un cambio en el pensamiento estratégico, la revisión de doctrinas, la capacitación del personal para actuar en los nuevos escenarios y la configuración de estructuras capaces de actuar eficazmente frente a amenazas cambiantes, a partir de la incorporación de nuevas tecnologías.

La literatura estratégica contemporánea coincide en que la guerra ha experimentado una profunda transformación en las últimas décadas. Según diversos autores, el conflicto moderno ya no puede entenderse exclusivamente desde la perspectiva militar tradicional, dado que incorpora dimensiones políticas, económicas, tecnológicas, informacionales y sociales que interactúan simultáneamente.

Autores como Martin van Creveld (1991) y Mary Kaldor (2012) señalaron de manera anticipada que la guerra del siglo XXI estaría marcada por la disminución del monopolio estatal del uso de la fuerza, la proliferación de actores no estatales y la creciente importancia de la información como recurso estratégico. Esta visión coincide con lo expuesto en el Doctrina Básica para la Acción Militar Conjunta (EMCFFAA, 2023), donde se reconoce que el entorno operacional contemporáneo es multidimensional e interagencial.

El concepto “guerra híbrida” se consolidó a partir de los estudios de Frank Hoffman (2007), quien la definió como un tipo de conflicto que integra de manera sinérgica

capacidades convencionales, tácticas irregulares, terrorismo, crimen organizado, operaciones encubiertas, ciberataques y campañas de desinformación. Posteriormente, Michael Galeotti (2016) y Thomas Rid (2020) ampliaron el concepto al incorporar el uso estratégico de la manipulación informativa, las operaciones psicológicas y la explotación de vulnerabilidades sociales y políticas del adversario.

Olguín Noriega (2014), en su trabajo de investigación *"Organización del campo de batalla en el contexto de guerras híbridas"* al momento de referirse a esta nueva forma de librar la guerra, ha hecho hincapié en los diferentes actores que se encuentran envueltos en dichos conflictos armados, resaltando la existencia de tres tipos de fuerzas. En primer lugar, las fuerzas regulares que ejecutan operaciones convencionales empleando medios también convencionales; en segundo lugar, las fuerzas irregulares tales como insurgentes, terroristas y guerrilleros que desarrollan acciones de terrorismo, emboscadas, guerra de información, entre otras; y por último las fuerzas criminales que realizan actividades de apoyo a través del tráfico de armas, de drogas, de personas y lavado de dinero.

Por su parte, Korybko (2015) ha definido en su obra *"Guerras híbridas. De las revoluciones de colores a los golpes"* el concepto de guerra híbrida entendido como la combinación de la utilización de herramientas de propaganda y estudios psicológicos combinados con el empleo de redes sociales (denominado por el autor como golpe suave) para desestabilizar gobiernos y crear conflictos internos, y la ejecución de una guerra no convencional llevada a cabo por fuerzas irregulares para, en caso de no ser suficiente el golpe suave, ejecutar un golpe duro que permita derribar y sustituir al gobierno.

La doctrina conjunta reconoce que el Instrumento Militar debe ser capaz de operar no solo en el dominio físico, sino también en los dominios cognitivo, informacional y cibernético. El trabajo elaborado por Casale (2022) enfatiza que la eficacia del accionar militar depende de la capacidad para influir en la voluntad del adversario, controlar la información disponible y proteger los sistemas propios.

En el marco de una amenaza híbrida, el Instrumento Militar debe detectar operaciones de manipulación de la información, dar respuestas efectivas ante ciberataques, coordinar acciones con otros organismos del Estado, sostener la legitimidad de las operaciones, y anticipar o prevenir efectos negativos en el dominio cognitivo.

En cuanto a las Tecnologías de la Información y la Comunicación existen diversas investigaciones. Todos ellas, independientemente del enfoque en que sean abordadas, hacen referencia a los avances tecnológicos de los últimos años y a cómo estos, se han insertado en las diferentes herramientas que se emplean en los conflictos actuales.

A su vez, hacen hincapié en la importancia que revista la aplicación de tales tecnologías en los conflictos modernos. En tal sentido, un trabajo acerca de las nuevas tecnologías en la guerra y la sorpresa (Etcheverry, 2019) ha descripto que la evolución tecnológica es lo que ha ido caracterizando la forma de hacer la guerra, obligando a quienes la aplican a adaptar sus modos para lograr la victoria.

Locatelli (2019), al referirse a los rasgos distintivos que se presentan en un conflicto híbrido, resalta la idea que el adecuado y oportuno manejo de los medios de comunicación, provoca que las acciones se diseminen con una notable inmediatez, logrando con ello influenciar rápidamente en las mentes de las personas.

En el año 2020 un trabajo sobre el impacto de la comunicación social en la toma de decisiones del nivel operacional (Castro) ha reflejado que los cambios tecnológicos han producido nuevas formas de cobertura de los medios de comunicación durante los conflictos armados, moldeando la percepción de la opinión pública.

El proceso de digitalización global ha convertido a la información en un recurso de poder fundamental para los Estados. De acuerdo con Nye (2004), el poder informacional constituye una forma de influencia capaz de modelar percepciones, modificar conductas y orientar decisiones sin recurrir al uso directo de la fuerza.

La importancia de las TIC no radica exclusivamente en su función instrumental, sino en su capacidad para alterar la posición relativa de los actores dentro del sistema internacional, incrementando la vulnerabilidad de las sociedades y exponiendo las infraestructuras críticas a un espectro creciente de amenazas.

Las Tecnologías de la Información y la Comunicación poseen atributos que las tornan especialmente relevantes en entornos híbridos. Estos son: velocidad, que permite actuar ante el adversario en lugar de verse obligado a reaccionar; masividad, que posibilita influir sobre grandes audiencias; anonimato y no atribución, que dificulta la identificación del agresor;

equilibrio de poder, que facilita la intervención de actores no estatales en un conflicto; y efectos amplificados que pueden incrementarse en el ámbito cognitivo y social.

Estas características coinciden con los análisis efectuados por Casale (2022), donde señala que el dominio cibernético y el dominio informacional son espacios de creciente relevancia estratégica.

La intrínseca relación entre el concepto de guerra híbrida y las Tecnologías de la Información y la Comunicación es desarrollada explícitamente por Jorquera Escobar (2024) en su artículo *"Redes sociales y guerra híbrida, un desafío para la defensa"*, en el cual ha resaltado que las acciones que se llevan a cabo en un conflicto híbrido se centran en la ejecución de ciberataques, desinformación y propaganda, aprovechando los espacios generados por las TIC y las redes sociales, buscando influir en la opinión pública. A su vez, ha planteado que en muchas ocasiones las acciones de propaganda ofrecen información sesgada o manipulada, reflejando con ello una evidente intención de desinformar.

Podemos afirmar entonces, que la aplicación de las nuevas Tecnologías de la Información y la Comunicación en las guerras híbridas, cobran mayor relevancia conforme evoluciona la tecnología.

Cabe destacar, tal como fuera mencionado con anterioridad, que ambos conceptos se hallan profundamente arraigados en los conflictos recientes.

El análisis de una amenaza híbrida exige recurrir a marcos conceptuales amplios que integren diferentes instrumentos del poder nacional. Basándonos en la obra *"Estrategia"* de Liddell Hart (1967), la Gran Estrategia consiste en la coordinación de todos los recursos de un Estado, militares, económicos, diplomáticos, financieros, tecnológicos y morales, para alcanzar objetivos políticos de largo plazo.

Este enfoque se relaciona con los criterios expuestos en *"Los escritos académicos en la formación militar"* (2014), donde se destaca la articulación coherente de los niveles Estratégico Nacional, Estratégico Militar y Operacional.

La Estrategia Nacional define los objetivos de Seguridad y Defensa del Estado y orienta el empleo de los diferentes instrumentos del poder nacional. De acuerdo con la Doctrina Básica para la Acción Militar Conjunta (EMCFFAA, 2023), esta estrategia

determina los intereses vitales, establece prioridades y fija las líneas de acción necesarias para garantizar la supervivencia, la integridad territorial y la estabilidad institucional.

Dentro de este marco, las TIC se presentan como un componente transversal, puesto que afectan a todos los instrumentos del poder nacional y transforman la manera en que se planifican, comunican y ejecutan políticas de seguridad.

La Estrategia Militar traduce los objetivos nacionales en capacidades operacionales y modos de acción para el Instrumento Militar. Según la mencionada doctrina básica para la AMC (2023), este nivel estratégico debe adaptarse a la naturaleza cambiante del entorno operacional, incorporando nuevas tecnologías, fortaleciendo capacidades de ciberdefensa, desarrollando estructuras organizativas especializadas en operaciones de información y realizando una revisión de las doctrinas de empleo conjunto.

En escenarios híbridos, la Estrategia Militar debe incorporar: operaciones en el dominio informacional; protección y defensa de infraestructuras críticas; acciones psicológicas y acciones para contrarrestar campañas de desinformación; ciberoperaciones ofensivas, defensivas y de exploración; y coordinación interagencial e integración multidemensional.

En esta línea de pensamiento, Hoffman (2007) señala que las amenazas híbridas incorporan un amplio espectro de diferentes modos de hacer la guerra, incluyendo capacidades convencionales, tácticas irregulares, acciones terroristas y crimen organizado. Asimismo, resalta que el adversario híbrido busca explotar vulnerabilidades de su oponente, evitando la confrontación directa con fuerzas convencionales superiores. Esto define claramente que el adversario híbrido no se limita exclusivamente al enfrentamiento directo de la fuerza militar.

