ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

TESIS

Evolución de la Guerra Inteligente y Desafíos Estratégicos para la Seguridad y Defensa Nacional en América Latina, 2015 - 2025

AUTORES:

BACH. He Wang

(orcid.org/0009-0000-6231-8661)

BACH. Yan Houyi

(orcid.org/0009-0000-7723-4698)

Para optar el Grado Académico de

MAESTRO EN GEOPOLÍTICA Y ESTRATEGIA

ASESOR:

DR. ENVER VEGA FIGUEROA

(orcid.org/0000-0002-1602-2875)

TRADUCTOR:

BACH. MIGUEL ANGEL ALVA SALVADOR

(orcid.org/0000-0002-7564-4658)

LÍNEA DE INVESTIGACIÓN:

Anticipación Estratégica - Disrupción e Innovación

2025

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 008 – 2025/ DGI/PAME

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los once (11) días del mes de diciembre del año dos mil veinticinco, siendo las 10:22 horas, se reunió el jurado evaluador conformado por los docentes:

❖	**Doctor**	**GAMALIEL MANUEL GUSTAVO TALAVERA PRADO**	**Presidente**
❖	**Maestro**	**LIZET MILAGROS CACHO DE LA CRUZ**	**Secretario**
❖	**Doctor**	**MIGUEL ANGEL CHIMA CERDAN**	**Vocal**

Designados según Resolución de Expedito para Sustentación de Tesis **N° 008-2025/SIE/DGI/ESGE-EPG** del 02 de diciembre de 2025, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"EVOLUCIÓN DE LA GUERRA INTELIGENTE Y DESAFÍOS ESTRATÉGICOS PARA LA SEGURIDAD Y DEFENSA NACIONAL EN AMÉRICA LATINA, 2015 - 2025"**, presentado por los Bachilleres **YAN HOUYI y HE WANG**, para optar el Grado Académico de Maestro en Estrategia y Geopolítica, de acuerdo a lo establecido en el artículo 45° de la Ley Universitaria N° 30220.

Luego de atender la sustentación presencial, defensa de la tesis de grado y realizadas las preguntas de rigor, el jurado acordó concederle la calificación de ...Diecisiete (17.00).....

En mérito del cual, el jurado .....aprueba..... (aprueba / no aprueba) que se le otorgue el Grado Académico de Maestro en Estrategia y Geopolítica.

Firmado, en Chorrillos a los once (11) días del mes de diciembre del año dos mil veinticinco.

DR. GAMALIEL MANUEL GUSTAVO TALAVERA PRADO	**MG. LIZET MILAGROS CACHO DE LA CRUZ**	**DR. MIGUEL ANGEL CHIMA CERDAN**
PRESIDENTE	**SECRETARIO**	**VOCAL**

AGRADECIMIENTOS

Agradecemos profundamente al Dr. Enver Vega Figueroa por su guía decisiva durante la investigación. Expresamos también nuestro sincero reconocimiento al Mayor EP Miguel Ángel Alva Salvador por su apoyo en la traducción y coordinación de entrevistas.

A la Escuela Superior de Guerra, a sus autoridades, docentes, áreas administrativas y de investigación, les agradecemos por las facilidades, la formación recibida y el soporte institucional. Extendemos igualmente nuestro agradecimiento al Embajador de China en Perú y al Asistente de Agregado de Defensa por su colaboración.

Finalmente, expresamos nuestro más sincero agradecimiento a nuestras familias, cuyo apoyo hizo posible la culminación de este trabajo.

INDICE

PORTADA	**1**
ACTA DE SUSTENTACION	**2**
AGRADECIMIENTOS	**3**
INDICE	**4**
RESUMEN	**6**
ABSTRAC	**7**
REPORTE DE SIMILITUD	**8**
DECLARACION JURADA DE AUTENTICIDAD Y NO PLAGIO	**9**
INTRODUCCION	**10**
CAPITULO I: PLANTEAMIENTO DEL PROBLEMA	**12**
1.1 Descripción de la Situación	**12**
1.2 Formulación del Problema	**17**
1.3 Objetivos de Investigación	**18**
1.4 Justificación de Investigación	**18**
1.5 Viabilidad de la Investigación	**20**
CAPITULO II: ESTADO DEL ARTE	**24**
2.1 Antecedentes de la Investigación	**24**
2.2 Bases Teóricas	**37**
2.3 Marco Conceptual	**41**
2.4 Definición de Términos Básicos	**43**
CAPITULO III: METODOLOGIA	**47**

3.1 Diseño Metodológico 47

3.2 Diseño Muestral 49

3.3 Técnicas e instrumentos de Recolección de Información 49

3.4 Técnicas Estadísticas para el Procesamiento de la Información 51

3.5 Aspectos Éticos 51

CAPITULO IV: ANALISIS Y SINTESIS 53

4.1 Definición de Categorías y Subcategorías 53

4.2 Soporte de Categorías 60

4.3 Red Semántica 168

4.4 Triangulación 189

CAPITULO V: DIALOGO TEORICO EMPIRICO 224

CONCLUSIONES 235

RECOMENDACIONES 239

PROPUESTA PARA ENFRENTAR LA REALIDAD PROBLEMÁTICA 244

REFERENCIAS BIBLIOGRAFICAS 249

ANEXOS

1. **Matriz de Consistencia 256**
2. **Validación de Instrumento 258**
3. **Instrumentos de Recolección de Información 261**
4. **Autorización para la Recolección de Información**
5. **Consentimiento Informado**

RESUMEN

La investigación analiza cómo la evolución de la guerra inteligente, sustentada en inteligencia artificial, sistemas de armas autónomas, ciberestrategias y guerra cognitiva, reconfigura los marcos de seguridad y defensa nacional en América Latina entre 2015 y 2025. Se adopta un enfoque cualitativo, teórico-empírico, con estudio de caso múltiple comparativo de seis países (Argentina, Brasil, Chile, Colombia, México y Perú), basado en análisis documental, revisión bibliográfica sistemática y entrevistas a expertos. El marco analítico se organiza en cuatro categorías: impacto de la guerra inteligente, capacidades estatales, vacíos de gobernanza y competencia geoestratégica.

En términos generales, América Latina enfrenta la guerra inteligente desde una posición de vulnerabilidad estructural, marcada por capacidades fragmentadas, gobernanza insuficiente, dependencia tecnológica profunda y presiones geopolíticas externas crecientes. Estos factores limitan la autonomía estratégica, amplifican los riesgos y dificultan la construcción de un marco regional coherente frente a la transformación bélica de la nueva era. Superar estas brechas requiere fortalecer la industria militar regional, consolidar doctrinas tecnológicas compartidas, diseñar marcos ético-normativos robustos y articular una cooperación regional capaz de integrar la innovación soberana, la resiliencia digital y la estabilidad geoestratégica continental.

Palabras clave: guerra inteligente; seguridad y defensa; inteligencia artificial militar; autonomía estratégica; América Latina.

ABSTRACT

This research analyzes how the evolution of intelligent warfare, grounded in artificial intelligence, autonomous weapons systems, cyberstrategies, and cognitive warfare, reshapes national security and defense frameworks in Latin America between 2015 and 2025. A qualitative, theoretical–empirical approach is adopted through a comparative multiple-case study of six countries (Argentina, Brazil, Chile, Colombia, Mexico, and Peru), based on documentary analysis, systematic literature review, and expert interviews. The analytical framework is structured around four categories: the impact of intelligent warfare, state capabilities, governance gaps, and geostrategic competition. The findings reveal doctrinal transformation and security architectures under pressure from new cyber and cognitive risks, within a context of significant technological dependence and regional disparities in digital infrastructure, cyberdefense, and military AI development. Legal, ethical, and operational gaps are identified in regulating the use of disruptive technologies, along with the peripheral insertion of Latin America in the strategic rivalry between China and the United States, which constrains its strategic autonomy. The study proposes guidelines aimed at strengthening digital sovereignty, techno-military governance, and regional cooperation in defense.

Keywords: intelligent warfare; security and defense; military artificial intelligence; strategic autonomy; Latin America.

TESIS Yan Hou Yi & He Wang IFI - XVI PAME 2025 .pdf

TESIS 2025
TESIS 2025
Escuela Militar de Chorrillos Coronel Francisco Bolognesi

Detalles del documento

Identificador de la entrega
trn:oid:::12350:544462591

Fecha de entrega
6 ene 2026, 5:37 p.m. GMT-5

Fecha de descarga
6 ene 2026, 6:27 p.m. GMT-5

Nombre del archivo
TESIS Yan Hou Yi & He Wang IFI - XVI PAME 2025 .pdf

Tamaño del archivo
2.7 MB

270 páginas

54.370 palabras

340.635 caracteres

9% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

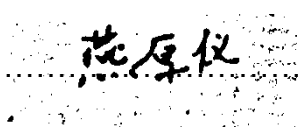
Fuentes principales

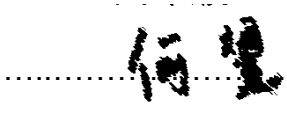
9% Fuentes de Internet
2% Publicaciones
2% Trabajos entregados (trabajos del estudiante)

DECLARACION JURADA DE AUTENTICIDAD Y NO PLAGIO

Por el presente documento, nosotros YAN HOUYI, identificado con PASAPORTE N° PE3290502; y HE WANG, identificado con PASAPORTE N° 3290501, egresados del XVI Programa de Alto Mando Del Ejército ,informamos que hemos elaborado el Trabajo de Investigación denominado “Evolución de la Guerra Inteligente y Desafíos Estratégicos para la Seguridad y Defensa Nacional en América Latina, 2015-2025¨, Para optar el Grado Académico de MAESTRO EN ESTRATEGIA Y GEOPOLÍTICA, y declaramos que este trabajo ha sido desarrollado íntegramente por los suscritos y afirmamos que no existe plagio de ninguna naturaleza. Así mismo, dejamos en constancia de que las citas de otros autores han sido debidamente identificadas en el trabajo, por lo que no se ha asumido como propias las ideas vertidas por terceros, ya sea de fuentes encontradas en medios escritos como en Internet.

Así mismo, afirmamos que somos responsables solidarios de todo su contenido y asumimos, como autores, las consecuencias ante cualquier falta, error u omisión de referencias en el documento. Sabemos que este compromiso de autenticidad y no plagio puede tener connotaciones éticas y legales. En caso de incumplimiento, nos ponemos a disposición de las normas académicas que considere el Escuela Superior de Guerra del Ejército – Escuela de Posgrado y a lo estipulado en el Reglamento interno.





YAN HOUYI

PASAPORTE N° PE3290502

HE WANG

PASAPORTE N° 3290501

INTRODUCCIÓN

La acelerada transformación tecnológica que caracteriza al sistema internacional durante la última década ha introducido cambios profundos en la manera en que los Estados conciben, estructuran y ejecutan sus estrategias de seguridad y defensa. En este contexto, la denominada guerra inteligente; sustentada en inteligencia artificial militar, sistemas de armas autónomas, ciberestrategias ofensivas y defensivas, capacidades satelitales avanzadas y modalidades emergentes de guerra cognitiva; redefine los umbrales del uso de la fuerza, acelera los tiempos de decisión y genera nuevas vulnerabilidades en las arquitecturas estatales. América Latina, región históricamente rezagada en innovación militar y con alta dependencia tecnológica, enfrenta estos cambios en un escenario marcado por crecientes disputas geoestratégicas entre potencias como Estados Unidos y China, procesos internos de fragmentación institucional y limitadas capacidades de gobernanza tecno-militar.

A partir de esta problemática, la presente investigación se orienta a comprender cómo la evolución de la guerra inteligente impacta los marcos de seguridad y defensa nacional de Argentina, Brasil, Chile, Colombia, México y Perú entre 2015 y 2025, así como qué desafíos estratégicos emergen en términos de gobernanza, autonomía tecnológica y cooperación regional. Complementariamente, se examinan las capacidades institucionales, doctrinarias y tecnológicas de los Estados, y los vacíos normativos, éticos y operativos que condicionan su adaptación a este nuevo paradigma bélico.

Metodológicamente, el estudio adopta un enfoque cualitativo, con un diseño teórico-empírico de estudio de caso múltiple comparativo. Se emplean métodos

de análisis documental, revisión sistemática de literatura, y entrevistas semiestructuradas a expertos del sector defensa, constituyendo así una triangulación que fortalece la validez interpretativa. La población de análisis incluye especialistas, oficiales superiores y académicos vinculados a la seguridad internacional; la muestra es intencional y conformada por informantes clave seleccionados por su experiencia técnica.

La tesis se estructura en cinco capítulos. El Capítulo 1 expone el planteamiento del problema, las preguntas y los objetivos. El Capítulo 2 desarrolla el marco teórico y el estado del arte respecto a la guerra inteligente y sus implicancias estratégicas. El Capítulo 3 presenta la metodología. El Capítulo 4 expone el análisis teórico-empírico y los hallazgos comparados. Finalmente, el Capítulo 5 presenta las conclusiones, recomendaciones y la propuesta estratégica para América Latina frente al escenario emergente de guerra inteligente.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la Situación Problemática

La evolución de la guerra inteligente, basada en inteligencia artificial (IA), armas autónomas, ciberestrategias y sistemas de vigilancia inteligente, ha transformado las doctrinas militares, los esquemas de seguridad y los equilibrios geopolíticos globales (Osimen et al., 2024). Esta revolución tecnológica ha dado lugar a una nueva carrera armamentista entre potencias como Estados Unidos, China y Rusia, elevando las tensiones estratégicas, la automatización bélica y los dilemas ético-políticos sobre el uso de la fuerza (Burton & Soare, 2019). Si bien América Latina no lidera esta innovación, enfrenta sus impactos indirectos en materia de defensa, soberanía tecnológica y gobernanza regional.

La transformación hacia una guerra inteligente ha modificado profundamente las doctrinas militares y los sistemas de seguridad, estableciendo una nueva lógica basada en la automatización y el control algorítmico de la fuerza. Este cambio no solo redefine la estructura de la guerra, sino también las relaciones de poder entre Estados y actores tecnológicos (Burton & Soare, 2019). La competencia entre potencias como Estados Unidos, China y Rusia ha reconfigurado la disuasión estratégica, impulsando la automatización bélica y abriendo dilemas ético-políticos sobre el control humano en decisiones letales (Osimen et al., 2024). Aunque América Latina no participa directamente en esta carrera, sus sistemas de defensa se ven afectados por los efectos de la dependencia tecnológica, la vulnerabilidad informacional y la falta de marcos comunes de gobernanza regional.

En las dos primeras décadas del siglo XXI, la inteligencia artificial modificó radicalmente los escenarios de seguridad y defensa global, configurando un nuevo paradigma militar sustentado en la integración hombre-máquina y la automatización del mando. Long y Xu (2022) evidenciaron que la aplicación militar de la IA redujo los umbrales de guerra e incrementó la inestabilidad estratégica, mientras Zhao et al. (2023) demostraron que las capacidades de aprendizaje profundo, visión computacional y procesamiento del lenguaje natural redefinieron la recopilación y el análisis de información militar. Estos avances consolidaron un modelo de guerra inteligente basado en datos, algoritmos y autonomía operacional, con efectos directos sobre la velocidad de decisión y la letalidad de los sistemas.

Los avances en inteligencia artificial modificaron las condiciones del conflicto armado al disminuir los umbrales para el uso de la fuerza y aumentar la velocidad y complejidad de las decisiones estratégicas. Long y Xu (2022) advirtieron que la automatización militar incrementa el riesgo de escaladas imprevistas, mientras Zhao et al. (2023) demostraron que la integración hombre-máquina redefine la inteligencia militar y la gestión de datos en tiempo real. La guerra inteligente, sustentada en el análisis algorítmico y la autonomía de sistemas, introdujo una nueva fase de combate donde la información se convierte en el principal recurso estratégico y la capacidad de decisión automática en la ventaja decisiva.

Tao y Yang (2024) y Wang et al. (2023) identificaron que las aplicaciones más maduras de la IA se concentran en la percepción situacional, el reconocimiento de objetivos y el apoyo al mando y control, aunque persisten brechas tecnológicas en guerra electrónica e inteligencia logística.

Paralelamente, Long y Xu (2020) y Lu (2024) subrayaron los vacíos normativos internacionales y los dilemas ético-jurídicos que plantea el uso de armas autónomas, como la atribución de responsabilidad legal o la compatibilidad con el derecho internacional humanitario. Estas tensiones evidencian la falta de gobernanza global sobre la autonomía bélica y la necesidad de cooperación multilateral en la regulación de tecnologías disruptivas.

La investigación de Tao y Yang (2024) y Wang et al. (2023) evidenció que las aplicaciones de IA militar más desarrolladas se encuentran en el reconocimiento de objetivos y la percepción situacional, consolidando la autonomía operacional de los sistemas inteligentes. Sin embargo, Long y Xu (2020) y Lu (2024) subrayaron que persisten vacíos normativos sobre la responsabilidad en decisiones letales y el control ético de la autonomía bélica. Estos dilemas revelan la urgencia de construir un marco de gobernanza multilateral que regule las tecnologías disruptivas, evite su uso indiscriminado y garantice la estabilidad estratégica internacional.

A nivel regional, América Latina muestra una persistente dependencia tecnológica y escasa producción estratégica, lo que genera vulnerabilidades frente a ciberamenazas, conflictos híbridos y campañas de desinformación (Filgueiras, 2023; Batista et al., 2020). La débil regulación del uso militar de la IA y la fragmentación institucional agravan estas debilidades (Saavedra, 2004; Bianculli, 2024). Campos (2025) confirmó que la adopción tecnológica en la región es desigual y que las capacidades institucionales no acompañan el ritmo de innovación, mientras que Saavedra (2024) demostró que los sistemas de ciberdefensa latinoamericanos carecen de una arquitectura cooperativa y multidimensional. Asimismo, Pomares (2024) observó que las estrategias

nacionales de IA —en países como Argentina, Brasil, Chile, Colombia, Ecuador, México, Perú y Uruguay— son mayoritariamente aspiracionales y se concentran en la dimensión económica, relegando la seguridad y la ética militar.

La región latinoamericana continúa rezagada en el desarrollo de capacidades tecnológicas y defensivas, lo que la expone a ciberamenazas y conflictos híbridos (Filgueiras, 2023; Batista et al., 2020). La ausencia de una regulación militar coherente y la fragmentación institucional dificultan la adopción de políticas integrales (Saavedra, 2004; Bianculli, 2024). Según Campos (2025) y Pomares (2024), los planes nacionales de IA privilegian los objetivos económicos y sociales, dejando en segundo plano la seguridad digital, la ética militar y la autonomía estratégica, factores esenciales para una defensa moderna y soberana.

En este contexto, los países de la región experimentan tensiones entre la modernización militar y el riesgo de nuevas dependencias tecnológicas, en un escenario geopolítico influido por las potencias globales (Krivolapov & Stepanova, 2023). Becker et al. (2025) evidenciaron que la inteligencia artificial generativa impacta directamente en la integridad informacional y en los procesos electorales, mientras que Meza (2019) y Macher (2021) alertaron sobre los dilemas jurídicos de los sistemas de armas autónomas letales y la insuficiencia del marco legal internacional.

Brasil, Colombia y Argentina experimentan tensiones entre la necesidad de modernizar sus sistemas militares y el riesgo de consolidar nuevas dependencias tecnológicas frente a las potencias globales (Krivolapov & Stepanova, 2023). Becker et al. (2025) alertaron que la IA generativa afecta directamente la integridad informacional, abriendo vulnerabilidades en los

sistemas políticos y democráticos. Por su parte, Meza (2019) y Macher (2021) advirtieron que los marcos normativos internacionales son insuficientes para contener los riesgos ético-jurídicos derivados de la guerra automatizada, lo que incrementa la exposición de la región ante amenazas tecnológicas sin regulación efectiva.

De manera complementaria, Luo et al. (2023) y Zhang et al. (2022) mostraron que la guerra inteligente da paso a nuevas formas de confrontación, como la guerra cognitiva, los enjambres de drones o la interferencia cibernético-electrónica, lo que amplía el espectro de amenazas híbridas y transforma la relación entre tecnología, poder y democracia. Estas dinámicas plantean la urgencia de analizar cómo los países latinoamericanos responden, o no responden, mediante políticas de anticipación estratégica, cooperación regional e innovación soberana.

Los estudios de Luo et al. (2023) y Zhang et al. (2022) mostraron que la guerra inteligente da paso a estrategias basadas en la manipulación cognitiva, los enjambres de drones y las operaciones cibernéticas distribuidas, ampliando los límites del combate convencional. Estas transformaciones afectan la relación entre tecnología, poder y democracia, al convertir la información en un recurso de control político. En este escenario, América Latina carece de políticas de anticipación y cooperación regional que permitan construir una arquitectura de defensa soberana frente a los desafíos de la guerra cognitiva y la inteligencia artificial.

En síntesis, la guerra inteligente redefine no solo el campo militar, sino también la estructura del poder global y la capacidad de los Estados para garantizar su autonomía estratégica. América Latina enfrenta esta transición con

escasas capacidades tecnológicas, doctrinarias y regulatorias, lo que acentúa su vulnerabilidad ante amenazas emergentes. Por ello, comprender la evolución de la guerra inteligente y sus implicancias estructurales para la seguridad y defensa nacional en América Latina no constituye solo una tarea académica, sino una necesidad política para fortalecer marcos de seguridad más autónomos, éticos y resilientes en la región.

Por lo tanto, la guerra inteligente no solo transforma los instrumentos de combate, sino que reconfigura la estructura misma del poder mundial y la capacidad de los Estados para ejercer soberanía. América Latina enfrenta esta transición con limitaciones doctrinarias, tecnológicas y normativas, lo que incrementa su vulnerabilidad estratégica. Por ello, analizar la evolución de la guerra inteligente y sus implicancias estructurales constituye una tarea estratégica prioritaria para el fortalecimiento de marcos de seguridad autónomos, éticos y resilientes en la región.

1.2 Formulación del Problema

- ¿Cómo está impactando la evolución de la guerra inteligente, incluyendo el uso militar de inteligencia artificial, armas autónomas y ciberestrategias, en los marcos de seguridad y defensa nacional de los países de América Latina, y qué desafíos estratégicos plantea en términos de gobernanza, autonomía tecnológica y cooperación regional?
- ¿Qué capacidades institucionales, doctrinarias y tecnológicas poseen los Estados latinoamericanos para responder a las amenazas emergentes de la guerra inteligente, y cómo varían dichas capacidades entre países?

- ¿Cuáles son los vacíos normativos, éticos y operativos más críticos en los marcos legales y de gobernanza de América Latina frente a la proliferación de tecnologías de guerra inteligente?
- ¿Cómo influye la competencia geoestratégica entre grandes potencias, como China y Estados Unidos, en la configuración de las respuestas regionales frente a la guerra inteligente, y qué implicancias tiene ello para la autonomía estratégica de América Latina?

1.3 Objetivos de la Investigación

- Interpretar cómo la guerra inteligente transforma los marcos de defensa y seguridad en América Latina y qué desafíos plantea en gobernanza, autonomía y cooperación.
- Analizar las capacidades institucionales, doctrinarias y tecnológicas de los Estados latinoamericanos frente a la guerra inteligente y sus variaciones entre países.
- Identificar los vacíos normativos, éticos y operativos en la gobernanza latinoamericana ante el avance de tecnologías de guerra inteligente.
- Comprender cómo la competencia entre grandes potencias influye en las respuestas regionales y en la construcción de autonomía estratégica en América Latina.

1.4 Justificación de la Investigación

La presente investigación se justifica por la urgente necesidad de comprender el impacto geoestratégico y doctrinario de la inteligencia artificial, las armas autónomas y las ciberestrategias en la transformación de la guerra contemporánea. En la actualidad, el mundo asiste a una nueva carrera armamentista tecnológica, donde el dominio de la información, los algoritmos y

la automatización del poder militar están redefiniendo las lógicas de disuasión, control y soberanía. Este escenario global plantea profundas tensiones entre innovación, seguridad y ética, afectando directamente las arquitecturas de defensa y los equilibrios geopolíticos internacionales (Osimen et al., 2024; Burton & Soare, 2019).

En este marco, América Latina se encuentra en una posición estratégica y vulnerable a la vez: su rezago tecnológico y su dependencia de plataformas extranjeras limitan la capacidad de los Estados para garantizar la soberanía digital, la seguridad informacional y la autonomía operativa. La región enfrenta el doble desafío de modernizar sus estructuras de defensa nacional e insertarse en la revolución tecnológica global sin perder control sobre sus procesos decisionales y sus recursos estratégicos (Filgueiras, 2023; Krivolapov & Stepanova, 2023). Comprender la evolución de la guerra inteligente permite anticipar los riesgos de subordinación tecnológica y los escenarios de inestabilidad que podrían comprometer la seguridad regional.

En el plano teórico, la investigación contribuirá a profundizar la comprensión crítica de la guerra inteligente como fenómeno multidimensional, integrando perspectivas de la geopolítica, la estrategia, la sociología militar y los estudios de seguridad internacional. Su aporte radica en conceptualizar la guerra inteligente no solo como una innovación tecnológica, sino como una mutación del poder y la racionalidad estratégica en el siglo XXI, capaz de alterar los fundamentos del equilibrio global y de la gobernanza de la seguridad.

En el plano práctico y estratégico, el estudio proporcionará insumos analíticos y prospectivos para los sectores estatales de defensa, planificación estratégica y gobernanza digital, ofreciendo una base para diseñar políticas

públicas orientadas al fortalecimiento de la autonomía tecnológica, la cooperación regional y la resiliencia institucional. Asimismo, su enfoque permitirá identificar oportunidades de integración entre los sistemas de defensa, la academia y el sector tecnológico, orientadas al desarrollo de capacidades soberanas en inteligencia artificial aplicada a la seguridad.

Finalmente, en el plano metodológico y académico, la investigación propone un enfoque transdisciplinar, que combina análisis documental, interpretación estratégica y revisión comparada de doctrinas militares, con el fin de construir un marco de análisis adaptable a la realidad latinoamericana. Este enfoque integrador contribuirá al desarrollo del pensamiento estratégico regional y fortalecerá la capacidad de prospectiva del Ejército del Perú frente a los nuevos escenarios de la guerra inteligente.

En suma, esta investigación no solo responde a una demanda académica y doctrinaria, sino también a una necesidad política y estratégica: la de generar conocimiento propio que oriente la toma de decisiones en defensa, seguridad y geopolítica en un mundo cada vez más condicionado por la inteligencia artificial, la automatización militar y la competencia entre potencias globales.

1.5 Viabilidad de la Investigación

La presente investigación sobre la Evolución de la guerra inteligente y los desafíos estratégicos para la seguridad y defensa nacional en América Latina es viable técnica, metodológica, institucional y éticamente, dado que dispone de las condiciones necesarias para su desarrollo, la pertinencia académica dentro del campo de la geopolítica y la estrategia, así como el respaldo documental y bibliográfico requerido para sustentar su análisis comparativo y prospectivo.

En primer lugar, la viabilidad teórica y académica se sustenta en la amplia disponibilidad de fuentes científicas actualizadas; artículos indexados, informes estratégicos y estudios comparados de origen chino, estadounidense y latinoamericano; que abordan la transformación de la guerra contemporánea desde la inteligencia artificial, la automatización bélica y la ciberdefensa (Long & Xu, 2022; Tao & Yang, 2024; Zhao et al., 2023; Saavedra, 2024; Campos, 2025). Estos antecedentes proveen un marco conceptual sólido y plural, que permite comprender la guerra inteligente como un fenómeno sistémico y multidimensional, articulado a las transformaciones tecnológicas y geopolíticas globales.

En segundo lugar, la viabilidad metodológica radica en el diseño cualitativo, de carácter descriptivo y analítico-comparativo, orientado a interpretar los marcos doctrinarios, normativos y tecnológicos que configuran las respuestas de América Latina ante la guerra inteligente. Este enfoque no requiere trabajo de campo costoso ni experimentación tecnológica, sino un proceso riguroso de análisis documental, revisión de literatura, interpretación teórica y triangulación de fuentes secundarias. Además, el estudio aprovecha la experiencia académica y profesional de los autores; oficiales investigadores del Ejército de China; en el análisis estratégico y prospectivo de la seguridad internacional, lo que otorga consistencia técnica y metodológica al desarrollo del proyecto.