Ampliando el concepto vertido en el párrafo anterior, Galeotti (2016) destaca en su obra que la guerra en la que se encuentra inmerso Occidente no es una guerra de tipo clásico, sino que se trata de una mezcla entre lo militar y lo político, frecuentemente descripta como “guerra híbrida”.

Resulta importante señalar que la Estrategia Nacional define líneas de acción concretas en materia de Seguridad y Defensa, mientras que la Estrategia Militar debe

transformar dichos lineamientos en capacidades operacionales, estructuras organizacionales y doctrinas de empleo.

A su vez, el pensamiento estratégico militar debe enfocarse en comprender la complejidad de los escenarios actuales, identificar factores críticos, analizar problemas de manera integral y anticipar efectos adversos en el corto y mediano plazo.

El presente trabajo se centra en analizar los impactos de las tecnologías de la información y la comunicación ante una amenaza híbrida en la que deba actuar el instrumento militar, evaluando su incidencia en la toma de decisiones, en la conducción estratégica y en la eficacia operacional. El objetivo es identificar de qué manera las TIC condicionan el desarrollo del conflicto en el ámbito operacional, cuáles son las principales vulnerabilidades que pueden ser explotadas por un actor híbrido y qué capacidades debería desarrollar el Instrumento Militar para garantizar una respuesta adecuada, oportuna y coherente con la Estrategia Nacional.

Asimismo, este trabajo se propone contribuir a la formación profesional militar desde una perspectiva multidisciplinar. La comprensión del conflicto híbrido no puede limitarse a la dimensión técnica o tecnológica; requiere considerar aspectos políticos, psicológicos, sociales y comunicacionales. La incorporación de esta mirada abarcativa resulta esencial para la toma de decisiones en entornos complejos donde las percepciones, las narrativas y el constante flujo de información influyen de manera significativa en la legitimidad de las acciones adoptadas por un Estado y en la cohesión social de este.

Su naturaleza ambigua exige una comprensión interdisciplinaria del conflicto, el impacto de las TIC sobre la percepción pública, la legitimidad estatal, la cohesión social y la resiliencia institucional obliga a ampliar el análisis más allá del campo de batalla, abordando la dimensión estratégica de la información como factor determinante del poder nacional.

La estructura de este trabajo responde a una metodología descriptiva analítica. En su carácter descriptivo prescinde de hipótesis a corroborar ya que se pretende alcanzar el objetivo general de extraer enseñanzas del impacto de las TIC en las guerras híbridas. Dividida en dos capítulos. El primer capítulo caracteriza la amenaza híbrida, describiendo sus componentes tácticos y operacionales, y analizando conflictos que tuvieron lugar en el siglo XXI tales como Afganistán, Iraq y Rusia-Ucrania, analizando fuentes públicas, tales como:

Bing West, 2009; Baqués, 2015; Cordesman, 2006; Galeotti, 2016; Hammes, 2004; Hoffman, 2007; Policante, 2019; entre otras. Finalmente, el segundo capítulo analiza los impactos específicos de estas tecnologías sobre el Instrumento Militar, examinando sus vulnerabilidades, oportunidades, requerimientos y capacidades necesarias para operar en los escenarios que se presentan en la actualidad.

Entender el impacto de las Tecnologías de la Información y la Comunicación sobre el Instrumento Militar, resulta insoslayable para que el Estado pueda proteger y preservar sus intereses vitales frente a adversarios que operan en la ambigüedad, la adaptabilidad y la innovación constante.

CAPÍTULO I
LA AMENAZA HÍBRIDA EN EL SIGLO XXI

3.1. Conceptualización de la amenaza híbrida

El objetivo de este capítulo es analizar a la luz de los conflictos del siglo XXI, Afganistán, Iraq y Rusia-Ucrania, la comprensión del concepto de amenaza híbrida.

En este sentido, numerosos autores coinciden en señalar que, a diferencia de las guerras clásicas del período industrial, las amenazas híbridas no se ajustan a una tipología única ni a un modelo operativo rígido. Por el contrario, representan un continuo dinámico donde los actores, estatales o no estatales, adaptan sus capacidades, sus cursos de acción (en el nivel operacional, líneas de operaciones) y sus objetivos a las vulnerabilidades del adversario. Como plantea Hoffman (2007), lo híbrido no es una categoría nueva en sí misma, sino la manifestación contemporánea de la flexibilidad estratégica de los actores que explotan simultáneamente múltiples formas o modalidades de conflicto.

Siguiendo esta línea de pensamiento, Locatelli (2019) se ha referido en su artículo "La metamorfosis de la guerra" al concepto desarrollado en los párrafos precedentes, de la siguiente manera:

> Las Fuerzas Armadas deben prepararse para las guerras que deban pelear y no para las que se quieran pelear. Las nuevas guerras por ganar, sin duda, han vulnerado los patrones convencionales. La forma de la guerra ha evolucionado hasta hacerse híbrida por la complejidad de acciones que se deben enfrentar y que no han encontrado aún una denominación adecuada. (Locatelli, 2019, pág 75).

Desde la perspectiva latinoamericana y específicamente de la bibliografía militar conjunta de las fuerzas armadas argentinas, esta tendencia ha sido observada de manera creciente. La doctrina básica para la AMC reconoce que las amenazas actuales no pueden comprenderse sin considerar la convergencia de tácticas irregulares, operaciones de información, capacidades cibernéticas y acciones de presión socioeconómica, todas ellas presentes en los conflictos recientes. Capdevilla (2022) agrega que las nuevas tecnologías, especialmente las Tecnologías de la Información y la Comunicación, constituyen en la actualidad un instrumento transversal que potencia cada dimensión de la guerra híbrida, modificando tanto la forma de desarrollar acciones como la velocidad y el alcance de sus efectos.

Los trabajos académicos de la Escuela Superior de Guerra y de la Escuela Superior de Guerra Conjunta también reflejan esta evolución conceptual. Olguín Noriega (2014) identifica la presencia simultánea de tres tipos de fuerzas en los conflictos híbridos. Las fuerzas regulares que ejecutan operaciones convencionales, las fuerzas irregulares, incluidos insurgentes, guerrilleros y terroristas, que desarrollan emboscadas, acciones asimétricas y operaciones de información; y las fuerzas criminales dedicadas a actividades como tráfico ilícito, lavado de dinero y provisión logística clandestina (narcotráfico). Esta coexistencia de actores con distinto nivel de organización y legitimidad confirma que una amenaza híbrida opera como un fenómeno estructural más que como una anomalía táctica.

Autores como Korybko (2015) profundizan este enfoque señalando que la guerra híbrida puede incluir fases *"suaves"* basadas en manipulación de la información, propaganda y presión social y económica mediante el empleo de redes sociales y/o medios de comunicación, seguidas (si fuere necesario) por fases *"duras"* caracterizadas por la acción armada irregular. Esta lectura evidencia el rol estratégico de las TIC en la construcción del conflicto, especialmente en su dimensión cognitiva. En la misma línea de pensamiento, Jorquera Escobar (2024) advierte que las redes sociales actualmente constituyen uno de los principales vectores de desinformación y propaganda en entornos híbridos, donde la batalla por la opinión pública y la legitimidad opera como un multiplicador de fuerza.

La investigación de Policante (2019) amplía esta perspectiva al analizar la interacción interagencial en escenarios híbridos, destacando que este tipo de conflictos se desarrollan simultáneamente en múltiples dominios, terrestre, aéreo, ciberespacial, entre otros. En consecuencia, los Estados deben operar con estructuras flexibles y coordinadas, capaces de integrar capacidades civiles y militares. A su vez, Locatelli (2019) destaca que la metamorfosis de la guerra implica un cambio profundo en los estándares tradicionales de empleo del poder militar, generando la necesidad de preparar a las fuerzas armadas para escenarios donde lo convencional y lo no convencional se combinan sin solución de continuidad.

Desde una perspectiva comparada, estudios como los de Baqués (2015) muestran que incluso las grandes potencias, dotadas de superioridad militar evidente, han enfrentado dificultades para imponerse a enemigos irregulares mediante operaciones clásicas. Esta disparidad obligó a repensar la relación entre superioridad de medios y eficacia operacional,

uno de los elementos clave para comprender por qué la guerra híbrida se ha convertido en el paradigma predominante del conflicto contemporáneo.

Por otra parte, resulta indispensable resaltar que el concepto de amenaza híbrida no es uniforme en todas las doctrinas militares. Mientras en Occidente, particularmente en Estados Unidos y en los países que conforman la OTAN, la noción de guerra híbrida se ha institucionalizado como marco doctrinario, autores como Colom Piella (2018) y otros especialistas en estudios rusos destacan que este concepto no se corresponde con la doctrina oficial de Moscú. En consecuencia, el término *"guerra híbrida"* puede ser un rótulo útil para el análisis occidental, pero no necesariamente una concepción autóctona de la estrategia rusa.

En definitiva, la amenaza híbrida puede definirse, para efectos del presente trabajo, como un tipo de conflicto caracterizado por: la convergencia de tácticas, técnicas y procedimientos convencionales e irregulares; la participación simultánea de actores estatales, paraestatales, no estatales y organizaciones criminales; el uso intensivo de Tecnologías de la Información y la Comunicación para operar en el dominio cognitivo, informacional y cibernético; la búsqueda de efectos estratégicos sin necesidad de emplear fuerzas regulares de manera abierta; y la explotación de las vulnerabilidades del adversario mediante acciones coordinadas en múltiples dominios

Esta concepción integral permite comprender que la guerra híbrida no constituye sólo una modalidad o variante de combate, sino una forma de pensamiento estratégico orientada a combinar recursos militares, de información, sociales, económicos, políticos y tecnológicos para erosionar la cohesión y la voluntad de lucha del oponente. Para las fuerzas armadas argentinas, esta comprensión ofrece un marco indispensable para analizar los impactos de las TIC, cuyo estudio específico será desarrollado en capítulos posteriores.