En tercer lugar, la viabilidad institucional se garantiza por el respaldo académico y logístico de la Escuela Superior de Guerra del Ejército del Perú, que promueve la investigación aplicada a la defensa nacional, la geopolítica y la seguridad multidimensional. La investigación se alinea con las líneas de estudio

priorizadas por la institución, especialmente aquellas referidas a la transformación tecnológica de la guerra, la defensa regional y la autonomía estratégica del Estado. Asimismo, la articulación con fuentes de organismos internacionales, centros de pensamiento militar y bases de datos especializadas (CNKI, Scopus, Web of Science, CLAD, SELA, entre otras) asegura la validez científica y la trazabilidad de la información utilizada.

En cuarto lugar, la viabilidad operativa y de recursos es favorable, ya que el proyecto no requiere inversiones materiales significativas ni equipamiento especializado. Su desarrollo se basa en el acceso digital a bibliotecas académicas, repositorios institucionales y bases de datos abiertas. El cronograma previsto permite cumplir con los plazos de revisión, sistematización y redacción, garantizando la culminación del estudio dentro del marco temporal establecido por el programa de maestría.

Finalmente, la viabilidad ética está asegurada, dado que la investigación se sustenta exclusivamente en fuentes secundarias y no involucra manipulación de personas, instituciones o tecnologías sensibles. El tratamiento de la información se realizará conforme a los principios de integridad académica, respeto a la propiedad intelectual y confidencialidad de los datos. Además, el análisis abordará los dilemas éticos de la guerra inteligente; uso de IA en decisiones letales, autonomía de sistemas y gobernanza tecnológica; desde una perspectiva crítica y responsable, orientada al fortalecimiento de la seguridad humana y la estabilidad regional.

En conjunto, estas condiciones demuestran que el estudio es plenamente viable y pertinente, tanto en el plano técnico como institucional. Su desarrollo contribuirá a fortalecer la comprensión estratégica de la guerra inteligente y a

proponer lineamientos analíticos que orienten la formulación de políticas de defensa y cooperación tecnológica en América Latina, en consonancia con los objetivos académicos de la Escuela Superior de Guerra del Ejército del Perú y con los intereses estratégicos del Estado.

CAPITULO II: ESTADO DEL ARTE

2.1 Antecedentes de la Investigación

2.1.1. Antecedentes mundiales

Tao y Yang (2024) desarrollaron un estudio con el propósito fue analizar los principales escenarios y direcciones de aplicación militar de la inteligencia artificial, así como evaluar su nivel de madurez tecnológica en el contexto de la competencia estratégica global. La investigación adoptó un enfoque cuantitativo y descriptivo-aplicado, sustentado en el método de análisis de patentes tecnológicas y la curva de madurez de Gartner, con un diseño no experimental basado en fuentes documentales y bases de datos de propiedad intelectual entre 2000 y 2021. La población de referencia estuvo compuesta por patentes y desarrollos tecnológicos en el campo de la inteligencia artificial aplicada a la defensa, y el instrumento principal fue el análisis comparativo de indicadores de madurez (TRL). Los resultados mostraron que las aplicaciones más avanzadas se concentran en la percepción situacional y el reconocimiento de objetivos (TRL7), mientras que áreas como la guerra electrónica, el apoyo a la toma de decisiones y la inteligencia logística aún se encuentran en niveles intermedios (TRL4–5). Se concluyó que la inteligencia artificial constituye un eje central en la transformación militar contemporánea, con impactos directos en la velocidad de decisión, la autonomía de sistemas y la capacidad adaptativa de las fuerzas armadas. El estudio aporta una tipología de ocho direcciones clave de desarrollo, desde la automatización operativa hasta el refuerzo humano, y un modelo metodológico útil para evaluar la madurez tecnológica de sistemas inteligentes militares, lo que ofrece una base analítica sólida para investigaciones sobre la

evolución de la guerra inteligente y los desafíos estratégicos de seguridad y defensa en América Latina.

Lu (2024) desarrolló una investigación con el objetivo de analizar los desafíos que plantea el desarrollo acelerado de la inteligencia artificial para el derecho internacional y proponer estrategias jurídicas para su regulación global. Desde un enfoque cualitativo de carácter descriptivo y analítico, la investigación se sustentó en el examen documental y comparado de tratados, convenciones y marcos normativos internacionales, considerando como unidad de análisis los principios de responsabilidad estatal, soberanía, derechos humanos y derecho internacional humanitario. Los principales hallazgos evidenciaron que la autonomía de los sistemas inteligentes genera vacíos en la atribución de responsabilidad legal, incrementa los riesgos de violación a los derechos humanos, por sesgos algorítmicos, afectación de la privacidad y desigualdad digital, y amenaza la estabilidad del orden jurídico internacional mediante el uso de armas autónomas y la inseguridad de los datos transfronterizos. El estudio concluye que es indispensable fortalecer la cooperación multilateral mediante tratados, normas blandas y marcos nacionales armonizados, a fin de crear un sistema jurídico internacional integral que garantice el desarrollo seguro, ético y controlado de la inteligencia artificial. Su aporte radica en ofrecer una perspectiva normativa comparada que puede servir como base para investigaciones futuras sobre la gobernanza tecnológica y los marcos jurídicos internacionales aplicables a la seguridad y defensa en la era de la inteligencia artificial.

Wang et al. (2023) desarrollaron un estudio cuyo objetivo fue diseñar un concepto de operación para un sistema terrestre de asalto inteligente orientado a la guerra del futuro, respondiendo a las demandas de modernización militar.

La investigación adoptó un enfoque cuantitativo y aplicado, con un diseño experimental basado en simulaciones computacionales sobre la plataforma Matlab; su alcance fue explicativo y evaluativo, considerando como población los distintos subsistemas y nodos de interacción del sistema de asalto, mientras que los instrumentos fueron modelos estructurales DoDAF y pruebas de simulación funcional. Los resultados mostraron que el sistema inteligente presentó una mayor agilidad en la cadena de ataque, mayor capacidad de fuego y una carga de comunicación adicional asumible dentro de los límites tecnológicos actuales. Se concluyó que la arquitectura planteada, el diseño de los subsistemas y la asignación de recursos resultan coherentes y factibles, validando el modelo como referencia para el desarrollo de futuros equipos de combate terrestre. El estudio aporta evidencia empírica sobre la viabilidad de integrar sistemas autónomos y colaborativos en operaciones militares, ofreciendo una base metodológica para investigaciones posteriores sobre guerra inteligente y transformaciones estratégicas en la defensa nacional latinoamericana.

Zhao et al. (2023) analizó de manera sistemática la evolución y el estado actual de las aplicaciones de la inteligencia artificial en el ámbito de la inteligencia militar, con el objetivo de ofrecer referentes para fortalecer la toma de decisiones estratégicas y el desarrollo tecnológico en defensa. Bajo un enfoque cualitativo de tipo descriptivo-explicativo y un diseño documental analítico, los autores revisaron proyectos y programas representativos, particularmente los impulsados por Estados Unidos, utilizando como fuentes informes institucionales, artículos científicos y proyectos de innovación tecnológica. Los resultados evidenciaron que la inteligencia artificial, en especial el aprendizaje profundo, la visión computacional y el procesamiento del lenguaje natural, ha

transformado los procesos de recopilación, análisis y decisión en el campo militar, generando un modelo de servicio de inteligencia basado en cuatro niveles: infraestructura, datos, análisis y aplicación. Las conclusiones destacan que la integración hombre-máquina, el análisis multimodal y la fusión civil-militar son tendencias decisivas para el futuro de la guerra inteligente, dado que amplían la capacidad de respuesta y precisión en contextos bélicos complejos. El aporte principal de esta investigación radica en ofrecer un marco teórico y técnico para comprender cómo la inteligencia artificial redefine los sistemas de información y decisión estratégicos, constituyendo una base relevante para estudios posteriores sobre los desafíos de la guerra inteligente y la seguridad nacional en América Latina durante el periodo 2015–2025.

Luo et al. (2023) desarrollaron una investigación cuyo objetivo fue analizar la evolución, fundamentos teóricos y metodológicos de la guerra inteligente y los sistemas de simulación aplicados a la defensa nacional desde una perspectiva de la teoría de juegos. La metodología empleada fue de enfoque cualitativo y exploratorio, basada en revisión documental y análisis comparativo de experiencias internacionales, especialmente de proyectos del Departamento de Defensa de los Estados Unidos y desarrollos recientes en inteligencia artificial aplicada a la simulación de conflictos. El estudio tuvo un alcance descriptivo-explicativo y un diseño teórico-analítico sustentado en la observación de modelos y sistemas de decisión asistidos por IA, utilizando como instrumentos la revisión sistemática de literatura y el análisis de arquitecturas tecnológicas como DARPA, GEMS y sistemas de simulación distribuidos. Los resultados evidenciaron que la integración de la inteligencia artificial y la teoría de juegos ha permitido la creación de sistemas de *wargaming* inteligentes con capacidades de

aprendizaje, predicción y cooperación multientidad, posibilitando la modelización de guerras híbridas y estrategias de confrontación en tiempo real. Se concluye que la evolución hacia arquitecturas de guerra inteligente y la adopción de modelos basados en *meta-games*, simulaciones en la nube y aprendizaje reforzado están transformando la manera en que las potencias planifican y evalúan conflictos estratégicos. El principal aporte radica en ofrecer un marco teórico y metodológico que vincula la inteligencia artificial, el análisis de decisiones y la simulación estratégica, constituyendo una base científica útil para la planificación de seguridad y defensa en América Latina frente a los desafíos de la guerra cognitiva y tecnológica contemporánea.

Long y Xu (2022) desarrollaron una investigación cuyo objetivo fue analizar los riesgos estratégicos y de seguridad internacional derivados de la aplicación militar de la inteligencia artificial, así como proponer un modelo de gobernanza global que permita mitigar sus impactos. El estudio emplea un enfoque cualitativo de tipo analítico-descriptivo, con alcance explicativo y diseño documental-comparativo, basado en el análisis de fuentes primarias y secundarias provenientes de organismos internacionales, marcos normativos y literatura científica sobre gobernanza de tecnologías disruptivas. Los resultados evidencian que la aplicación militar de la inteligencia artificial disminuye los umbrales de guerra, incrementa la inestabilidad estratégica, acelera la carrera armamentista y plantea amenazas de largo plazo asociadas al desarrollo de la superinteligencia. Los autores concluyen que la respuesta global requiere un modelo de gobernanza multinivel, sustentado en la cooperación internacional, la regulación preventiva de sistemas autónomos letales y el fortalecimiento de medidas de confianza estratégica entre potencias nucleares. El principal aporte

del estudio radica en ofrecer un marco conceptual y normativo escalonado para la gobernanza de los riesgos militares de la inteligencia artificial, constituyéndose en un antecedente valioso para investigaciones sobre la evolución de la guerra inteligente y los desafíos estratégicos de la seguridad y defensa nacional en América Latina.

Zhang et al. (2022) analizaron los nuevos rasgos del enfrentamiento cibernético-electrónico en la era de la inteligencia artificial, con el objetivo de identificar cómo los avances en algoritmos, automatización y sistemas autónomos están transformando las estrategias de guerra moderna. La investigación, de enfoque cualitativo y aplicado, tuvo un alcance descriptivo-explicativo y un diseño documental-analítico, basado en la revisión de literatura científica, informes militares y casos de desarrollo tecnológico en potencias como Estados Unidos, Rusia y China. Los autores no trabajaron con una población empírica, sino con fuentes secundarias y estudios de caso como la “guerra cognitiva” y los programas de enjambres de drones. Entre los principales resultados, destacaron la emergencia de nuevas formas de confrontación, como los sistemas inteligentes de interferencia electrónica, las unidades mixtas humano-máquina, las operaciones distribuidas y la guerra cognitiva, donde la manipulación informativa y psicológica se convierte en un eje de poder. En sus conclusiones, los autores sostienen que la superioridad en la guerra inteligente depende de la capacidad para desarrollar algoritmos de decisión, optimizar la cooperación humano-máquina y fortalecer la autonomía operativa de los sistemas de combate. El aporte central de este estudio radica en ofrecer un marco conceptual y estratégico para comprender la transición desde la guerra informacional hacia una guerra cognitiva y autónoma, aportando bases analíticas

útiles para investigaciones sobre la evolución de la guerra inteligente y los desafíos estratégicos para la seguridad y defensa en América Latina, 2015-2025.

Miao y Wang (2022) analizaron los principales dilemas éticos derivados del desarrollo y aplicación de la inteligencia artificial en distintos campos sociales, incluyendo la defensa y la seguridad. Su objetivo fue sistematizar los riesgos éticos emergentes asociados a la autonomía tecnológica y sus implicaciones sobre la subjetividad humana, la privacidad, la justicia algorítmica y la seguridad militar. La metodología utilizada fue de enfoque cualitativo, tipo descriptivo y alcance analítico-sintético, sustentada en el método de revisión documental y análisis de contenido de 124 artículos científicos, nueve tesis y diversas obras teóricas indexadas en CNKI, sin aplicación de instrumentos empíricos. Los resultados mostraron que la expansión de la inteligencia artificial genera cinco grandes categorías de riesgo: la alienación de la subjetividad humana, la vulneración de la privacidad, el desplazamiento de los vínculos afectivos, los sesgos algorítmicos y el uso militar autónomo, señalando que estos fenómenos reconfiguran las relaciones sociales y las nociones tradicionales de responsabilidad. Concluyeron que las investigaciones existentes presentan una distribución temática desequilibrada, con predominio del análisis técnico sobre el filosófico, y que se requiere integrar enfoques interdisciplinarios y evaluaciones éticas sistemáticas para la gobernanza tecnológica. El principal aporte del estudio radica en ofrecer un marco de referencia integral para identificar y gestionar los riesgos éticos de la inteligencia artificial, contribuyendo a futuras investigaciones sobre los impactos estratégicos y de seguridad en América Latina, particularmente en el contexto de la guerra inteligente y su regulación ética y militar.