El análisis de los componentes tácticos de la amenaza híbrida resulta fundamental para comprender cómo los actores hostiles, tanto los estatales como los no estatales, ejecutan acciones concretas para generar efectos operacionales y estratégicos. Si bien la amenaza híbrida se expresa en todos los niveles de la guerra, es en el nivel táctico donde se materializan las maniobras que combinan lo convencional y lo irregular, lo físico y lo no físico (informacional), lo visible y lo encubierto. Desde esta perspectiva, las tácticas híbridas pueden entenderse como la aplicación coordinada de acciones cinéticas y no cinéticas

destinadas a explotar vulnerabilidades puntuales del adversario, con el propósito de afectar su capacidad de respuesta y su voluntad de lucha.

Diversos autores coinciden en que el nivel táctico de la guerra híbrida se basa en la lógica de la adaptabilidad y la asimetría. Locatelli (2019) plantea que uno de los rasgos centrales y distintivos de la metamorfosis de la guerra es la diversificación de las formas de empleo táctico, donde fuerzas regulares e irregulares y organizaciones criminales actúan de manera interoperable, dentro de campos de batalla imprecisos, sin frentes identificables y, peor aún, con escasa distinción entre fuerzas convencionales y no convencionales.

En un enfoque similar, Olguín Noriega (2014) sostiene que la coexistencia de estas fuerzas genera un entorno táctico caracterizado por la ambigüedad, donde los límites entre combatientes y no combatientes se presentan difusos, dificultando la aplicación efectiva de normas y doctrinas tradicionales.

Uno de los componentes tácticos más característicos de la guerra híbrida es el uso de acciones irregulares como emboscadas, ataques de oportunidad, artefactos explosivos improvisados (IED), sabotajes y hostigamiento a convoyes logísticos. Estas técnicas, ampliamente documentadas en conflictos como Iraq y Afganistán, demuestran que actores con capacidades limitadas pueden infligir daños significativos a fuerzas convencionales mediante tácticas de bajo costo. Baqués (2015) advierte que incluso fuerzas armadas poderosas, equipadas con tecnología de última generación, han sido vulnerables a estas formas de acción táctica al operar en territorios donde el adversario domina el plano social, cultural e informacional.

La dimensión informacional constituye otro elemento esencial del nivel táctico híbrido. En este sentido, las operaciones de propaganda, manipulación de narrativas, difusión de información falsa y empleo coordinado de redes sociales permiten aumentar sensiblemente el impacto de acciones físicas menores. Korybko (2015) resalta que incluso operaciones tácticas de bajo impacto pueden adquirir relevancia estratégica si son acompañadas de campañas de comunicación capaces de desmoralizar a la población, desacreditar a las fuerzas armadas o generar caos social. Esto otorga una capacidad táctica invaluable a actores relativamente débiles, que pueden influir en percepciones y comportamientos más allá de lo que sus capacidades cinéticas permitirían prever.

La aplicación de ciber acciones tácticas, como la interferencia e interrupción de comunicaciones, ataques a sistemas de control de supervisión y adquisición de datos, o intrusiones a medios o redes de baja seguridad, también emerge como una herramienta recurrente. Rid (2020) y Galeotti (2016) coinciden en que estas acciones, aunque limitadas en su alcance técnico, pueden tener efectos psicológicos importantes, particularmente cuando afectan servicios esenciales o generan la percepción de vulnerabilidad institucional. En un escenario híbrido, estas acciones suelen coordinarse con operaciones físicas, de información o psicológicas, potenciando la sensación de caos y amenaza.

La presencia de organizaciones criminales constituye otro componente táctico que torna más complejo el panorama general del conflicto híbrido. Policante (2019) destaca que estos actores aportan redes logísticas, financiamiento, acceso a mercados ilícitos y capacidad para realizar actividades encubiertas. En ocasiones, las tácticas híbridas incluyen extorsiones, secuestros, tráfico de armas y contrabando, tanto para financiar operaciones como para erosionar la autoridad del Estado. Esta convergencia entre crimen organizado y actores político-militares refuerza la naturaleza multiagencial del escenario táctico.

Asimismo, la guerra híbrida incorpora tácticas destinadas a explotar las vulnerabilidades sociales, como la movilización de protestas, la infiltración en movimientos civiles, la instigación de conflictos étnicos o religiosos y la manipulación del descontento social. Kaldor (2013) sostiene que las *"nuevas guerras"* se caracterizan precisamente por el empleo de la violencia y la información para polarizar sociedades, fracturar comunidades y generar un clima de inestabilidad que beneficie la acción del actor híbrido. Estas tácticas, aunque no constituyen acciones militares en sentido estricto, producen efectos directos en el campo táctico al dificultar la operación de las fuerzas regulares y debilitar la presencia del Estado.

Resulta insoslayable destacar que la interoperabilidad táctica entre fuerzas regulares, irregulares, milicianas, mercenarias o criminales es una característica distintiva de la guerra híbrida. Esta sinergia táctica puede manifestarse en la coordinación de ataques simultáneos, en la provisión de inteligencia por parte de actores civiles, en el empleo de drones comerciales para reconocimiento táctico o en el uso combinado de fuego directo, sabotaje y desinformación. Las TIC, tal como señala Capdevilla (2022), actúan como un multiplicador de estas capacidades al mejorar la comunicación, el Comando y Control, y la difusión rápida de información en tiempo real.

En definitiva, los componentes tácticos de la amenaza híbrida se caracterizan por su flexibilidad, su capacidad para operar en entornos ambiguos y la combinación simultánea de acciones cinética y no cinéticas. Su análisis permite entender cómo un adversario híbrido, aún con recursos limitados, puede generar efectos tácticos que se traducen en impactos operacionales y estratégicos significativos, especialmente en Estados cuyas fuerzas armadas, doctrinas o sistemas de seguridad no se encuentran plenamente preparados para enfrentar amenazas de esta naturaleza. Este punto será fundamental para evaluar posteriormente cómo las Tecnologías de la Información y la Comunicación condicionan la capacidad del Instrumento Militar para operar eficazmente en escenarios híbridos.

Desde la perspectiva operacional, la amenaza híbrida despliega un conjunto integrado de acciones que buscan generar efectos estratégicos decisivos sin recurrir a una guerra declarada ni a la confrontación convencional. A diferencia de los componentes tácticos, orientados a producir impactos inmediatos en el terreno, los componentes operacionales actúan sobre las infraestructuras críticas del Estado, combinando herramientas militares y no militares para erosionar su orden y cohesión interna, afectar su capacidad de decisión y degradar progresivamente sus capacidades de disuasión y respuesta.

Ampliando las ideas expuestas en los anteriores párrafos y según la conceptualización consolidada por la OTAN en el año 2016 (Jorquera Escobar, 2024), y los aportes de Hoffman (2007), estos componentes operacionales interactúan en un entorno informacional complejo que aumenta exponencialmente sus efectos mediante el uso intensivo de tecnologías emergentes o disruptivas.

Un elemento fundamental es la conducción de operaciones de información y psicológicas, orientadas a influir en percepciones, conductas y decisiones de diversos públicos estratégicos. Estas operaciones incluyen campañas de desinformación, manipulación de narrativas, uso coordinado de redes sociales, filtración controlada de documentos, operaciones psicológicas y acciones destinadas a deteriorar la legitimidad de las instituciones de un Estado. Las Tecnologías de la Información y la Comunicación (TIC) potencian la efectividad de estas acciones, ya que permiten segmentar audiencias, aumentar contenidos mediante automatización y aprovechar la velocidad del ecosistema digital para instalar narrativas en tiempo real. El impacto operacional de estas actividades no radica sólo en modificar percepciones, sino en generar confusión, polarización y desconfianza, debilitando el consenso social y dificultando el proceso de toma de decisiones de un Estado.

Junto a las acciones psicológicas, los actores híbridos ejecutan ciberoperaciones ofensivas, defensivas y de exploración, orientadas a neutralizar, alterar o inutilizar sistemas tecnológicos críticos. Estas operaciones abarcan desde intrusiones para recolectar información estratégica (espionaje digital), hasta ataques de denegación de servicio, secuestro de datos, interrupción de redes gubernamentales y sabotaje de infraestructuras críticas. Su relevancia operacional radica en su bajo costo, su alta capacidad de negación y su potencial para generar efectos disruptivos con implicancias estratégicas. Al operar en el ciberespacio, un dominio donde la atribución de las acciones es compleja, los actores híbridos pueden ejecutar acciones agresivas sin asumir públicamente su autoría, manteniendo así la iniciativa y regulando la escalada del conflicto.

A estas actividades se suma la instrumentalización política, económica y jurídica como herramienta de presión operacional. Las amenazas híbridas recurren a medidas como bloqueo de cadenas de suministro, coerción económica o financiera, manipulación de mercados, corrupción de actores políticos locales, utilización del derecho como arma, y establecimiento de redes de influencia destinadas a inclinar decisiones gubernamentales en favor del actor agresor. Estas acciones, si bien no poseen un carácter militar directo, cumplen un propósito claramente operacional, crear condiciones desfavorables que limiten la capacidad del Estado afectado para responder de manera criteriosa y con la velocidad requerida. En este sentido, la guerra híbrida actúa como una expresión contemporánea de la Gran Estrategia, utilizando todos los recursos disponibles del Estado, no sólo los militares, para obtener ventajas significativas a lo largo del tiempo.

Otro componente relevante es la participación de actores no estatales, irregulares o proxy, empleados como instrumentos indirectos para incrementar el alcance operativo de la agresión. Estos actores pueden incluir milicias, organizaciones criminales, grupos insurgentes, empresas militares privadas, y otros. Su empleo ofrece múltiples ventajas. Proporcionan negabilidad al momento de asumir sus acciones, permiten ejecutar acciones que un Estado no podría asumir públicamente y generan presión simultánea en ámbitos donde el Instrumento Militar convencional del adversario no puede actuar con libertad. En el nivel operacional, estos actores introducen una capa adicional de complejidad al multiplicar los frentes de conflicto, conjugar lo criminal con lo político y generar un entorno caracterizado por la ambigüedad y la superposición de responsabilidades.

A modo de síntesis, la amenaza híbrida puede recurrir a acciones cinéticas limitadas, destinadas a producir efectos específicos sin escalar hacia un conflicto abierto declarado. Tales acciones incluyen sabotajes selectivos, uso táctico de drones comerciales, incursiones menores, ataques a infraestructuras críticas u ostentaciones de fuerza. Existe una dualidad en cuanto a su función operacional. Por un lado, poner a prueba las capacidades de respuesta del adversario y, por otro, causar daños concretos sin cruzar los umbrales que activarían una reacción convencional. La coordinación entre acciones cinéticas y no cinéticas es una de las características distintivas de este tipo de amenazas, ya que permite generar efectos multidimensionales que se refuerzan mutuamente.

Entendidos conjuntamente, estos componentes operacionales conforman un entramado coherente cuyo propósito es paralizar la capacidad de decisión y, por consiguiente, de respuesta del Estado oponente, desgastarlo económica y socialmente, disminuir su credibilidad interna y externa, y modelar el entorno estratégico a favor del actor que conduce la amenaza híbrida. El desafío para el Instrumento Militar radica en comprender que el escenario operacional ya no se limita al espacio físico, sino que se expande hacia dominios informacionales, cibernéticos, políticos y sociales, donde la vertiginosidad y la ambigüedad constituyen factores decisivos para la conducción del conflicto.

3.2. Comparación doctrinaria entre Occidente y Oriente

La comprensión de la amenaza híbrida requiere analizar las diferencias doctrinarias entre Occidente y Oriente, ya que cada tradición estratégica concibe el conflicto, el uso de la fuerza y la integración de las TIC desde marcos conceptuales distintos. En el ámbito occidental, la doctrina se apoya en los postulados vertidos por Clausewitz (1984) en su obra *"De la guerra"*, y en el desarrollo modernizador de Liddell Hart (1967), quienes sentaron las bases del pensamiento operacional y la maniobra indirecta. Este enfoque consolidó una cultura estratégica que distingue con claridad los niveles táctico, operacional y estratégico, priorizando la proporcionalidad en el uso de la fuerza, la centralidad del Estado y la articulación entre conducción política y empleo del Instrumento Militar.

Autores como Hammes (2004) y Lind (1989) continúan esa línea conceptual al describir la evolución del conflicto hacia formas descentralizadas y no lineales, características de la denominada "Guerra de Cuarta Generación", pero aún enmarcadas dentro de una matriz occidental que mantiene límites normativos y marcos jurídicos definidos. Tal como señala

Hoffman (2007), la guerra híbrida en el mundo occidental tiende a encuadrarse en lógicas estatales que, si bien combinan lo militar y lo no militar, lo hacen sin disolver completamente los límites entre la paz y el conflicto armado.

En Oriente, por el contrario, la concepción estratégica se apoya en tradiciones históricas que entienden el conflicto como un fenómeno permanente, en el que la distinción entre la guerra y la paz es difusa. Este enfoque tiene sus raíces en el pensamiento de Sun Tzu y se encuentra expresado en la obra *"Guerra Irrestricta"* de Liang & Xiangsui (1999), la cual propone la utilización combinada y simultánea de instrumentos militares, económicos, de información, financieros y culturales para desestabilizar al adversario sin recurrir necesariamente al enfrentamiento directo. La doctrina china enfatiza la manipulación del entorno cognitivo y la saturación del espacio de información, considerando que la superioridad estratégica deriva del control de la percepción más que del enfrentamiento explícito de fuerzas. A su vez, la tradición soviética, analizada por autores como Galeotti (2016), adopta una lógica híbrida donde las operaciones psicológicas, las campañas de desinformación, el empleo de grupos que operan encubiertos y la acción militar limitada conforman un continuo estratégico diseñado para erosionar la cohesión interna del adversario.

Aunque no existe una doctrina Gerasimov como tal, sino que más bien forma parte del pensamiento militar, sí se observa un patrón ruso que concibe el conflicto como un espectro amplio donde los medios no militares son tan importantes como los militares, especialmente en el dominio informacional. En tal sentido, Galeotti (2016) destaca que la práctica rusa contemporánea se basa en la explotación deliberada de los espacios grises y en la combinación flexible de instrumentos militares y no militares, especialmente en el dominio informacional y cognitivo.

La comparación entre ambas tradiciones doctrinarias revela diferencias sustanciales. Mientras el pensamiento occidental mantiene marcos institucionales estrictos y una estructura de empleo de la fuerza escalonada y diferenciada, el enfoque oriental integra de manera fluida todos los factores del poder nacional, tornando difusas las fronteras entre medios, ámbitos y actores. Occidente tiende a concebir las TIC como herramientas para mejorar la precisión operacional, la interoperabilidad y el Comando y Control (Hoffman, 2007; Hammes, 2004). Oriente, en cambio, las considera instrumentos estratégicos de influencia destinados a moldear percepciones, saturar el espacio de información y desestabilizar la cohesión interna del adversario (Liang & Xiangsui, 1999; Galeotti, 2016).

En este contexto, las TIC actúan como un multiplicador de ambas lógicas doctrinarias, pero con usos diferenciados. En Occidente refuerzan la precisión, la interoperabilidad y el Comando y Control. En Oriente constituyen un medio para moldear percepciones, influir en la opinión pública y generar entornos informacionales que desestabilicen al adversario sin necesidad de recurrir al empleo de la fuerza abiertamente. Esta asimetría conceptual resulta fundamental para comprender la amenaza híbrida contemporánea, ya que actores con doctrinas orientales, estatal o no estatal, tienden a emplear las TIC como un arma estratégica que opera más allá de los límites tradicionales de la guerra, mientras que en Occidente predomina una utilización más regulada, orientada al apoyo de operaciones militares convencionales.

La heterogeneidad entre ambas concepciones, lejos de ser simplemente teórica, tiene implicancias directas para el diseño de fuerzas y el planeamiento militar. Los marcos occidentales, sistematizados, normativos y escalonados, se ven desafiados por estrategias orientales que combinan de manera fluida lo político, lo militar, lo tecnológico y lo informacional. Comprender estas diferencias doctrinarias no sólo permite identificar patrones de comportamiento estratégico, sino también anticipar las modalidades específicas que puede adoptar una amenaza híbrida contra un Estado occidental, especialmente en el dominio informativo y cognitivo donde la influencia oriental ha demostrado ser particularmente eficaz.

3.3. Análisis comparado de casos: Afganistán, Iraq y Rusia-Ucrania

El análisis de diferentes conflictos recientes resulta indispensable para comprender cómo se manifiestan en la práctica los principios de la guerra híbrida y el rol de las Tecnologías de la Información y la Comunicación (TIC) en los distintos niveles de la conducción. Los casos de Afganistán, Iraq y Rusia-Ucrania permiten observar tres modelos diferentes de confrontación, con actores estatales y no estatales, marcos normativos distintos y niveles variables de empleo del poder militar e informacional. Aunque cada conflicto posee particularidades históricas y geopolíticas, su análisis revela patrones comunes que reflejan la consolidación del paradigma híbrido en el siglo XXI.

La intervención de Estados Unidos y de la OTAN en Afganistán (2001 - 2021) constituye un ejemplo paradigmático del modo en que un actor no estatal puede explotar las TIC para erosionar las ventajas convencionales de una coalición militar superior. Hammes

(2004) sostiene que los talibanes adoptaron rápidamente un estilo de combate propio de la guerra de cuarta generación, combinando operaciones de guerrilla, terrorismo, acción psicológica y manipulación social mediante redes y medios locales. La superioridad militar occidental se vio contrarrestada por una insurgencia que utilizaba teléfonos celulares, mensajería encriptada y propaganda digital para coordinar ataques, controlar poblaciones y moldear percepciones.

Hoffman (2007) resalta que en Afganistán se consolidó la práctica híbrida de emplear simultáneamente tácticas irregulares, presión mediática y campañas de desinformación dirigidas tanto a la población local como a la opinión pública internacional. Los insurgentes aprovecharon la fragmentación social, la debilidad institucional y la topografía para multiplicar el impacto de acciones tácticas de bajo costo, pero de alto valor estratégico. La guerra de narrativas, manifestada a través de videos, comunicados, rumores y operaciones psicológicas, debilitó progresivamente la legitimidad y credibilidad de la coalición internacional, demostrando que el dominio informacional puede incidir directamente en la voluntad política de los Estados intervinientes.