Macher (2021) analizó el potencial de los sistemas de aprendizaje automático aplicados al ámbito bélico y su compatibilidad con el Derecho Internacional Humanitario. El estudio se desarrolló bajo un enfoque cualitativo, descriptivo y analítico, utilizando fuentes doctrinarias y normativas. Los resultados mostraron que la militarización de la IA plantea amenazas éticas y legales sin precedentes, especialmente en la capacidad de distinguir entre combatientes y civiles. Concluyó que la regulación actual es insuficiente para los desafíos de la guerra automatizada. Su aporte se centra en anticipar los riesgos de una transición hacia conflictos dominados por inteligencia artificial, contribuyendo a la reflexión sobre la gobernanza de la guerra inteligente.

Long y Xu (2020) desarrollaron una investigación que tuvo como objetivo analizar los obstáculos conceptuales, políticos, tecnológicos y jurídicos que enfrenta el control internacional de los sistemas de armas autónomas letales (LAWS, por sus siglas en inglés), así como proponer rutas y estrategias de cooperación, particularmente desde la perspectiva china; para fortalecer la gobernanza global de dichas armas. La metodología adoptada fue de enfoque cualitativo, de tipo aplicada y alcance descriptivo-explicativo; se basó en el análisis documental de tratados internacionales, resoluciones de Naciones Unidas, informes de organismos multilaterales y literatura académica especializada, aplicando un diseño no experimental y analítico. Entre sus resultados, los autores identificaron una falta de consenso internacional sobre la definición de “autonomía” en los sistemas de armas, la disparidad de intereses entre potencias militares y países en desarrollo, las dificultades técnicas de verificación y los dilemas éticos asociados a la responsabilidad por decisiones letales tomadas por máquinas. Concluyeron que el progreso del control de

armamentos en este campo depende de la clarificación conceptual, el fortalecimiento de los principios de distinción y proporcionalidad del derecho internacional humanitario y la creación de un marco de regulación dentro del Convenio sobre Ciertas Armas Convencionales (CCW) de la ONU. Su aporte radica en ofrecer una propuesta estructurada para integrar la regulación de los sistemas de armas autónomas letales en la arquitectura jurídica y estratégica internacional, además de subrayar la necesidad de una participación activa de China y de los países del Sur Global en la formulación de normas internacionales, lo que brinda un referente teórico y comparativo clave para investigaciones sobre la evolución de la guerra inteligente y los desafíos estratégicos de la defensa nacional en América Latina.

La investigación de Meza (2019) se propuso analizar las implicaciones jurídicas del desarrollo y uso de los sistemas de armas autónomas letales (SAAL) en los conflictos armados internacionales. Se aplicó una metodología cualitativa, transversal e interdisciplinaria, con enfoque jurídico y prospectivo. El diseño fue analítico-descriptivo, sustentado en revisión documental de instrumentos del derecho internacional humanitario y resoluciones de la ONU. Los resultados identificaron vacíos normativos en la regulación de la autonomía bélica y en la rendición de cuentas por violaciones de derechos humanos. Concluyó que la ausencia de control humano significativo en los SAAL genera dilemas éticos y legales que desafían la arquitectura del derecho internacional contemporáneo. Su aporte radica en sentar las bases teóricas para discutir la legitimidad de la guerra inteligente en el marco del derecho humanitario y la ética militar.

Wang y Yang (2017) desarrollaron un estudio con el objetivo de analizar la evolución de las tecnologías de inteligencia artificial (IA), cómputo cognitivo y

sistemas de apoyo a la decisión, así como su impacto en la estructura económica y social futura. La investigación adoptó un enfoque cualitativo con carácter descriptivo-explicativo y diseño documental, basado en la revisión y sistematización de literatura científica, informes técnicos y políticas nacionales sobre IA. No trabajó con una población empírica, sino con fuentes secundarias y modelos tecno-económicos. Entre los principales resultados, los autores identificaron que la IA, el aprendizaje automático y la computación cognitiva están redefiniendo los medios de producción y las relaciones laborales, desplazando el eje económico desde los recursos materiales hacia los datos como principal fuerza productiva. Además, determinaron que la aplicación masiva de la IA requiere infraestructura de datos abiertos, plataformas colaborativas y marcos de decisión soportados en algoritmos adaptativos. Concluyeron que la IA constituye un factor estructurante de la economía de la información y un elemento estratégico para la configuración de nuevas arquitecturas de seguridad y defensa, dado que modifica la lógica de poder basada en el control de recursos físicos hacia el control de información y conocimiento. El estudio aporta una comprensión sistémica del papel de la IA en la transformación de los sistemas productivos y sociales, ofreciendo bases conceptuales útiles para investigaciones sobre la evolución de la guerra inteligente y los desafíos estratégicos de defensa en América Latina, 2015–2025.

2.1.2 Antecedentes regionales

El estudio de Campos (2025) tuvo como objetivo analizar el papel de la inteligencia artificial (IA) en la modernización del sector público y su impacto en las políticas públicas de América Latina y el Caribe. Empleó un enfoque cualitativo de tipo descriptivo y analítico, basado en la revisión documental de

estrategias nacionales de IA, informes de organismos multilaterales y políticas gubernamentales entre 2018 y 2024. Su diseño fue no experimental, con un alcance exploratorio y analítico, sin población ni muestra delimitada, utilizando como instrumentos matrices de categorización y análisis comparativo. Los resultados evidenciaron una brecha estructural entre la adopción tecnológica y la capacidad institucional, destacando que los países con mayores niveles de digitalización presentan políticas más robustas de gobernanza algorítmica y ética pública. Concluyó que la IA constituye una herramienta para la innovación administrativa y la construcción de ciudadanía digital, aunque plantea dilemas éticos y regulatorios significativos. Su aporte a la investigación radica en ofrecer un marco de referencia regional sobre los desafíos éticos, jurídicos y estratégicos de la IA, relevante para analizar su incidencia en la seguridad y defensa nacional.

Saavedra (2024) analizó los desafíos estratégicos que enfrenta América Latina en materia de ciberseguridad y defensa digital, con énfasis en la relación entre inteligencia artificial, infraestructura crítica y diplomacia cibernética. Se adoptó un enfoque cualitativo de tipo exploratorio y analítico, apoyado en revisión bibliográfica y estudios de caso sobre políticas nacionales de ciberdefensa. Los resultados indicaron que la región carece de políticas integrales para proteger la infraestructura crítica, y que el avance de la IA en seguridad y defensa no está acompañado de suficiente conocimiento técnico, lo que aumenta la vulnerabilidad estatal. Concluyó que la ciberseguridad debe entenderse como parte de la seguridad multidimensional y que requiere cooperación regional. Su aporte radica en integrar la dimensión tecnológica con la geopolítica, útil para analizar la evolución de la guerra inteligente en América Latina.

Pomares (2024) tuvo como objetivo examinar las tendencias de gobernanza de la inteligencia artificial en América Latina y su grado de alineación con el modelo europeo de regulación digital. Empleó un enfoque cualitativo de tipo analítico y comparativo, centrado en el análisis documental de estrategias nacionales de IA en ocho países (Argentina, Brasil, Chile, Colombia, Ecuador, México, Perú y Uruguay). Los resultados revelaron un avance desigual, con estrategias en su mayoría aspiracionales y escasa implementación. Concluyó que, aunque la región se inspira en el “efecto Bruselas”, emergen enfoques propios que priorizan inclusión y desarrollo económico sobre la regulación restrictiva. El estudio aporta una perspectiva de gobernanza regional que permite entender cómo la regulación de IA puede incidir en la seguridad digital y la autonomía estratégica regional.

El trabajo elaborado por Becker et al. (2025) tuvo como propósito examinar cómo la inteligencia artificial afecta la integridad informativa y los procesos electorales en América Latina, con énfasis en los casos de México y Brasil. Su metodología fue cualitativa, descriptiva y comparativa, basada en el análisis de casos y revisión documental de materiales electorales, legislación y contenido digital. Los resultados demostraron que el uso de IA generativa amplificó tanto la desinformación política como las oportunidades de participación ciudadana, afectando especialmente a grupos vulnerables. Se concluyó que la ausencia de marcos regulatorios coherentes incrementa los riesgos democráticos y de manipulación digital. El principal aporte del estudio consiste en visibilizar el nexo entre IA, democracia y seguridad informacional, ofreciendo lineamientos de política pública para fortalecer la integridad digital en contextos de competencia política.

Los estudios revisados coinciden en reconocer que la inteligencia artificial está redefiniendo los paradigmas de seguridad, defensa y gobernanza global. Mientras Campos Ríos (2025) y Pomares (2024) destacan la dimensión política y regulatoria de la IA en América Latina, Becker Castellaro et al. (2025) y Saavedra (2024) enfatizan los riesgos para la integridad informacional y la ciberseguridad regional. Por su parte, Meza Rivas (2019) y Macher Reyes (2021) abordan los dilemas ético-jurídicos de las armas autónomas, anticipando las tensiones entre innovación tecnológica y derecho humanitario. Se observa un vacío teórico en la integración de estos enfoques en un marco estratégico regional sobre guerra inteligente, lo que justifica la necesidad de la presente investigación sobre la evolución de la guerra inteligente y los desafíos estratégicos para la seguridad y defensa nacional en América Latina (2015–2025).

2.2 Bases Teóricas

2.2.1 Realismo político.

Slaughter (2004) plantea que los Estados actúan como agentes racionales que maximizan seguridad y poder dentro de un sistema anárquico, lo que conecta con la geopolítica tradicional y ofrece una base para leer la competencia estratégica en América Latina frente a la “guerra inteligente” y sus efectos sobre defensa nacional (Slaughter, 2004). Gatica (2025) complementa esta lectura al mostrar cómo la competencia EE. UU.–China en tecnologías digitales reconfigura narrativas de poder y, por tanto, reglas del juego estratégico en la región (Gatica, 2025). Mirzekhanov (2025) recuerda, además, que herencias histórico-institucionales, desde Viena hasta hoy, condicionan patrones de orden y conflicto, anclando el análisis realista en una temporalidad larga que incide sobre los desafíos actuales de seguridad (Mirzekhanov, 2025).

2.2.2 Constructivismo.

Flores y Vergara (2025) muestran que las identidades, normas e instituciones regionales (por ejemplo: ALBA-TCP) moldean la cooperación y el conflicto más allá de capacidades materiales, ofreciendo claves para entender arreglos de seguridad latinoamericanos en escenarios híbridos de guerra inteligente (Flores & Vergara, 2025). Luján (2023) añade que las percepciones latinoamericanas sobre el sistema mundial afectan preferencias de política exterior y, con ello, trayectorias de (in)seguridad, subrayando que las ideas públicas importan en el diseño estratégico (Luján, 2023).

2.2.3 Neorrealismo y realismo neoclásico

Slaughter (2004) y Gatica (2025) convergen en que capacidades y estructuras domésticas median la respuesta estatal frente a shocks tecnológicos,

lo que, en clave neoclásica, liga recursos materiales con variables internas para explicar política exterior y defensa (Slaughter, 2004; Gatica, 2025). Mirzekhanov (2025) refuerza que los legados institucionales sesgan el cálculo estratégico, articulando niveles sistémicos y domésticos (Mirzekhanov, 2025).

2.2.4 Modelos teóricos

Lash (2022) desarrolla un enfoque dual basado en la teoría de juegos para comprender las dinámicas estratégicas contemporáneas. Desde la teoría de juegos colaborativa, plantea que en la economía política y la seguridad internacional, especialmente en los ámbitos de la inversión extranjera directa (IED) y la competencia económica, las interacciones no se reducen a la rivalidad, sino que se estructuran en arreglos cooperativos que coexisten con la competencia geopolítica propia de la guerra inteligente. Paralelamente, mediante la teoría de juegos de conflicto puro, el autor analiza escenarios de suma cero donde el poder actúa como recurso escaso, lo que permite modelar confrontaciones en dominios cibernéticos, cognitivos y tecnológicos, característicos de los nuevos entornos de conflicto estratégico (Lash, 2022).

2.2.4 Aportes y perspectivas específicas para América Latina

Las relaciones cívico-militares en América Latina muestran signos de agotamiento temático y teórico, según Velandia Pardo y Betancur Montoya (2025), quienes abogan por una renovación de la agenda a partir de la convergencia entre racionalismo, estructuralismo y culturalismo. Esta combinación, afín al pluralismo integrador, permite abordar fenómenos contemporáneos como la “guerra inteligente” desde una perspectiva regional, reconociendo las interdependencias entre defensa, tecnología y sociedad. En paralelo, Kosevich (2023) reinterpreta la noción de autonomía e integración

como ejes fundamentales de la política exterior latinoamericana, señalando cómo las presiones internas y externas reconfiguran las capacidades de maniobra estratégica de los Estados frente a las potencias tecnológicas. Desde otro ángulo, Rivera-Rodríguez, Beltrán Duque y Sánchez-López (2025) exploran las conexiones entre estrategia y gestión, identificando tendencias de investigación en torno a desarrollo sostenible, innovación, turismo y comercio, y localizando polos productivos regionales, como Brasil, México, Colombia y Chile, que pueden articularse con la agenda de seguridad a través de la innovación tecnológica. Finalmente, Mares y Kacowicz (2015) ofrecen una síntesis de la agenda al estructurar un programa analítico sobre la evolución de la seguridad en América Latina, articulando los niveles micro y macro para comprender las relaciones cívico-militares, la gobernanza democrática y su vinculación con las transformaciones estratégicas derivadas de la guerra inteligente.

2.2.5 Modelos y arquitecturas aplicadas a guerra inteligente

Sharmila et al. (2025) desarrollan un marco impulsado por inteligencia artificial (IA) orientado a optimizar las misiones ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) dentro de redes tácticas avanzadas. Su propuesta integra vehículos autónomos y sensores inalámbricos sin batería, capaces de operar de manera coordinada en entornos hostiles, priorizando la eficiencia energética, la escalabilidad y la seguridad de las comunicaciones. Este enfoque busca fortalecer la conectividad y la autonomía operativa de los sistemas de defensa, ofreciendo una arquitectura adaptable y resiliente que refleja la convergencia entre inteligencia artificial, robótica y guerra.

Ding et al. (2024) desarrollan un sistema de combate urbano inteligente concebido a partir del marco DoDAF (Department of Defense Architecture

Framework) y del modelado SysML, combinando rigurosamente diagramas de casos de uso, definiciones de bloques, actividades y secuencias. Este enfoque arquitectónico permite anticipar y simular interacciones complejas entre unidades, sensores y entornos urbanos, configurando un modelo prospectivo para la planificación de operaciones en contextos densamente poblados. La propuesta no solo introduce innovaciones técnicas, sino que también ofrece una metodología replicable para el diseño de capacidades urbanas futuras, aplicable a escenarios donde la inteligencia artificial, la automatización y la toma de decisiones en tiempo real redefinen la naturaleza del combate.

2.2.6 Fundamentación Teórica de la Investigación

Slaughter (2004), Flores y Vergara (2025) y Mirzekhanov (2025) sostienen que el realismo y el constructivismo, anclados en una lectura histórica de larga duración, proveen un piso interpretativo robusto para comprender los desafíos estratégicos latinoamericanos en la era de la guerra inteligente, al articular tanto las dinámicas de poder como la construcción social del orden (Slaughter, 2004; Flores & Vergara, 2025; Mirzekhanov, 2025). En esa línea, en cuanto a herramientas analíticas, Lash (2022) introduce modelos de teoría de juegos colaborativos y de conflicto puro que permiten mapear zonas de cooperación/competencia y simular decisiones en cadenas de valor y dominios tecnológicos, claves para escenarios de disputa interestatal e intraestatal característicos de la “guerra inteligente” (Lash, 2022). Metodológicamente, Banta y Kaufman (2022) y Valizadeh y Kazemi (2022) proponen un pluralismo integrador y la lente de la cultura estratégica para captar la complejidad, historicidad y geografía de las opciones de seguridad y defensa, combinando niveles de análisis, métodos y fuentes en diseños que dialogan con las

especificidades regionales (Banta & Kaufman, 2022; Valizadeh & Kazemi, 2022). Desde perspectivas críticas y narrativas, Teschke y Pfaler (2024) y Gatica (2025) suman una lectura histórico-material y una cartografía de narrativas digitales que iluminan cómo se reordenan jerarquías y esferas de influencia en un ecosistema tecno-geopolítico cada vez más denso (Teschke & Pfaler, 2024; Gatica, 2025). Finalmente, en dominios emergentes, Gómez (2015), Castro Valdebenito y Monteverde Sánchez (2018) y Kefeli y colaboradores (2025) colocan la seguridad humana, la ciberseguridad y la seguridad cognitiva como ejes transversales de doctrinas y políticas de defensa, abriendo un abanico de problemas que van desde la protección de infraestructuras críticas hasta la integridad del espacio informacional y la conciencia pública (Gómez, 2015; Castro Valdebenito & Monteverde Sánchez, 2018; Kefeli et al., 2025). Todo ello converge en una agenda latinoamericana que, como muestran Velandia Pardo y Betancur Montoya (2025), Kosevich (2023), Rivera-Rodríguez y colegas (2025) y Mares y Kacowicz (2015), delimita líneas de investigación y capacidades institucionales para actualizar marcos y prácticas de seguridad en la región, integrando reformas cívico-militares, autonomía e integración, y ecosistemas de innovación estratégica (Velandia Pardo & Betancur Montoya, 2025; Kosevich, 2023; Rivera-Rodríguez et al., 2025; Mares & Kacowicz, 2015).

2.3 Marco Conceptual

2.3.1 Pluralismo integrador

Banta y Kaufman (2022) defienden combinar marcos (racionalistas, estructuralistas, culturalistas) para fenómenos complejos de seguridad, lo que habilita diseños analíticos multimétodo ante la convergencia ciber-tecnológica y operativa de la guerra inteligente (Banta & Kaufman, 2022).

2.3.2 Cultura estratégica.

Valizadeh y Kazemi (2022) muestran que geografía, historia y narrativas compartidas configuran patrones de decisión y respuesta ante amenazas, dimensión clave para leer repertorios latinoamericanos de disuasión, resiliencia y cooperación (Valizadeh & Kazemi, 2022).

2.3.3 Marxismo geopolítico.

Teschke y Pfaler (2024) integran materialismo histórico con análisis geopolítico para explicar formación de órdenes y dinámicas de poder, aportando una lente crítico-histórica para evaluar dependencias tecnológicas y asimetrías en la región (Teschke & Pfaler, 2024).

2.3.4 Geopolítica neoclásica.

Gatica (2025) combina capacidades materiales con factores ideacionales para analizar narrativas digitales que reconfiguran jerarquías y zonas de influencia, útil para mapear alineamientos y estrategias latinoamericanas (Gatica, 2025).

Geopolítica constructivista.

Flores y Vergara (2025) enfatizan la construcción social del orden y el rol de normas e instituciones, abriendo a hipótesis sobre cómo marcos regionales moldean prácticas de ciberdefensa y cooperación (Flores & Vergara, 2025).

2.3.5 Seguridad humana.

Gómez (2015) propone ampliar la seguridad hacia el ciudadano y el entramado social, lo que en América Latina dialoga con agendas de crimen organizado, ciber-amenazas y protección de infraestructuras críticas (Gómez, 2015).

2.3.6 Ciberseguridad.

Castro Valdebenito y Monteverde Sánchez (2018) documentan la adaptación hemisférica a nuevas tecnologías y avances cooperativos para sancionar el cibercrimen, plataforma imprescindible frente a la “guerra inteligente” (Castro Valdebenito & Monteverde Sánchez, 2018).

2.3.7 Guerra/ciberseguridad cognitiva.

Kefeli et al. (2025) conceptualizan la seguridad cognitiva como campo emergente de la guerra híbrida, centrado en operaciones sobre la conciencia pública y riesgos tecno-geopolíticos, clave para doctrinas y políticas de defensa (Kefeli et al., 2025).

2.4 Definición de Términos Básicos

Autonomía estratégica

Capacidad de un Estado, o de un bloque regional, para tomar decisiones soberanas en materia de seguridad y defensa sin dependencia crítica de actores externos en tecnologías militares, infraestructura digital o marcos doctrinarios. En América Latina, esta autonomía se ve limitada por la importación de sistemas y doctrinas de potencias como Estados Unidos y China, lo que condiciona la libertad de acción estratégica de la región (Kosevich, 2023; Campos, 2025; Krivolapov & Stepanova, 2023).

Ciberdefensa

Conjunto de doctrinas, capacidades técnicas y arreglos institucionales orientados específicamente a la protección militar y estratégica de infraestructuras críticas y sistemas de información frente a ataques cibernéticos, sabotaje digital y operaciones hostiles de penetración tecnológica. A diferencia de la ciberseguridad; que también cubre al ciudadano y al sector civil; la

ciberdefensa se sitúa en el campo de la defensa nacional y la seguridad estratégica del Estado (Saavedra, 2024).

Desinformación estratégica

Uso deliberado y técnicamente amplificado de contenidos manipulados, falsos o fuera de contexto con el fin de alterar percepciones públicas, deslegitimar instituciones democráticas o influir en procesos de decisión política y militar. La capacidad de generar y escalar desinformación mediante IA convierte este recurso en un vector directo de inestabilidad y, por tanto, en una amenaza de seguridad nacional (Becker et al., 2025; Luo et al., 2023).

Guerra cognitiva

Forma de confrontación que busca intervenir la voluntad política, la cohesión social y la percepción pública del adversario mediante operaciones psicológicas, manipulación algorítmica de la información y ataques a la confianza institucional. Se considera un dominio emergente de la guerra inteligente porque desplaza el conflicto hacia la esfera mental y social más que hacia el enfrentamiento físico directo (Luo et al., 2023; Zhang et al., 2022).

Guerra híbrida

Estrategia de conflicto que combina medios militares convencionales con ciberataques, sabotaje informacional, presión económica, uso de actores no estatales y operaciones psicológicas coordinadas. En el escenario de guerra inteligente, la guerra híbrida se fortalece con enjambres de drones, interferencia electrónica y IA aplicada a segmentar objetivos y narrativas en tiempo real (Zhang et al., 2022; Luo et al., 2023).

Guerra informacional

Disputa estratégica por el control de los flujos de información con valor militar, político y psicológico. Incluye la captura, bloqueo, distorsión o explotación prioritaria de datos críticos del adversario. En esta investigación se entiende como la base funcional tanto de la guerra cognitiva como de la guerra inteligente, dado que coloca la información, y no solo el territorio físico, como recurso central de poder (Zhang et al., 2022; Zhao et al., 2023).

Guerra inteligente

Transformación estructural de la guerra sustentada en la integración de inteligencia artificial, automatización bélica, percepción situacional en tiempo real, mando y control algorítmico y operaciones coordinadas en dominios múltiples (tierra, ciberespacio, espectro electromagnético, dimensión cognitiva). La guerra inteligente reduce los tiempos de decisión, baja los umbrales de uso de la fuerza y desplaza la ventaja estratégica hacia quien controla datos y capacidad de procesarlos (Long & Xu, 2022; Zhao et al., 2023; Tao & Yang, 2024; Wang et al., 2023).

Gobernanza tecnológica de la defensa

Arreglo normativo, ético e institucional mediante el cual un Estado intenta regular el desarrollo, la adquisición, la interoperabilidad y el uso operativo de tecnologías militares disruptivas (IA militar, armas autónomas, ciberarmas, vigilancia algorítmica). Supone asegurar control humano significativo sobre el empleo de la fuerza letal y mantener responsabilidad jurídica en contextos de automatización bélica (Long & Xu, 2020; Lu, 2024; Meza, 2019; Macher, 2021).

Inteligencia artificial militar

Aplicación de técnicas avanzadas de aprendizaje automático, visión computacional y procesamiento automático del lenguaje para ampliar velocidad, precisión, autonomía y letalidad de las decisiones militares. Incluye reconocimiento automático de objetivos, fusión de sensores, simulación de escenarios de combate y apoyo algorítmico al mando. Esta IA no solo acelera procesos: redefine quién decide, bajo qué criterios y a qué escala temporal se decide en un teatro de operaciones (Zhao et al., 2023; Tao & Yang, 2024; Wang et al., 2023).

Soberanía digital

Capacidad de un Estado para controlar y proteger sus infraestructuras críticas de información, sus datos estratégicos, sus cadenas tecnológicas y sus sistemas de decisión algorítmica sin quedar subordinado a proveedores, marcos regulatorios o arquitecturas técnicas externas. En América Latina, la soberanía digital es condición previa para cualquier forma real de autonomía estratégica en defensa y seguridad (Pomares, 2024; Campos, 2025).

CAPITULO III: METODOLOGÍA

3.1 Diseño Metodológico

3.1.1 Enfoque de Investigación

El presente estudio adopta un enfoque cualitativo, ya que busca interpretar las transformaciones doctrinarias, tecnológicas y estratégicas derivadas de la evolución de la guerra inteligente en América Latina, comprendiendo los significados, percepciones y racionalidades que subyacen a las políticas y estructuras de defensa regional. Según Hernández et al. (2021), el enfoque cualitativo se caracteriza por el análisis interpretativo de los fenómenos sociales en su contexto natural, priorizando la comprensión profunda antes que la medición estadística. Este enfoque resulta pertinente porque la investigación no pretende cuantificar variables, sino comprender las dinámicas de poder, gobernanza y autonomía tecnológica que emergen en los sistemas de defensa ante la revolución de la inteligencia artificial y las armas autónomas.

3.1.2 Tipo de Investigación

La investigación es de tipo teórico–empírico, dado que integra la revisión y sistematización de teorías estratégicas, geopolíticas y tecnológicas con el análisis documental de casos, doctrinas y marcos normativos regionales. De acuerdo con Bernal (2010), este tipo de estudio permite combinar la reflexión conceptual con la interpretación de datos y documentos empíricos, articulando teoría y evidencia en un mismo proceso analítico. En ese sentido, el estudio examina la literatura científica, informes institucionales y documentos estratégicos para interpretar la interacción entre innovación tecnológica y autonomía estratégica en los sistemas de defensa latinoamericanos.

3.1.3 Método de Investigación

Se emplea el método de estudio de caso múltiple comparativo, que permite analizar experiencias y doctrinas nacionales en materia de defensa y gobernanza tecnológica en América Latina. Yin (2018) señala que este método es idóneo cuando se busca comprender fenómenos complejos contemporáneos dentro de su contexto real, utilizando múltiples fuentes de evidencia. Los casos seleccionados: Brasil, Argentina, Chile, Colombia, México y Perú, representan distintos grados de desarrollo tecnológico y capacidades institucionales, permitiendo comparar respuestas nacionales ante los desafíos de la guerra inteligente. El método se sustenta en una lógica interpretativa y transversal, apoyada en la triangulación de fuentes secundarias, análisis documental y revisión estratégica.

3.1.4 Escenario de Estudio

El escenario de estudio está constituido por los sistemas nacionales de defensa y seguridad de América Latina, particularmente en su relación con la incorporación de tecnologías disruptivas de inteligencia artificial, ciberdefensa y armas autónomas. Este escenario incluye tanto el contexto institucional y doctrinario de los ministerios de defensa y fuerzas armadas, como el marco normativo y político que regula la cooperación tecnológica regional. En el plano conceptual, el estudio se sitúa en la intersección entre geopolítica, estrategia y gobernanza digital, ámbitos que definen el espacio de análisis donde se manifiestan las tensiones entre dependencia tecnológica, soberanía y modernización militar.

3.2 Diseño Muestral

La muestra es de carácter intencional, seleccionada según la relevancia estratégica, doctrinaria y tecnológica de los casos nacionales analizados. En investigación cualitativa, la selección intencional permite elegir informantes, documentos o contextos que aporten información significativa sobre el fenómeno de estudio (Patton, 2015).

En este caso, se consideran seis unidades de análisis principales: Brasil, Argentina, Chile, Colombia, México y Perú, representativas por su nivel de desarrollo en inteligencia artificial aplicada a la defensa, sus estrategias de ciberseguridad y sus modelos institucionales de gobernanza. Cada país se analiza a partir de documentos oficiales, estrategias nacionales, marcos normativos y literatura académica reciente (2015–2025). La muestra documental comprende 25 fuentes especializadas (artículos, *policy papers*, informes estratégicos, doctrinas y marcos legales), que constituyen el corpus para la interpretación comparativa.

La información básica de los cuatro expertos que entrevistamos es la siguiente:

- General EP VEGA CASTRO Hugo, Cmdte. Gral. de Operaciones Cibernéticas del Ejército del Perú. Con 15 años de experiencia en el campo de la ciberdefensa y Graduado de la escuela interamericana de defensa Washington DC– EEUU
- Coronel EP CONCHA LOAIZA Edgar, Director de la escuela de comunicaciones del Ejército del Perú. Oficial graduado en el Diplomado en operaciones de ciberseguridad dictado en la escuela George marshal center de Alemania año 2018.