La guerra de Afganistán, denota que la amenaza híbrida puede surgir desde grupos reducidos, sin una tecnológica sofisticada equivalente a la de un Estado. La clave radica en la adaptabilidad, la explotación del entorno cultural y la capacidad para influir en la percepción pública, factores que resultan decisivos en sociedades tribales donde la información se transmite a través de redes digitales o medios informales.

El conflicto en Iraq (2003 - 2011) constituye un claro ejemplo para comprender la evolución de la guerra híbrida. La fase inicial de este conflicto, signada por el empleo masivo de fuerza convencional por parte de Estados Unidos, dio paso a una compleja insurgencia que combinó acciones terroristas, milicias armadas, infiltración política, crimen organizado y operaciones de información. Lind et al. (1989) anticiparon este tipo de escenarios al describir cómo la erosión de la estructura del Estado y los enfrentamientos en zonas urbanizadas favorecían la aparición de conflictos confusos, donde el adversario opera sin estructuras jerárquicas rígidas.

Las milicias chiitas y grupos como Al-Qaeda en Iraq no sólo combatieron mediante emboscadas, artefactos explosivos improvisados y ataques selectivos, sino que también desarrollaron una sofisticada estrategia de comunicación. Esta, incluía videos de propaganda,

difusión viral de atentados, manipulación de identidades en línea y campañas para exacerbar tensiones sectarias. La insurgencia iraquí utilizó internet como multiplicador de fuerza y como herramienta de reclutamiento global, sentando las bases para las posteriores capacidades informacionales del Estado Islámico (ISIS).

La respuesta estadounidense, influenciada por doctrinas contrainsurgentes clásicas y por el pensamiento de Liddell Hart (1967) sobre la importancia de la legitimidad y la población, intentó adaptarse mediante estrategias de estabilización, reconstrucción institucional y dominio y control de la información. Sin embargo, la ruptura sociopolítica del país dificultó estas acciones. El conflicto en Iraq, evidencia las limitaciones del poder militar clásico frente a un híbrido insurgente que aprovecha las TIC para coordinar ataques, manipular percepciones y generar desgaste político y social.

El conflicto entre Rusia y Ucrania (2014 - actualidad) representa el ejemplo más acabado de una estrategia híbrida aplicada a gran escala por un Estado. A diferencia de Afganistán e Iraq, donde la amenaza híbrida surgió de actores irregulares, en este caso es un Estado el que articula deliberadamente operaciones militares, ciberoperaciones, presión económica, campañas de desinformación y empleo de fuerzas irregulares y paramilitares. Galeotti (2016) destaca que este modelo ruso se apoya en una tradición estratégica donde la manipulación psicológica, la ambigüedad y el dominio de la información ocupan un lugar central.

La anexión de Crimea y la intervención en el Donbás se llevaron a cabo mediante tácticas de negación, operaciones encubiertas, empleo de *"hombres verdes"*, sabotajes, guerra electrónica y campañas de desinformación sistemáticas dirigidas tanto a la población local como a audiencias internacionales. El empleo de *bots* y *trolls* alineados con intereses estatales permitió saturar el espacio de la información con narrativas divergentes, generando incertidumbre y dificultando la atribución clara de las acciones (Rid, 2020).

La invasión a gran escala del año 2022 confirmó esta tendencia, acompañada por ciberataques a infraestructuras críticas ucranianas, campañas masivas de manipulación digital y operaciones psicológicas orientadas a quebrantar la moral de la población. No obstante, Ucrania, con el apoyo de occidente, respondió con una estrategia de información efectiva basada en transparencia, comunicación estratégica y uso inteligente de redes sociales para

influir en la opinión pública internacional. Este aspecto demuestra que el dominio de la información se ha convertido en un campo de batalla tan determinante como el terrestre.

El conflicto entre Rusia y Ucrania evidencia una manifestación consolidada de la guerra híbrida, donde un Estado integra todos los factores del poder nacional en un esquema coherente de presión continua. La guerra se torna permanente, multidimensional y orientada a moldear percepciones más que a destruir fuerzas enemigas.

El análisis comparado de Afganistán, Iraq y el conflicto entre Rusia y Ucrania deja en evidencia un conjunto de lecciones estratégicas que permiten comprender la relevancia de las Tecnologías de la Información y la Comunicación en la dinámica contemporánea de la guerra híbrida. En primer lugar, se confirma que la superioridad tecnológica no garantiza por sí sola la victoria. Tanto en Afganistán como en Iraq, las fuerzas occidentales disponían de notables capacidades en materia de vigilancia, Comando y Control y precisión para ejecutar acciones, pero se enfrentaron a adversarios capaces de diluirse entre la población, de explotar al máximo el conocimiento del terreno y de adaptar rápidamente sus tácticas. La tecnología resultó indispensable para operar, pero insuficiente para garantizar efectos estratégicos sostenibles.

En segundo término, los casos analizados denotan que el dominio del ciberespacio y de la información constituye un factor decisivo de la guerra híbrida. Tanto la insurgencia afgana e iraquí, como Rusia en Ucrania, utilizaron operaciones de influencia, campañas de desinformación y narrativas coordinadas para erosionar la cohesión social, moldear percepciones y degradar la legitimidad del oponente. Las TIC aumentaron notablemente la capacidad de actores estatales y no estatales para operar simultáneamente en los planos cognitivo, social y político, desplazando la trascendencia del espacio físico (terrestre).

A su vez, se observa que la rapidez para adaptarse a los cambios resulta un factor decisivo. Las fuerzas talibanes y las milicias iraquíes demostraron flexibilidad para combinar acciones cinéticas y no cinéticas, mientras que Rusia integró capacidades cibernéticas, psicológicas y convencionales con un grado de coordinación y sincronización que sorprendió a los analistas occidentales en 2014, aspecto que volvió a manifestarse en 2022. Las fuerzas que no logran adaptar su doctrina y sus sistemas decisorios al ritmo impuesto por el entorno informacional pierden su capacidad de prevención y anticipación, y se ven obligadas simplemente a reaccionar.

En definitiva, los casos analizados evidencian la necesidad de integrar de manera orgánica las ventajas que ofrecen las TIC dentro de la estrategia nacional y militar. La interoperabilidad entre los niveles político, estratégico, operacional y táctico, así como entre agencias civiles y organizaciones militares, surge como condición insoslayable para enfrentar amenazas híbridas.

CAPÍTULO II
IMPACTOS DE LAS TIC EN EL INSTRUMENTO MILITAR FRENTE A AMENAZAS HÍBRIDAS

La creciente relevancia de la información en los conflictos armados contemporáneos ha redefinido la función, las capacidades y las exigencias del Instrumento Militar. En escenarios híbridos, donde convergen tácticas convencionales, irregulares, cibernéticas, psicológicas y comunicacionales, las Tecnologías de la Información y la Comunicación se configuran en factores decisivos para la eficacia operacional y la protección de los intereses de una nación.

El presente capítulo analiza los impactos específicos de dichas tecnologías sobre el empleo del poder militar, considerando sus vulnerabilidades, oportunidades, requerimientos y capacidades necesarias para operar en las condiciones actuales.

La incorporación acelerada de Tecnologías de la Información y la Comunicación dentro del ámbito militar ha transformado profundamente la naturaleza de los conflictos contemporáneos. Este proceso, si bien aumenta la eficacia, la precisión y el alcance operacional del Instrumento Militar, también genera un conjunto de vulnerabilidades que actores híbridos explotan de manera sistemática. En escenarios donde los límites entre paz y conflicto se tornan difusos, tal como señalan Hoffman (2007) y Galeotti (2016), la dependencia tecnológica, la manipulación de la información, la exposición de datos en fuentes abiertas y las debilidades institucionales para gestionar crisis en el manejo de la información se convierten en factores críticos que condicionan la conducción de las operaciones y la eficiencia en la toma de decisiones.

4.1. Vulnerabilidades del Instrumento Militar potenciadas por las TIC

La digitalización y la evolución de las TIC ha potenciado la complejidad del ambiente operacional, ampliando los dominios en que se desarrollan las operaciones y exponiendo al Instrumento Militar a riesgos que exceden la dimensión netamente tecnológica. En un conflicto híbrido, donde coexisten operaciones cinéticas, ciberoperaciones, campañas de desinformación y acciones psicológicas, cada vulnerabilidad (entendida como debilidad) se transforma en una oportunidad para el adversario. Diversos autores (Hoffman, 2007; Rid, 2020; Galeotti, 2016) coinciden en que la guerra contemporánea se caracteriza por una

creciente interdependencia entre los dominios físico, de la información y cognitivo, configuración que afecta directamente a las fuerzas armadas y condiciona su accionar.

La integración masiva de las TIC en todos los niveles de la conducción ha aumentado el espectro de vulnerabilidades que pueden ser explotadas por actores estatales y no estatales. Tales vulnerabilidades ya no se limitan a las infraestructuras físicas o materiales, sino que se extienden al plano informacional, cognitivo, social y político.

La incorporación masiva de sistemas digitales tales como comunicaciones encriptadas, redes satelitales, software de logística, sistemas de Comando y Control, drones, sensores y bases de datos, incrementa la eficiencia, pero también genera lo que Rid (2020) describe como "vulnerabilidades estructurales de la guerra en red".

A mayor digitalización de la información, mayor exposición a ataques que pueden neutralizar o degradar infraestructuras críticas. Entre los principales riesgos que implica este fenómeno, se pueden destacar: la afectación de sistemas de Comando y Control, que puede llegar a restringir notoriamente la conducción de las operaciones; la interferencia o inhibición de señales de geolocalización (GPS); la penetración de sistemas de vigilancia y sensores, pudiendo ocasionar la pérdida de información táctica y estratégica; y la vulneración de datos sensibles mediante intrusiones persistentes avanzadas (ciberataques sofisticados y sigilosos).

La experiencia ucraniana anterior al año 2022 ya evidenciaba esta tendencia. Unidades enteras quedaron temporalmente aisladas tras ciberataques rusos contra redes de energía y telecomunicaciones (Galeotti, 2016). En Afganistán e Iraq también se registraron ataques a sistemas logísticos y bases de datos biométricas, a menudo ejecutados por actores no estatales asistidos por capacidades tecnológicas externas.

El ambiente informacional o de la información es un espacio de disputa permanente. Las TIC permiten que cualquier actor, desde un Estado hasta una organización insurgente, proyecte narrativas capaces de influir sobre la percepción pública, la moral de los combatientes y la toma de decisiones en todos los niveles de la conducción.

Jorquera Escobar (2024) sostiene que la desinformación en escenarios híbridos ha alcanzado un nivel de sofisticación que conlleva al replanteo constante de la veracidad de la información, convirtiéndose en un aspecto fundamental del conflicto para desestabilizar al

adversario. Esto implica que las fuerzas armadas no sólo deben combatir en el espacio terrestre, sino también lo debe hacer en el espacio cognitivo, donde los adversarios buscan sembrar confusión, disminuir la confianza en la cadena de mando, debilitar la cohesión y la moral, influir en la opinión pública para restar apoyo político al empleo militar, instalar percepciones erróneas que condicionen la conducción estratégica.

Las campañas de desinformación rusas en Crimea, en la región del Donbás y la invasión del año 2022, complementadas por operaciones psicológicas y ciberoperaciones, exhiben cómo la manipulación de la información puede preceder, acompañar o incluso sustituir acciones militares directas (Galeotti, 2016; Rid, 2020).

La amplia disponibilidad de fuentes abiertas permite que actores hostiles exploten errores menores con resultados operacionales significativos. La publicación de fotografías, geolocalizaciones, rutinas diarias o información personal por parte de personal militar ha sido utilizada eficazmente en Iraq y en Ucrania para detectar posiciones, identificar comandantes o unidades, anticipar acciones, ajustar ataques de artillería o drones, y otros tantos fines.

Etcheverry (2019) expresa que, en las guerras de cuarta generación, *"…el papel que desempeña la tecnología y fundamentalmente lo vinculado a optimizar los sistemas de información es cada vez es más importante, tanto en la etapa de planeamiento como en la de ejecución de las operaciones"*. La combinación de análisis de datos, inteligencia artificial e inteligencia de fuentes abiertas aumenta esta vulnerabilidad, permitiendo a actores con recursos limitados producir inteligencia de alto valor estratégico.

La configuración estructural tradicional de las fuerzas armadas, orientada al planeamiento y control vertical y jerárquico, enfrenta dificultades para responder a crisis en la gestión de la información que se propagan en cuestión de minutos. La falta de protocolos de comunicación estratégica, la ausencia de organizaciones especializadas en la detección temprana de campañas hostiles y la limitada coordinación con organismos civiles aumentan la exposición del Instrumento Militar a narrativas emitidas por el oponente que erosionan la legitimidad institucional, filtraciones o manipulaciones que afectan la moral interna, daños a la reputación de individuos o fuerzas que condicionan decisiones estratégicas posteriores.

4.2. Oportunidades generadas por las TIC para el Instrumento Militar

Si bien, tal como fuera indicado en los párrafos precedentes, las TIC incrementan riesgos, también constituyen un multiplicador de poder que puede fortalecer la capacidad operacional, mejorar la toma de decisiones y extender el alcance operacional del Instrumento Militar.

La posibilidad de integrar información proveniente de radares y sensores, redes sociales y otros medios de comunicación, bases de datos y sistemas de vigilancia avanzada proporciona ventajas decisivas para anticipar acciones del adversario y reducir la incertidumbre.

Etcheverry (2019) resalta que la sorpresa estratégica en la guerra moderna depende principalmente de la capacidad para procesar datos en tiempo real y convertirlos en inteligencia sumamente valiosa.

En escenarios híbridos, la batalla por la legitimidad y la percepción pública es tan importante como el poder de combate. La información se convierte en un recurso de poder ya que permite influir, disuadir, persuadir, exponer acciones hostiles y sostener la cohesión y el orden social.

En tal sentido, el Instrumento Militar puede explotar estas oportunidades mediante una comunicación efectiva, contra narrativas, el uso responsable de redes sociales, y la coordinación interagencial para la gestión de la información.

Las TIC mejoran la rapidez y la precisión del proceso de toma de decisiones, especialmente cuando se integran sistemas interoperables y redundantes que permitan operar en entornos afectados por la acción enemiga. Los modelos de *"misión comando"* (entendidos por nuestra doctrina como órdenes tipo misión) utilizados por Estados Unidos y por la OTAN para otorgar flexibilidad y libertad de acción, denotan que el aprovechamiento de las capacidades digitales incrementa la autonomía y la flexibilidad táctica, y facilita la coordinación de acciones entre las organizaciones dotadas de los mencionados modelos.

4.3. Requerimientos para la adaptación del Instrumento Militar

Los impactos descritos con anterioridad obligan a replantear los diseños organizacionales, la doctrina y los procesos de capacitación del Instrumento Militar. Estos

requerimientos constituyen condiciones necesarias para operar eficazmente en un ambiente híbrido.

La transformación digital y el empleo de las TIC exige un cambio en la cultura organizacional que reconozca el valor estratégico de la información. Esto implica entre otras cosas: comprender el ciberespacio como un dominio operacional, incorporar la gestión de la información en el planeamiento militar, combinar capacidades tácticas, estratégicas, tecnológicas y cognitivas.

Hoffman (2007) sostiene que la comprensión de la guerra híbrida requiere romper la división tradicional entre operaciones cinéticas y no cinéticas, integrando las operaciones tácticas y las operaciones de información de manera coherente.

El ambiente híbrido obliga a integrar esfuerzos entre las fuerzas armadas, como así también, con organismos estatales, fuerzas de seguridad, agencias de inteligencia, entidades gubernamentales, organizaciones privadas y actores internacionales. Las TIC sólo ofrecen ventajas si existe un sistema nacional capaz de compartir información de manera segura, confiable y oportuna, logrando con ello una adecuada sinergia.

La protección ante ciberataques no puede depender exclusivamente del accionar de las fuerzas armadas. Requiere de una adecuada y cuidadosa coordinación con organismos especializados, organizaciones privadas, organismos estatales y el sector científico-tecnológico. En este sentido, se torna indispensable establecer protocolos de ciberdefensa, implementar redundancias tecnológicas, y desarrollar capacidades de detección temprana y de respuesta ante agresiones.

4.4. Capacidades necesarias para operar en escenarios híbridos

Ante las mencionadas vulnerabilidades, las fuerzas armadas se ven obligadas a desarrollar un conjunto de capacidades que exceden la mera incorporación de tecnología. En primer lugar, resulta insoslayable incrementar las capacidades de ciberdefensa, entendidas no sólo como protección de redes, sino como un sistema integral que contempla detección temprana, respuesta coordinada, y protección de infraestructuras críticas. Rid (2020) señala que la ciberdefensa efectiva combina inteligencia humana, automatización de datos, análisis predictivo y cooperación interagencial, elementos que deben integrarse en doctrinas

actualizadas y ejercicios periódicos destinados a la preparación para prevenir y neutralizar ciberataques.

A su vez, la adaptación del Instrumento Militar a la guerra híbrida exige el desarrollo de una serie de capacidades integrales que combinen tecnología, doctrina, organización y competencias cognitivas. Se trata de un proceso gradual que requiere inversión, planeamiento y coordinación interagencial. Según Hoffman (2007), la clave no radica sólo en adquirir equipamiento, sino en modificar el concepto de empleo del poder militar hacia un enfoque multidominio e interagencial.

Las fuerzas armadas deben contar con la capacidad de proteger, detectar y responder ante diferentes ciberoperaciones ejecutadas por el enemigo. Ello exige la implementación de equipos permanentes de monitoreo y análisis, la elaboración y/o actualización de doctrinas específicas de defensa activa, el establecimiento de protocolos de respuesta ante intrusiones, la realización de ejercicios regulares de ciberoperaciones, la inversión en equipamiento y la capacitación del personal con el fin de fortalecer las capacidades de ciberdefensa.

Rid (2020) afirma que la ciberdefensa moderna sólo es efectiva si combina tecnología con inteligencia humana, anticipación estratégica y coordinación interagencial; no basta con herramientas técnicas aisladas.

La inteligencia en múltiples fuentes, especialmente la inteligencia de fuentes abiertas, adquiere un valor estratégico. La capacidad para recolectar, filtrar y analizar grandes volúmenes de datos se convierte en una ventaja decisiva en entornos caracterizados por la desinformación y la ambigüedad. La superioridad en las operaciones de información radica en la capacidad para transformar datos en comprensión situacional, algo que requiere de especialistas o analistas geoespaciales, monitoreo de redes, inteligencia automatizada y fusión de datos provenientes de radares, sensores, satélites, vehículos aéreos no tripulados y fuentes abiertas.

En tal sentido, la capacidad de recolectar, procesar e integrar grandes volúmenes de información constituye un requisito esencial. Esto incluye el análisis de redes sociales, el monitoreo de información geolocalizada, la interpretación de imágenes satelitales, y el uso de inteligencia artificial para detectar patrones.