- General EP(r) CASTILLO FUERMAN Luis, Doctor y magister en gestión y desarrollo en el instituto de ciencia y tecnología del ejercito (ICTE), con estudios en el programa de alta dirección y administración pública de la Universidad del Pacífico, así como graduado del Diplomado de “Mando Superior” en la Universidad de Defensa Nacional del Ejército Popular de Liberación de China.
- Coronel EP (r) CASSARETTO BARDALES Julio, Magister en Desarrollo y Defensa nacional en el Centro de Altos Estudios Nacionales (CAEN) y magister en Ciencias Militares por la ESGE-EPG. Docente de la escuela de guerra AF-2025.

3.3 Técnicas e Instrumentos de Recolección de Información

3.3.1 Técnicas

Se utilizaron tres técnicas principales de recolección de información:

- Entrevista a expertos.
- Análisis documental, aplicado a políticas, doctrinas y marcos regulatorios en defensa y tecnología.
- Revisión bibliográfica sistemática, orientada a identificar tendencias académicas y estratégicas sobre guerra inteligente, IA militar y autonomía tecnológica.
- Análisis comparativo, para establecer similitudes, diferencias y patrones regionales en las respuestas institucionales frente a la disrupción tecnológica.

Estas técnicas permiten construir una visión integradora del fenómeno, conforme a lo planteado por Flick (2014), quien sostiene que la triangulación metodológica fortalece la validez interpretativa en estudios cualitativos.

3.3.2 Instrumentos

Los instrumentos utilizados fueron:

- Guía de entrevista semiestructurada.
- Guía de análisis documental, diseñada para sistematizar la información según categorías temáticas: doctrina, tecnología, gobernanza, ética y cooperación.
- Ficha de registro bibliográfico, para clasificar autores, enfoques y aportes conceptuales relevantes.
- Matriz comparativa de países, donde se organizan las variables analíticas (capacidades tecnológicas, marcos normativos, autonomía estratégica y cooperación regional).

3.3.3 Validación de los Instrumentos

Los instrumentos fueron sometidos a validación por juicio de expertos, procedimiento recomendado por Martínez (2012) para asegurar la coherencia y pertinencia de los ítems respecto a los objetivos de investigación. Cinco especialistas en geopolítica, defensa y análisis estratégico de la Escuela Superior de Guerra del Ejército del Perú revisaron las guías, sugiriendo ajustes en las dimensiones “ética y gobernanza tecnológica” y “capacidad institucional”. Esta validación garantizó la pertinencia conceptual y metodológica de los instrumentos, los cuales se incluyen en los anexos correspondientes.

3.4 Técnicas para el Procesamiento de la Información

El procesamiento de la información siguió las etapas propuestas por Miles, Huberman y Saldaña (2014):

- Transcripción y organización de la información documental en una base de datos cualitativa.

- Codificación abierta y axial, para identificar categorías emergentes y relaciones temáticas.
- Análisis interpretativo y triangulación, combinando perspectivas teóricas, doctrinarias y normativas.

La información se sistematizó mediante el software Atlas.ti 25, permitiendo establecer redes semánticas y relaciones entre las categorías analíticas: guerra inteligente, autonomía estratégica, gobernanza tecnológica, cooperación regional y ética militar.

El proceso de análisis se orientó a construir un marco interpretativo de segunda generación, donde los hallazgos empíricos se articulan con los fundamentos teóricos revisados en el Capítulo II, conforme al principio de diálogo teórico-empírico característico de la investigación cualitativa interpretativa.

3.5 Aspectos Éticos

El estudio se desarrolló bajo los principios éticos de integridad académica, confidencialidad, transparencia y respeto a la propiedad intelectual, conforme a las recomendaciones de la Escuela Superior de Guerra del Ejército del Perú y a los lineamientos del Comité de Ética en Investigación.

Dado que la investigación se basa exclusivamente en fuentes secundarias, no involucra manipulación de personas ni tecnologías sensibles, por lo que no presenta riesgos éticos directos. Sin embargo, se adoptaron medidas de protección de datos y respeto a las fuentes utilizadas, garantizando la correcta citación y reconocimiento de autores conforme a las normas APA 7ª edición.

Además, el análisis aborda explícitamente los dilemas éticos de la guerra inteligente; autonomía de sistemas, uso de IA en decisiones letales y gobernanza

tecnológica; desde una perspectiva crítica y humanista, orientada a fortalecer la seguridad humana y la estabilidad estratégica regional

CAPÍTULO IV: ANÁLISIS Y SÍNTESIS

4.1 Definición de Categorías y Subcategorías

La investigación se estructura en torno a cuatro categorías analíticas que permiten comprender, desde una perspectiva integral, cómo la evolución de la guerra inteligente está reconfigurando los marcos de seguridad y defensa en América Latina. La Categoría 1, Impacto de la guerra inteligente, examina las transformaciones doctrinarias, la reconfiguración de las arquitecturas de seguridad, los riesgos emergentes derivados de la IA y los sistemas autónomos, así como los desafíos que enfrentan los Estados en términos de gobernanza tecno-militar, autonomía tecnológica y cooperación regional. Esta categoría responde directamente a la pregunta central sobre cómo la guerra inteligente impacta los marcos de seguridad, y articula los ejes que sustentan el primer objetivo de la investigación: interpretar la manera en que estas tecnologías reconfiguran las doctrinas y capacidades estratégicas de la región.

La Categoría 2, Capacidades estatales, aborda las dimensiones institucionales, doctrinarias y tecnológicas que determinan la capacidad de los Estados latinoamericanos para enfrentar amenazas emergentes, así como las brechas regionales y los niveles de preparación y resiliencia. En paralelo, la Categoría 3, Vacíos de gobernanza, identifica los déficits legales, éticos y operativos que dificultan el establecimiento de marcos regulatorios adecuados y que abren espacio a fenómenos como la captura tecnológica y la insuficiente rendición de cuentas. Finalmente, la Categoría 4, Competencia geoestratégica, analiza cómo la rivalidad China–Estados Unidos, la dependencia tecnológica y las respuestas regionales condicionan la autonomía estratégica latinoamericana

en un escenario global marcado por la disputa por tecnologías críticas. En conjunto, estas cuatro categorías permiten responder de manera articulada las preguntas y objetivos de la investigación, proporcionando un marco analítico robusto para interpretar las transformaciones, capacidades, vacíos y tensiones geoestratégicas que definen la inserción de América Latina en la era de la guerra inteligente.

Tabla 1

Definición de categorías, subcategorías y técnicas de recopilación de información

Categorías	Subcategorías	Técnicas
Categoría 1: Impacto de la guerra inteligente	- Transformación doctrinaria - Arquitectura de seguridad - Riesgos emergentes - Gobernanza tecno-militar - Autonomía tecnológica - Cooperación regional	Entrevistas Documentos
Categoría 2: Capacidades estatales	- Institucionales - Doctrinarias - Tecnológicas - Brechas regionales - Preparación y resiliencia	Entrevistas Documentos
Categoría 3: Vacíos de gobernanza	- Legal - Ético - Operativo - Captura tecnológica - Rendición de cuentas	Entrevistas Documentos
Categoría 4: Competencia geoestratégica	- Rivalidad China-EE. UU. - Dependencia tecnológica - Respuestas regionales - Autonomía estratégica - Agenda hemisférica	Entrevistas Documentos

4.1.1 Impacto de la guerra inteligente

Se refiere a los efectos estructurales, doctrinarios, tecnológicos y geopolíticos que produce la incorporación de inteligencia artificial, sistemas autónomos, ciberestrategias y tecnologías disruptivas en los marcos de seguridad y defensa de los Estados. Implica analizar cómo estas innovaciones transforman las capacidades militares, los patrones de conflicto y la manera en que se configura el poder en el ámbito internacional.

4.1.1.1 Transformación doctrinaria

Cambios en los principios, enfoques y concepciones operacionales de las fuerzas armadas derivados de la adopción de tecnologías inteligentes. Incluye la revisión de conceptos de disuasión, mando y control, superioridad informacional y empleo de sistemas autónomos.

4.1.1.2 Arquitectura de seguridad

Reconfiguración de estructuras institucionales, arreglos organizacionales, sistemas de vigilancia y modelos de coordinación interagencial necesarios para enfrentar amenazas híbridas, cibernéticas y asistidas por IA.

4.1.1.3 Riesgos emergentes

Amenazas nuevas o amplificadas generadas por la guerra inteligente, como ciberataques de alta escala, manipulación algorítmica, fallas autónomas, escalamiento inadvertido o vulnerabilidades en infraestructuras críticas.

4.1.1.4 Gobernanza tecno-militar

Conjunto de reglas, mecanismos de control, protocolos éticos y marcos institucionales que regulan el desarrollo y uso de tecnologías militares avanzadas. Incluye supervisión civil, estándares de transparencia y responsabilidad estatal.

4.1.1.5 Autonomía tecnológica

Capacidad de un Estado para desarrollar, adaptar o controlar tecnologías críticas sin depender de potencias externas. Supone infraestructura científica, sistemas de innovación y soberanía en datos, software y hardware estratégico.

4.1.1.6 Cooperación regional

Mecanismos de coordinación, intercambio de información, ejercicios conjuntos y construcción de capacidades entre países latinoamericanos para responder a amenazas de guerra inteligente de manera colectiva.

4.1.2 Capacidades estatales

Hace referencia al nivel de desarrollo institucional, doctrinario, tecnológico y organizacional que poseen los Estados para anticipar, prevenir, responder y adaptarse a los desafíos de la guerra inteligente. Evalúa su solidez institucional, preparación operativa y resiliencia estratégica.

4.1.2.1 Institucionales

Fortaleza organizacional del Estado en términos de normativa, procesos, recursos y liderazgo para gestionar amenazas tecnológicas avanzadas. Incluye

ministerios, fuerzas armadas, agencias de ciberseguridad y sistemas de inteligencia.

4.1.2.2 Doctrinarias

Grado de actualización y adecuación de las doctrinas militares y de seguridad frente a la guerra inteligente. Involucra adaptaciones conceptuales, reglas de enfrentamiento y nuevas formas de planeamiento estratégico.

4.1.2.3 Tecnológicas

Disponibilidad y dominio de tecnologías clave como IA, ciberdefensa, robótica militar, infraestructura digital segura y análisis masivo de datos. Considera brechas en equipamiento y absorción tecnológica.

4.1.2.4 Brechas regionales

Desigualdades entre países o regiones respecto a capacidades institucionales, tecnológicas y doctrinarias. Estas brechas inciden en la asimetría de amenazas, vulnerabilidades y capacidades de respuesta.

4.1.2.5 Preparación y resiliencia

Capacidad del Estado para anticipar escenarios de crisis, mantener funcionamiento bajo estrés tecnológico, recuperarse de ataques y adaptarse a entornos de alta incertidumbre derivados de la guerra inteligente.

4.1.3 Vacíos de gobernanza

Hace referencia a las áreas donde los marcos regulatorios, éticos, institucionales u operativos no alcanzan a controlar adecuadamente los riesgos

y desafíos asociados a la guerra inteligente. Estos vacíos generan zonas grises que pueden ser explotadas por actores estatales y no estatales.

4.1.3.1 Legal

Insuficiencia, ambigüedad o desactualización de leyes relacionadas con IA militar, ciberoperaciones, uso de datos, responsabilidad en sistemas autónomos y control de tecnologías duales.

4.1.3.2 Ético

Problemas morales que surgen por el uso de tecnologías capaces de tomar decisiones letales, procesar información sensible o intervenir en procesos sociales mediante algoritmos. Incluye el debate sobre autonomía letal y control humano significativo.

4.1.3.3 Operativo

Limitaciones en protocolos, manuales, estándares y mecanismos de coordinación que dificultan una respuesta eficaz ante amenazas tecnológicas avanzadas. Incluye brechas en interoperabilidad y en capacidad de despliegue rápido.

4.1.3.4 Captura tecnológica

Dependencia excesiva de proveedores privados o potencias tecnológicas que condicionan las decisiones del Estado y comprometen su soberanía operativa. Abarca desde software propietario hasta infraestructura crítica.

4.1.3.5 Rendición de cuentas

Déficits en transparencia, supervisión civil y fiscalización pública sobre decisiones y operaciones tecno-militares. Considera la opacidad en adquisición de tecnologías, uso de datos y responsabilidad por fallas.

4.1.4 Competencia geoestratégica

Dimensión que analiza cómo la disputa entre grandes potencias por tecnologías críticas influye en las decisiones, alineamientos y márgenes de autonomía de América Latina. Incluye rivalidades globales, dependencia tecnológica y configuraciones de poder regional.

4.1.4.1 Rivalidad China-EE. UU.

Competencia por liderazgo en IA, 5G, infraestructura digital, estándares tecnológicos y provisión de equipamiento militar que impacta en la región. Afecta alianzas, preferencias tecnológicas y acceso a innovación militar.

4.1.4.2 Dependencia tecnológica

Situación en la que los Estados latinoamericanos dependen de proveedores externos para sistemas estratégicos, lo que condiciona su autonomía y capacidad de respuesta. Incluye hardware, software, capacidades de ciberseguridad y acceso a datos.

4.1.4.3 Respuestas regionales

Acciones colectivas o fragmentadas desarrolladas por América Latina para enfrentar riesgos y oportunidades derivados de la guerra inteligente:

políticas conjuntas, marcos normativos, estrategias de ciberdefensa o cooperación en defensa.

4.1.4.4 Autonomía estratégica

Capacidad de un Estado o región para tomar decisiones soberanas en materia de seguridad y tecnología, sin quedar subordinado a potencias externas. Abarca independencia decisional, tecnológica y geopolítica.

4.1.4.5 Agenda hemisférica

Temas prioritarios y dinámicas de seguridad definidos en el marco interamericano (OEA, JID, mecanismos de defensa regional) que incorporan ciberseguridad, innovación tecnológica militar y cooperación en inteligencia.