Otra capacidad esencial consiste en integrar la gestión estratégica de la información como parte indisoluble del planeamiento militar. Tal como indica Jorquera Escobar (2024), las fuerzas armadas comprenden el potencial que tienen las redes sociales como herramientas de comunicación estratégica, que proveen datos e información que puede ser utilizada para producir Inteligencia valiosa sobre el adversario y sus operaciones. En tal sentido, las fuerzas armadas deben desarrollar competencias en comunicación estratégica, en contra narrativas, manejo de la información en situaciones de crisis (mediante la implementación de protocolos) y articulación con organismos estatales y con entidades públicas y privadas responsables de la comunicación pública.

Las operaciones de información deben integrarse al planeamiento militar desde el nivel estratégico hasta el táctico. Complementariamente, resulta conveniente desarrollar competencias tales como producción de mensajes coherentes con los objetivos estratégicos, capacitación de voceros institucionales, y monitoreo permanente de percepciones sociales.

Jorquera Escobar (2024) resalta que, en entornos híbridos, se realizan operaciones de información a través del empleo de las TIC orientadas a influir en la opinión pública, adversaria o neutral. Esto exige que la comunicación deje de ser reactiva y pase a ser una capacidad operacional activa e integrada.

Resulta imprescindible adquirir e incrementar capacidades cognitivas y educativas que permitan al personal militar comprender la complejidad del entorno híbrido. Hoffman (2007) destaca que la comprensión del conflicto híbrido exige pensamiento crítico, flexibilidad, anticipación y capacidad para interpretar simultáneamente dimensiones políticas, sociales, tecnológicas y psicológicas del conflicto. Ello implica fortalecer la formación profesional, incorporar contenidos multidominio en los planes de estudio y promover un pensamiento estratégico militar que articule coherentemente recursos militares, diplomáticos, económicos, financieros y comunicacionales.

Cabe resaltar que la tecnología no sustituye al factor humano. En tal sentido, se requieren líderes capacitados en pensamiento estratégico militar (bajo el enfoque del multidominio), instruidos en el análisis crítico y reflexivo de la información, que comprendan el entorno en el que se hallan, y que desarrollen habilidades para adaptarse rápidamente a situaciones ambiguas.

En definitiva, estas capacidades permiten contrarestar las vulnerabilidades identificadas y contribuyen a que el Instrumento Militar pueda operar de manera eficaz, legítima y alineada con los objetivos de la Estrategia Nacional en un entorno donde la información, la percepción y la tecnología se han convertido en factores determinantes del poder.

5. CONCLUSIONES

El desarrollo del presente trabajo permite confirmar que las Tecnologías de la Información y la Comunicación constituyen uno de los factores que más transformó la naturaleza de la guerra en el siglo XXI. Los conflictos analizados, Afganistán, Iraq y Rusia-Ucrania, evidencian que el campo de batalla actual no se define exclusivamente por acciones cinéticas, sino por la convergencia entre operaciones militares, operaciones de información, ciberoperaciones y disputas cognitivas cuyo impacto se proyecta sobre la voluntad, la percepción y la legitimidad estratégica. En este tipo de escenarios híbridos, la información circula con rapidez, se manipula con facilidad y se transforma de un simple recurso a un objetivo de valor estratégico.

El análisis de los casos permite evaluar los principales impactos derivados del empleo de las TIC, especialmente en la guerra híbrida, cumpliendo de esta manera el primer objetivo específico trazado para este trabajo. Las campañas en Afganistán e Iraq denotaron que la superioridad tecnológica no logra traducirse en una ventaja operacional sostenida, más aún cuando la amenaza híbrida en oposición explota el espacio de la información, manipula narrativas y erosiona la voluntad política. En contraste, la guerra entre Rusia y Ucrania exhibió un uso plenamente integrado de drones, sistemas de Inteligencia, Vigilancia y Reconocimiento (ISR), fuentes abiertas, plataformas digitales y operaciones cibernéticas, consolidando al entorno informacional como un espacio decisivo para sostener la iniciativa.

A partir de tales impactos permite analizar con mayor precisión su proyección en el nivel operacional. En este plano, las TIC demostraron ser capaces de alterar el ritmo de las operaciones, acelerando la toma de decisiones, ampliando la conciencia situacional y extendiendo el alcance operacional de las fuerzas a través de sistemas distribuidos y redes colaborativas. Al mismo tiempo, generaron riesgos difíciles de gestionar. La dependencia tecnológica, la saturación de la información, la fragilidad del Comando y Control frente a ciberataques, y una creciente desventaja para quienes no logran integrar sus sistemas con rapidez. El nivel operacional, se consolida de esta manera, como el espacio donde se define la capacidad de una fuerza para coordinar maniobras físicas y operaciones de información, asegurando simultáneamente la protección de sus infraestructuras críticas y la explotación de las debilidades del adversario.

El objetivo específico trazado permite identificar posibles futuras amenazas para nuestras Fuerzas Armadas. Las tendencias observadas muestran que cualquier adversario, estatal o no estatal, con acceso a tecnologías relativamente accesibles puede generar efectos estratégicos mediante campañas de desinformación, interferencia de sistemas, ciberataques o la explotación de errores operativos, potenciados por el adecuado empleo de las redes sociales y otros medios de comunicación. La rapidez en la difusión de la información, la dificultad para comprobar la veracidad de los contenidos y la proliferación de herramientas de inteligencia artificial profundizan estos riesgos. De la misma manera, el análisis de los casos evidenció oportunidades relevantes tales como la posibilidad de emplear radares y sensores adecuadamente distribuidos, la explotación sistemática de fuentes abiertas, el fortalecimiento del Comando y Control mediante herramientas digitales y la construcción de una comunicación estratégica eficaz, capaz de preservar la legitimidad en situaciones de crisis.

A partir de estas observaciones, puede afirmarse que el interrogante fijado inicialmente al plantear el problema, *¿Qué aprendizajes pueden obtenerse del empleo de las TIC en las guerras híbridas recientes, pueden ser utilizados por las Fuerzas Armadas argentinas en el nivel operacional, para neutralizar futuras amenazas?*, encuentra una respuesta clara. El éxito en futuros conflictos dependerá de la capacidad de una fuerza para adaptarse a un entorno donde la información es tan relevante como la maniobra operacional. Ello exige incorporar una visión integral que considere al ciberespacio y al entorno cognitivo como dominios de relevancia equivalente al terrestre, marítimo y aéreo; fortalecer la inteligencia multidominio y las capacidades de ciberdefensa; integrar sensores y sistemas; y desarrollar una cultura organizacional que comprenda los riesgos que trae aparejado el uso de las TIC en los escenarios que se presentan en una guerra híbrida.

En definitiva, las lecciones derivadas del análisis de los conflictos recientes denotan que el Instrumento Militar no puede permanecer ajeno a la dinámica del espacio de la información. Las TIC no son un complemento, sino un elemento esencial del ambiente operacional contemporáneo. Las Fuerzas Armadas argentinas poseen la oportunidad, y la necesidad imperiosa, de incorporar estos aprendizajes para anticipar amenazas, proteger sus infraestructuras críticas, potenciar sus sistemas de toma de decisión y mantener la cohesión institucional frente a actores que buscarán, cada vez más, operar en la ambigüedad y la desinformación. Prepararse para este tipo de escenarios no implica replicar modelos externos,

sino adaptar los aprendizajes obtenidos para fortalecer una postura nacional basada en la interoperabilidad, la resiliencia tecnológica y un pensamiento estratégico militar que integre la información como centro de gravedad de la guerra moderna.

Desde el marco teórico se resalta que la relación entre las TIC y la guerra híbrida es un aspecto esencial para entender cómo han ido mutando los conflictos contemporáneos. La información se transformó en un factor decisivo para influir en percepciones, orientar la toma de decisiones y articular el empleo de los factores de poder del Estado. La guerra híbrida aparece como una modalidad de acción que combina medios convencionales, irregulares, de información y cibernéticos, generando escenarios donde los límites entre la paz y el conflicto se tornan difusos y donde diversos actores pueden explotar vulnerabilidades sin recurrir al enfrentamiento directo o a una declaración abierta de guerra.

Este marco evidencia que el uso intensivo de las TIC aporta ventajas, pero también aumenta las vulnerabilidades del Estado y de sus fuerzas armadas, al depender de redes y sistemas que pueden ser atacados con recursos de bajo costo y con un elevado impacto. Ello obliga a fortalecer la ciberdefensa, proteger la información y capacitar al personal para operar en un entorno donde el dominio cognitivo adquiere un rol significativo. La dimensión informacional, lejos de ser un complemento, constituye en la actualidad un "campo de batalla" decisivo, lo que requiere una estrecha articulación entre la acción del Instrumento Militar y los organismos estatales vinculados a inteligencia, telecomunicaciones, seguridad y relaciones exteriores. También destaca que el pensamiento estratégico militar debe adaptarse a esta complejidad, integrando en un mismo enfoque lo político, lo militar, lo económico, lo tecnológico y lo informacional. La Gran Estrategia y la Estrategia Nacional resultan esenciales para orientar coherentemente los recursos del Estado y guiar el diseño de la Estrategia Militar, que debe incorporar capacidades específicas para enfrentar amenazas híbridas. Finalmente, se arriba a la conclusión que la tecnología por sí sola no garantiza ventajas en el plano operacional. En tal sentido, la clave es contar con personal capacitado, doctrinas actualizadas y estructuras flexibles que permitan responder de manera integrada a un entorno dinámico, incierto y profundamente influido por las TIC.