4.2 Soporte de Categorías

En el desarrollo de la investigación “Evolución de la Guerra Inteligente y Desafíos Estratégicos para la Seguridad y Defensa Nacional en América Latina, 2015-2025”, el material recopilado mediante entrevistas y análisis documental permitió responder las preguntas de investigación: ¿Cómo está impactando la evolución de la guerra inteligente, incluyendo el uso militar de inteligencia artificial, armas autónomas y ciberestrategias, en los marcos de seguridad y defensa nacional de los países de América Latina, y qué desafíos estratégicos plantea en términos de gobernanza, autonomía tecnológica y cooperación regional? ¿Qué capacidades institucionales, doctrinarias y tecnológicas poseen los Estados latinoamericanos para responder a las amenazas emergentes de la guerra inteligente, y cómo varían dichas capacidades entre países? ¿Cuáles son los vacíos normativos, éticos y operativos más críticos en los marcos legales y

de gobernanza de América Latina frente a la proliferación de tecnologías de guerra inteligente? ¿Cómo influye la competencia geoestratégica entre grandes potencias, como China y Estados Unidos, en la configuración de las respuestas regionales frente a la guerra inteligente, y qué implicancias tiene ello para la autonomía estratégica de América Latina?

En las tablas que siguen a continuación se presenta el soporte de cada una de las categorías y subcategorías.

Tabla 2

Soporte de la categoría 1: Impacto de la guerra inteligente (guía de entrevistas semiestructuradas)

Subcategorías	Entrevistado	Unidades de significado
Arquitectura de seguridad	1. Coronel EP Edgar Concha Loaiza	en el marco de la OEA, ya existe y está en plena ejecución una red de cooperación mutua en este campo
Arquitectura de seguridad	1. Coronel EP Edgar Concha Loaiza	Esta red opera bajo la dirección de la Junta Interamericana de Defensa (JID), donde contamos con muchos especialistas
Arquitectura de seguridad	1. Coronel EP Edgar Concha Loaiza	Países como México y Brasil apoyan directamente a la JID y dan soporte con sus expertos
Arquitectura de seguridad	2. Gral. EP Dr. Ernesto Castillo Fuerman	Esto ha generado una ruptura doctrinal significativa. En la guerra cibernética, el atacante tiene una ventaja estructural sobre el defensor, configurando un escenario de guerra asimétrica donde incluso países con menor desarrollo tecnológico pueden generar efectos estratégicos sobre potencias tecnológicamente avanzadas.
Arquitectura de seguridad	2. Gral. EP Dr. Ernesto Castillo Fuerman	Varios países de la región ya han creado sus comandos de ciberdefensa y están avanzando en cooperación técnica, pero aún enfrentamos el reto de consolidar una autonomía tecnológica regional, con capacidad de respuesta ante amenazas híbridas y cibernéticas.
Arquitectura de seguridad	3. Gral. EP Hugo Vega Castro	la guerra inteligente exige que los Estados desarrollen una arquitectura de seguridad más integrada, dinámica y anticipatoria, capaz de responder simultáneamente en los ámbitos físico, informático y cognitivo.

Arquitectura de seguridad	4. Coronel EP Julio Sebastian Cassareto	Desde el Comando Conjunto de las Fuerzas Armadas se ha creado un Comando Operacional de Ciberdefensa, encargado de enfrentar las amenazas digitales
Arquitectura de seguridad	4. Coronel EP Julio Sebastian Cassareto	la arquitectura de seguridad regional, esta continúa centrada en el intercambio de información e inteligencia sobre amenazas tradicionales
Autonomía tecnológica	1. Coronel EP Edgar Concha Loaiza	Latinoamérica, en general, actúa como compradora, no como desarrolladora de tecnología militar
Autonomía tecnológica	1. Coronel EP Edgar Concha Loaiza	La segunda debilidad es la escasa Industria Militar Nacional (IMN)
Autonomía tecnológica	1. Coronel EP Edgar Concha Loaiza	indican que estamos aprendiendo la importancia de fomentar una IMN para generar valor económico y asegurar nuestra propia resiliencia tecnológica.
Autonomía tecnológica	2. Gral. EP Dr. Ernesto Castillo Fuerman	Solicitamos a nuestros ingenieros realizar ingeniería inversa —el programa estaba desarrollado en lenguaje C— y logramos reducir ese tiempo a una semana. Cuando los técnicos franceses vieron los resultados, se sorprendieron de nuestra capacidad de adaptación. Esto demostró que el conocimiento y la innovación local pueden compensar la dependencia tecnológica externa.
Autonomía tecnológica	2. Gral. EP Dr. Ernesto Castillo Fuerman	la base de la soberanía tecnológica reside en la formación de capital humano capaz no solo de operar herramientas, sino de desarrollarlas y adaptarlas.
Autonomía tecnológica	2. Gral. EP Dr. Ernesto Castillo Fuerman	Hoy, uno de los principales desafíos para los países latinoamericanos es superar la dependencia tecnológica

Autonomía tecnológica	3. Gral. EP Hugo Vega Castro	En cuanto a la autonomía tecnológica, América Latina aún se encuentra en una etapa incipiente. Los países de la región están dando sus primeros pasos en el desarrollo de tecnología propia, lo cual es indispensable para alcanzar una verdadera soberanía digital.
Autonomía tecnológica	3. Gral. EP Hugo Vega Castro	La soberanía tecnológica implica no solo la capacidad de usar tecnología, sino de crearla, adaptarla y protegerla conforme a los intereses nacionales.
Autonomía tecnológica	4. Coronel EP Julio Sebastian Cassareto	las Fuerzas Armadas han comenzado a enviar oficiales al extranjero para capacitarse en ciberdefensa e inteligencia artificial
Autonomía tecnológica	4. Coronel EP Julio Sebastian Cassareto	desarrollar software propio, generar cierta autonomía tecnológica y crear capacidades locales que nos permitan enfrentar los retos del ciberespacio.
Cooperación regional	1. Coronel EP Edgar Concha Loaiza	la Junta Interamericana de Defensa (JID) mantiene una cooperación regional activa en materia de tecnología, ciberseguridad, terrorismo y guerra híbrida. Contamos con una red de contactos que incluye a todos los Estados miembros del continente americano.
Cooperación regional	1. Coronel EP Edgar Concha Loaiza	Contamos con una red de contactos que incluye a todos los Estados miembros del continente americano.
Cooperación regional	1. Coronel EP Edgar Concha Loaiza	rantizar la capacitación. Hay una comunidad académica activa en las Escuelas Superiores de Guerra y en los centros de estudios nacionales.
Cooperación regional	2. Gral. EP Dr. Ernesto Castillo Fuerman	Asimismo, otra gran debilidad es la falta de cooperación regional estructurada. Si bien existen foros y reuniones impulsadas principalmente por países como Brasil o Estados Unidos, todavía no se ha logrado establecer un mecanismo sólido y continuo de intercambio de información, desarrollo conjunto o entrenamiento interoperable

Cooperación regional	2. Gral. EP Dr. Ernesto Castillo Fuerman	Este enfoque polarizado obstaculiza la cooperación técnica abierta, ya que coloca a los países latinoamericanos en la disyuntiva de alinearse con uno u otro bloque, cuando en realidad cada Estado debería actuar conforme a sus propios intereses estratégicos y de soberanía tecnológica
Cooperación regional	3. Gral. EP Hugo Vega Castro	La cooperación debe estructurarse sobre tres pilares fundamentales: el Estado, las Fuerzas Armadas y la Academia. Esta trilogía es esencial para fortalecer la resiliencia nacional, compartir conocimiento, desarrollar tecnología y construir capacidades conjuntas que permitan enfrentar amenazas híbridas.
Cooperación regional	3. Gral. EP Hugo Vega Castro	En la medida en que se logre articular este trabajo conjunto, la región podrá avanzar hacia una posición más sólida y autónoma en el nuevo escenario global de poder digital.
Cooperación regional	4. Coronel EP Julio Sebastian Cassareto	Existen vínculos de cooperación activa entre países vecinos —Perú, Ecuador, Colombia, Brasil, Bolivia y Chile
Cooperación regional	4. Coronel EP Julio Sebastian Cassareto	Este país (Brasil) incluso coopera con naciones vecinas, como el Perú, enviando oficiales y asesores especializados
Cooperación regional	4. Coronel EP Julio Sebastian Cassareto	las relaciones de cooperación se reducen a ejercicios bilaterales o a intercambios puntuales con Estados Unidos
Gobernanza tecno-militar	1. Coronel EP Edgar Concha Loaiza	La elección de tecnologías dependerá muchísimo de la orientación política que tenga cada país.
Gobernanza tecno-militar	1. Coronel EP Edgar Concha Loaiza	Los desafíos que enfrentarán algunos países serán definidos por la elección del lado tecnológico al que se inclinen.

Gobernanza tecno-militar	1. Coronel EP Edgar Concha Loaiza	Esta situación es un dilema que yo calificaría como una 'guerra fría' en materia tecnológica
Gobernanza tecno-militar	2. Gral. EP Dr. Ernesto Castillo Fuerman	En muchos casos, los líderes políticos y administrativos carecen de conocimiento sobre cómo la tecnología impacta la seguridad y la defensa. Mientras no se comprenda que el dominio cibernético es tan sensible y letal como el terrestre, marítimo o aéreo, persistirán las demoras, las interpretaciones erróneas y la falta de respuesta oportuna ante ataques reales.
Gobernanza tecno-militar	3. Gral. EP Hugo Vega Castro	Respecto a la gobernanza tecno-militar, algunos avances normativos han comenzado a consolidarse en la región. Existen marcos legales que buscan regular el uso de las tecnologías emergentes en defensa y seguridad, pero aún son insuficientes para enfrentar la velocidad con que evoluciona la innovación tecnológica.
Gobernanza tecno-militar	3. Gral. EP Hugo Vega Castro	Se requiere una gobernanza flexible, basada en principios éticos, jurídicos y estratégicos que garanticen el control civil, la transparencia y la rendición de cuentas, sin obstaculizar el desarrollo de capacidades defensivas.
Gobernanza tecno-militar	4. Coronel EP Julio Sebastian Cassareto	esa falta de cohesión limita cualquier posibilidad de construir una verdadera gobernanza tecno-militar regional.
Riesgos emergentes	1. Coronel EP Edgar Concha Loaiza	la mayor amenaza en Latinoamérica, incluso por encima de la rivalidad comercial entre potencias, es el Crimen Transnacional Organizado (CTO)
Riesgos emergentes	1. Coronel EP Edgar Concha Loaiza	El CTO se fortalece anualmente, posee sistemas logísticos eficientes y una capacidad de coerción interna efectiva
Riesgos emergentes	1. Coronel EP Edgar Concha Loaiza	Sus vastas ganancias les permiten adquirir tecnología militar avanzada, como el uso de drones para atacar instalaciones

Riesgos emergentes	2. Gral. EP Dr. Ernesto Castillo Fuerman	La guerra inteligente no busca únicamente destruir, sino desestabilizar la voluntad del adversario atacando su infraestructura vital: sistemas de energía, transporte, comunicaciones, redes financieras o plataformas logísticas. Es un tipo de guerra que puede paralizar un país sin necesidad de un solo disparo. Por eso debemos comprender que el futuro de la defensa pasa por la capacidad de proteger el entorno digital, desarrollar tecnología propia y formar especialistas capaces de operar en estos nuevos dominios.
Riesgos emergentes	3. Gral. EP Hugo Vega Castro	Un ataque cibernético que paralice la infraestructura de salud o energética de un país puede ponerlo de rodillas sin necesidad de un solo disparo.
Riesgos emergentes	4. Coronel EP Julio Sebastian Cassareto	un ataque cibernético puede desestabilizar a un país sin necesidad de disparar un solo proyectil.
Riesgos emergentes	4. Coronel EP Julio Sebastian Cassareto	El narcotráfico y la minería ilegal van a incorporar pronto herramientas basadas en IA para mejorar sus operaciones
Transformación doctrinaria	1. Coronel EP Edgar Concha Loaiza	En casi todos los países de Suramérica, ya existen avances importantes en ciberdefensa y estrategias de ciberseguridad
Transformación doctrinaria	1. Coronel EP Edgar Concha Loaiza	Sin embargo, hay un vacío esencial: no existe una guía de ciberdefensa unificada para el diseño, planeamiento e implementación de las unidades militares en la región. Ahí es donde radica el problema.
Transformación doctrinaria	1. Coronel EP Edgar Concha Loaiza	Todos los Estados tienen estrategias de ciberseguridad, y la IA se está empleando en la toma de decisiones,
Transformación doctrinaria	2. Gral. EP Dr. Ernesto Castillo Fuerman	A través de estas simulaciones —defensivas, ofensivas o de reconocimiento— los oficiales podían observar en tiempo real las consecuencias de sus decisiones, modificando así la rigidez tradicional de la doctrina militar.