En cuanto al primer capítulo, se destaca que la amenaza híbrida define la naturaleza de los conflictos recientes y actuales, donde tácticas, actores y tecnologías se integran entre sí de manera armónica y tornan difusos los límites entre lo militar y lo no militar. Los casos de Afganistán, Iraq y Rusia-Ucrania confirman que esta forma de confrontación se cimienta en

la interoperabilidad entre fuerzas regulares, irregulares y organizaciones criminales, potenciadas por un uso intensivo de las TIC que aumenta exponencialmente los efectos en todos los dominios, especialmente en el cognitivo.

En el nivel táctico, los conflictos analizados evidencian que acciones de bajo costo, como el uso de artefactos explosivos improvisados, las emboscadas, los sabotajes, las campañas de desinformación y el uso de drones comerciales para fines militares, pueden producir efectos significativos incluso contra fuerzas superiores, al explotar vulnerabilidades materiales, socioculturales y tecnológicas. Esto reafirma que la flexibilidad y la capacidad de adaptación son ventajas notables para los actores híbridos.

En el nivel operacional, la amenaza híbrida actúa mediante un enfoque indirecto que integra operaciones psicológicas, ciberoperaciones, manipulación de narrativas, presión económica-financiera y el empleo de actores proxy, todo orientado a erosionar la cohesión interna y el orden de los Estados, y afectar su capacidad de decisión sin desencadenar respuestas convencionales. Los conflictos recientes demuestran que la disputa por la legitimidad de las acciones o de una fuerza, la percepción de la población y de la opinión pública y la resiliencia institucional resultan tan determinantes como el control y dominio físico del terreno.

El análisis doctrinario entre Oriente y Occidente evidencia coincidencias en reconocer el valor del dominio de la información, pero también diferencias profundas en su integración. Mientras Occidente estructura el empleo del poder militar de manera escalonada y regulada, las doctrinas orientales conciben la guerra como un continuo que combina sin fragmentación alguna los medios militares, económicos, políticos y culturales. Esta divergencia explica la variedad de aproximaciones observadas en los conflictos contemporáneos.

En definitiva, este capítulo confirma que la guerra híbrida es una modalidad dominante del siglo XXI, caracterizada por su ambigüedad, multidimensionalidad y su capacidad para involucrar variados actores de manera simultánea. Este escenario exige que los Estados, incluido nuestro país, desarrollen capacidades específicas para enfrentar amenazas que se distinguen por la rapidez en la transmisión de la información, la manipulación cognitiva y la acción convergente en múltiples dominios, factores que condicionan directamente la eficacia del Instrumento Militar.

En cuanto al análisis del segundo capítulo se puede afirmar que las Tecnologías de la Información y la Comunicación se han vuelto un elemento esencial del ambiente operacional. En la guerra híbrida, donde conviven acciones convencionales, irregulares, cibernéticas y psicológicas, la información y la factibilidad de ser utilizada condicionan la eficacia de las operaciones en todos los niveles de la conducción, modificando tanto el planeamiento de las operaciones como la forma en que los adversarios conciben el conflicto.

Las vulnerabilidades identificadas denotan que la digitalización incrementa el riesgo para las fuerzas. En este sentido, es sabido que la dependencia tecnológica expone a fallas o errores, intrusiones y ataques sobre infraestructuras críticas, como así también, que la manipulación de la información afecta la percepción pública, la moral y la legitimidad del empleo Instrumento Militar. A lo anteriormente explicitado se suman debilidades institucionales en la gestión de la información, que dificultan la respuesta frente a acciones del oponente destinadas a erosionar la cohesión y la capacidad de decisión del Instrumento Militar.

Al mismo tiempo, las TIC generan oportunidades relevantes. Mejoran la obtención de inteligencia en tiempo real, permiten integrar múltiples fuentes de información, fortalecen el dominio de la información mediante una comunicación estratégica y optimizan el Comando y Control en entornos dinámicos y complejos. Estas capacidades reducen la incertidumbre, aceleran el proceso de la toma de decisiones y facilitan la coordinación interagencial.

El análisis llevado a cabo en este capítulo evidencia que operar eficazmente en escenarios híbridos exige adaptaciones estructurales. En tal sentido, se requiere desarrollar capacidades que permitan entender y ponderar a la información como un recurso estratégico, integrar el ciberespacio como un dominio esencial y promover mayores niveles de interoperabilidad conjunta e interagencial. La protección de infraestructuras críticas se torna prioritaria, demandando cooperación con organismos públicos y entidades privadas. A ello se suman capacidades imprescindibles, como la inteligencia multidominio, especialmente aquella basada en fuentes abiertas, la comunicación estratégica integrada al planeamiento y el fortalecimiento del pensamiento reflexivo del personal para actuar con criterio en entornos ambiguos.

Como corolario, las TIC representan simultáneamente una ventaja y una vulnerabilidad. La clave radica en desarrollar una fuerza militar resiliente, integrada en otros

estamentos o sectores de poder y orientada al dominio de la información. Logrando ello, el Instrumento Militar podrá sostener la eficacia operacional y la legitimidad institucional en el complejo escenario híbrido que se presenta en estos tiempos.

6. BIBLIOGRAFÍA

Baqués, J. (2015). *El papel de Rusia en el conflicto de Ucrania.* Revista de estudios en seguridad internacional. Universidad de Barcelona, España.

Bing West (2009). *Counterinsurgency lessons from Iraq*. Obtenido del sitio web oficial del gobierno de los Estados Unidos. https://www.army.mil/article/20621/counterinsurgency_lessons_from_iraq

Capdevilla, C. A. (2022). *Guerra híbrida: las nuevas tecnologías como instrumento de guerra*. Revista Centro de Estudios Estratégicos de Relaciones Internacionales (2).

Casale, C. G. (2022). *La Ciberdefensa como factor crítico en el desarrollo de Operaciones Militares en el Nivel Operacional.* (Trabajo de investigación, Escuela Superior de Guerra).

Castro, C. N. (2020). *El impacto de la comunicación social en la toma de decisiones del nivel operacional*. (Trabajo Final Integrador, Escuela Superior de Guerra de las Fuerzas Armadas).

Colom Piella, G. (2018). *La doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo.* (Ministerio de Defensa, Ed.) Revista del Ejército de Tierra Español (933).

Cordesman, A. H. (2006). *The Iraq War and Lessons for Counterinsurgency*. Center for Strategic and International Studies (CSIS).

Destro, L. A., de Vergara, E. A. & Dei, H. D. (2014). *Los escritos académicos en la formación militar: Guía didáctica para su elaboración y redacción* (1ra Ed.). Editorial Visión Conjunta. ESGCFFAA.

EMCFFAA (2019). *Glosario de términos de empleo militar para la acción militar conjunta*. EMCFFAA.

Etcheverry, J. F. (2019). *Las nuevas tecnologías en la guerra y la sorpresa*. (Trabajo Final Integrador, Escuela Superior de Guerra de las Fuerzas Armadas).

Galeotti, M. (2016). *Hybrid war or gibridnaya voyna? Getting Russia's non-linear military challenge right*. Mayak Intelligence.

Hammes, T. X. (2004). *The sling and the stone: On war in the 21st century*. Zenith Press.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.

Jorquera Escobar, R. (2024). *Redes sociales y guerra híbrida, un desafío para la defensa.* Centro de Estudios Estratégicos de la Fuerza Aérea de Chile. Obtenido de https://www.pucara.org/post/redes-sociales-y-guerra-h%C3%ADbrida-un-desaf%C3%ADo-para-la-defensa

Kaldor, M. (2012). *New and Old Wars: Organised Violence in a Global Era* (3rd Ed.). Stanford University Press.

Korybko, A. (2015). *Guerras híbridas. De las revoluciones de colores a los golpes.* (Batalla de ideas, Ed.) Instituto de estudios y predicciones estratégicas.

Liang, Q., & Xiangsui, W. (1999). *Unrestricted warfare*. People's Liberation Army Literature and Arts Publishing House.

Liddell Hart, B. H. (1967). *Strategy. The indirect approach* (2nd Ed.). Praeger.

Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilson, G. I. (1989). *The changing face of war: Into the fourth generation*. Marine Corps Gazette.

Locatelli, O. A. (2019). *La metamorfosis de la guerra.* Revista Visión Conjunta, año 11 (20).

NATO (2016). *NATO's response to hybrid threats*. NATO Public Diplomacy Division.

Nye, J. S. (2004). *Soft power: The means to success in world politics*. PublicAffairs.

Olguín Noriega, O. (2014). *Organización del campo de batalla en el contexto de guerras híbridas*. (Trabajo de investigación, Escuela Superior de Guerra).

PC 00-01 (2023). *Doctrina Básica para la Acción Militar Conjunta*. EMCFFAA. Min Def.

Policante, O. A. (2019). *El desarrollo de operaciones interagenciales dentro del nivel operacional en un contexto de guerra híbrida en el conflicto de Ucrania durante el 2014.* (Trabajo Final Integrador, Escuela Superior de Guerra Conjunta de las Fuerzas Armadas).

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

van Creveld, M. (2007). *La Transformación de la Guerra. La más radical reinterpretación del conflicto armado desde Clausewitz* (1ra Ed.). Buenos Aires.

von Clausewitz, C. (1984). *De la guerra*. Ministerio de Defensa de España. (Obra original publicada en 1832).