Transformación doctrinaria	2. Gral. EP Dr. Ernesto Castillo Fuerman	Estas experiencias demostraron que la doctrina clásica debía adaptarse a un entorno donde la inteligencia artificial y los sistemas de detección en tiempo real redefinen las reglas del combate.
Transformación doctrinaria	4. Coronel EP Julio Sebastian Cassareto	las ciberestrategias están transformando las doctrinas y arquitecturas de seguridad de manera desigual en cada país.
Transformación doctrinaria	4. Coronel EP Julio Sebastian Cassareto	cada instituto armado —Ejército, Marina y Fuerza Aérea— cuenta con sus propias divisiones de ciberdefensa, lo que demuestra un proceso de adaptación doctrinaria en marcha

Tabla 3

Soporte de la categoría 2: Capacidades estatales (guía de entrevistas semiestructuradas)

Subcategorías	Entrevistado	Unidades de significado
Doctrinarias	1. Coronel EP Edgar Concha Loaiza	existe una estructura de cooperación ya establecida a través de la Junta Interamericana de Defensa (JID), que provee una base en doctrina y capacidades de ciberdefensa y ciberseguridad.
Institucionales	1. Coronel EP Edgar Concha Loaiza	Las instituciones (FF. AA.) están sujetas a inspecciones, auditorías internas y al control directo de organismos estatales
Doctrinarias	1. Coronel EP Edgar Concha Loaiza	cooperación ya establecida a través de la Junta Interamericana de Defensa (JID), que provee una base en doctrina y capacidades de ciberdefensa y ciberseguridad.
Doctrinarias	1. Coronel EP Edgar Concha Loaiza	Vacíos Éticos: La ausencia de una legislación específica o de una doctrina interna sobre el uso de la IA en defensa genera automáticamente vacíos éticos.
Tecnológicas	1. Coronel EP Edgar Concha Loaiza	Esto resulta en una pérdida progresiva de capacidad para adquirir nuevas tecnologías y genera una significativa brecha de innovación.
Brechas regionales	1. Coronel EP Edgar Concha Loaiza	Los presupuestos de defensa en nuestros países son históricamente bajos
Brechas regionales	1. Coronel EP Edgar Concha Loaiza	la mayoría de nuestros sistemas de armas no son autónomo

Brechas regionales	1. Coronel EP Edgar Concha Loaiza	la mayoría de los países luchan por establecer industrias competitivas.
Preparación y resiliencia	1. Coronel EP Edgar Concha Loaiza	Identifico dos debilidades estructurales clave en materia de preparación, innovación y resiliencia tecnológica de defensa en la región.
Preparación y resiliencia	1. Coronel EP Edgar Concha Loaiza	El contexto de conflictos recientes nos obliga a priorizar urgentemente el desarrollo o ensamblaje de tecnologías de menor coste, como los drones y la IA, en lugar de depender únicamente de costosas adquisiciones tradicionales.
Institucionales	2. Gral. EP Dr. Ernesto Castillo Fuerman	En el año 2010, se me encomendó la creación del Centro de Simulación Táctica del Ejército, un proyecto que marcó un punto de inflexión en el uso de tecnologías emergentes dentro de las Fuerzas Armadas. En ese contexto, formulé el proyecto de inversión pública, supervisé la construcción de las instalaciones y, durante los dos primeros años, incorporamos un software francés con inteligencia artificial que nos permitió realizar simulaciones virtuales de escenarios tácticos.
Institucionales	2. Gral. EP Dr. Ernesto Castillo Fuerman	Aunque la ley establecía un plazo de 60 días para su reglamentación, el proceso tomó cinco años debido a la falta de comprensión técnica y legal sobre la materia. Algunos funcionarios civiles creían, por ejemplo, que podían comandar operaciones cibernéticas militares, cuando en realidad el mando de las Fuerzas Armadas recae constitucionalmente en el Presidente de la República, a través del Consejo de Defensa Nacional.
Tecnológicas	2. Gral. EP Dr. Ernesto Castillo Fuerman	Las capacidades institucionales, doctrinarias y tecnológicas de los Estados latinoamericanos para enfrentar los escenarios de guerra inteligente y amenazas híbridas aún se encuentran en una etapa inicial de desarrollo. Si bien se han logrado avances importantes, persisten brechas significativas en materia de preparación, innovación y resiliencia tecnológica.

Tecnológicas	2. Gral. EP Dr. Ernesto Castillo Fuerman	Este ataque expuso vulnerabilidades críticas en los sistemas de seguridad digital de varios países latinoamericanos y puso en evidencia las limitaciones estructurales de sus mecanismos de defensa cibernética.
Brechas regionales	2. Gral. EP Dr. Ernesto Castillo Fuerman	a nivel regional, aún existe una brecha considerable para alcanzar una seguridad cooperativa efectiva en materia de defensa cibernética.
Brechas regionales	2. Gral. EP Dr. Ernesto Castillo Fuerman	la interconectividad regional también puede convertirse en una fuente de riesgo compartido. Estos incidentes confirman que, a nivel regional, aún existe una brecha considerable para alcanzar una seguridad cooperativa efectiva en materia de defensa cibernética.
Preparación y resiliencia	2. Gral. EP Dr. Ernesto Castillo Fuerman	Hacia el año 2030, el principal desafío estratégico para América Latina será proteger su soberanía digital y garantizar la seguridad de sus activos críticos frente a las nuevas dinámicas de la guerra inteligente. La guerra contemporánea ya no depende del poder de fuego o del número de tropas, sino del control del espacio digital y de la información. En este contexto, el espacio digital tiene fronteras solo en la medida en que puede ser protegido; cuando no existe capacidad para hacerlo, esas fronteras se diluyen y con ellas la autonomía del Estado. Por eso, la protección del ciberespacio se ha convertido en un componente esencial de la soberanía nacional.
Preparación y resiliencia	2. Gral. EP Dr. Ernesto Castillo Fuerman	la protección del ciberespacio se ha convertido en un componente esencial de la soberanía nacional
Preparación y resiliencia	2. Gral. EP Dr. Ernesto Castillo Fuerman	Necesitamos invertir en hardware estratégico, en centros de datos soberanos y en algoritmos que respondan a nuestras propias necesidades
Preparación y resiliencia	3. Gral. EP Hugo Vega Castro	En cuanto a la preparación y capacitación, existen esfuerzos aislados, pero no articulados bajo una estrategia regional común.

Preparación y resiliencia	3. Gral. EP Hugo Vega Castro	la región muestra voluntad y algunos progresos normativos, pero aún carece de una visión estratégica conjunta que integre inversión tecnológica, desarrollo del conocimiento y cooperación efectiva para fortalecer la resiliencia y la capacidad de defensa
Brechas regionales	3. Gral. EP Hugo Vega Castro	A ello se suma la ausencia de marcos regulatorios homogéneos: cada país posee su propio marco legal, lo que dificulta la cooperación y la interoperabilidad entre naciones.
Brechas regionales	3. Gral. EP Hugo Vega Castro	Las iniciativas tienden a responder a intereses institucionales o nacionales más que a un objetivo compartido, lo que fragmenta los avances.
Tecnológicas	3. Gral. EP Hugo Vega Castro	Todavía dependemos en gran medida de tecnologías extranjeras, lo que impide alcanzar una verdadera soberanía tecnológica.
Tecnológicas	3. Gral. EP Hugo Vega Castro	La brecha más significativa en la región es precisamente la falta de capacidad para desarrollar tecnología propia.
Doctrinarias	3. Gral. EP Hugo Vega Castro	Las doctrinas militares tradicionales han debido adaptarse al concepto de operaciones multidominio, donde la ciberdefensa, la inteligencia artificial y los sistemas autónomos convergen en un mismo escenario operacional.
Brechas regionales	3. Gral. EP Hugo Vega Castro	Considero que las capacidades institucionales, doctrinarias y tecnológicas de los Estados latinoamericanos para responder a escenarios de guerra inteligente y amenazas híbridas aún se encuentran en un nivel bajo a medio.
Brechas regionales	3. Gral. EP Hugo Vega Castro	Existen avances normativos y algunas iniciativas en materia de modernización y ciberdefensa, pero la inversión en investigación, desarrollo e innovación sigue siendo muy limitada.
Preparación y resiliencia	4. Coronel EP Julio Sebastian Cassareto	la más profunda es la brecha de conocimiento. En América Latina hay un número reducido de especialistas en guerra inteligente, inteligencia artificial y ciberdefensa.

Preparación y resiliencia	4. Coronel EP Julio Sebastian Cassareto	El principal desafío que tienen los países de la región tiene que ver con el conocimiento: debemos generar una cultura del conocimiento sobre las nuevas tecnologías
Brechas regionales	4. Coronel EP Julio Sebastian Cassareto	Las capacidades institucionales, doctrinarias y tecnológicas de los Estados latinoamericanos para enfrentar escenarios de guerra inteligente y amenazas híbridas son profundamente desiguales
Brechas regionales	4. Coronel EP Julio Sebastian Cassareto	En contraste, países con menor desarrollo económico o institucional, como Haití, Honduras o Guatemala, prácticamente carecen de estructuras
Brechas regionales	4. Coronel EP Julio Sebastian Cassareto	América Latina avanza a distintas velocidades: algunos países están dando los primeros pasos hacia una autonomía digital y una doctrina de defensa tecnológica, mientras que otros permanecen prácticamente al margen
Doctrinarias	4. Coronel EP Julio Sebastian Cassareto	el Perú ha comenzado a desarrollar manuales, reglamentos y doctrina para que se pueda enseñar en los diferentes cursos y programas dentro del Ejército
Brechas regionales	4. Coronel EP Julio Sebastian Cassareto	Brasil se ubica claramente a la vanguardia: cuenta con una industria militar sólida, un presupuesto considerable destinado a defensa

Tabla 4

Soporte de la categoría 3: Vacíos de gobernanza (guía de entrevistas semiestructuradas)

Subcategorías	Entrevistado	Unidades de significado
Doctrinarias	1. Coronel EP Edgar Concha Loaiza	existe una estructura de cooperación ya establecida a través de la Junta Interamericana de Defensa (JID), que provee una base en doctrina y capacidades de ciberdefensa y ciberseguridad.
Operativo	1. Coronel EP Edgar Concha Loaiza	y la IA se está empleando en la toma de decisiones, pero creo que su implementación no es aún sostenible porque no hay presupuestos exclusivos y robusto
Legal	1. Coronel EP Edgar Concha Loaiza	no existe una Ley de IA específica para las Fuerzas Armadas (FF. AA.). Esto representa un vacío legal crucial.
Legal	1. Coronel EP Edgar Concha Loaiza	Las FF. AA. se verán obligadas a sujetarse a la normativa civil, lo cual es insuficiente,
Ético	1. Coronel EP Edgar Concha Loaiza	Vacíos Éticos: La ausencia de una legislación específica o de una doctrina interna sobre el uso de la IA en defensa genera automáticamente vacíos éticos
Ético	1. Coronel EP Edgar Concha Loaiza	Sin directrices claras sobre la toma de decisiones algorítmica, el sesgo de datos, y la responsabilidad en el uso de sistemas inteligentes, el accionar militar puede quedar expuesto a dilemas morales y jurídicos no resueltos.
Operativo	1. Coronel EP Edgar Concha Loaiza	Finalmente, la falta de una ley específica y, por ende, de una gobernanza formalizada de las tecnologías militares inteligentes

Operativo	1. Coronel EP Edgar Concha Loaiza	se traduce en vacíos operativos. Esto obstaculiza la estandarización, la adquisición segura, la interoperabilidad y, en última instancia, la capacidad de las FF. AA. para integrar estas herramientas de manera efectiva y regulada.
Rendición de cuentas	1. Coronel EP Edgar Concha Loaiza	El riesgo real reside en la atribución de la responsabilidad cuando una decisión o acción militar basada en la IA resulta errónea
Rendición de cuentas	1. Coronel EP Edgar Concha Loaiza	La dependencia tecnológica podría dificultar la auditoría del algoritmo o sistema,
Gobernanza tecno-militar"	2. Gral. EP Dr. Ernesto Castillo Fuerman	La dependencia tecnológica de proveedores extranjeros no solo compromete la soberanía, sino que puede generar captura tecnológica, limitando la autonomía de decisión nacional.
Legal	2. Gral. EP Dr. Ernesto Castillo Fuerman	Por ejemplo, el Perú promulgó recientemente una Ley de Inteligencia Artificial (2024), pero esta no aborda las implicancias de la IA en el ámbito de la defensa nacional. Este vacío evidencia la necesidad urgente de desarrollar marcos normativos integrales, que consideren aspectos de seguridad, ética algorítmica, control civil, soberanía tecnológica y responsabilidad operativa.
Legal	2. Gral. EP Dr. Ernesto Castillo Fuerman	Es indispensable implementar mecanismos de vigilancia y auditoría algorítmica para evitar abusos, vulneraciones de derechos o usos indebidos en vigilancia y control. Sin embargo, en la región aún estamos rezagados en estos aspectos.
Ético	2. Gral. EP Dr. Ernesto Castillo Fuerman	Mi recomendación fue impulsar una armonización regional de normas sobre inteligencia artificial, orientada a garantizar principios éticos, legales y de transparencia, especialmente en el uso militar de algoritmos. Es indispensable implementar mecanismos de vigilancia y auditoría algorítmica para evitar abusos, vulneraciones de derechos o usos indebidos en vigilancia y control. Sin embargo, en la región aún estamos rezagados en estos aspectos.

Operativo	2. Gral. EP Dr. Ernesto Castillo Fuerman	Sin esa adecuación legal, las unidades de ciberdefensa no podían recibir recursos ni operar formalmente, lo que generaba riesgos de observaciones presupuestarias o vacíos de responsabilidad.
Rendición de cuentas	3. Gral. EP Hugo Vega Castro	Asimismo, la región carece de un organismo regional que supervise, evalúe o exija rendición de cuentas sobre el desarrollo y la implementación de tecnologías militares inteligentes.
Rendición de cuentas	3. Gral. EP Hugo Vega Castro	En ese contexto, una eventual “captura tecnológica” sería catastrófica, ya que colocaría recursos esenciales en manos de terceros y limitaría la capacidad de los Estados para tomar decisiones independientes en materia de defensa y seguridad.
Operativo	3. Gral. EP Hugo Vega Castro	La coordinación entre el ámbito civil y militar es todavía muy limitada, y persiste una marcada desconexión entre la inversión pública y privada en innovación tecnológica.
Ético	3. Gral. EP Hugo Vega Castro	No existe una normativa regional que determine con precisión quién asume la responsabilidad ante el uso indebido o los daños provocados por sistemas autónomos, lo que deja un amplio margen de incertidumbre ética y jurídica.
Ético	3. Gral. EP Hugo Vega Castro	No existen leyes que establezcan controles medioambientales, éticos o de responsabilidad social en los proyectos vinculados al desarrollo de defensa tecnológica
Legal	3. Gral. EP Hugo Vega Castro	Los principales vacíos en la gobernanza de las tecnologías militares inteligentes en América Latina se evidencian en la ausencia de marcos regulatorios claros y actualizados sobre el uso de inteligencia artificial aplicada a la defensa, así como en la falta de legislación específica para las armas autónomas.

Tabla 5

Soporte de la categoría 4: Vacíos de gobernanza (guía de entrevistas semiestructuradas)

Subcategorías	Entrevistado	Unidades de significado
Rivalidad China-EE. UU.	1. Coronel EP Edgar Concha Loaiza	La competencia geoestratégica entre China y Estados Unidos tiene una influencia directa y creciente en la configuración de las políticas de defensa y seguridad de América Latina, especialmente frente a la guerra inteligente. Actualmente, la región se encuentra en un periodo de competencia activa entre ambas potencias.
Rivalidad China-EE. UU.	1. Coronel EP Edgar Concha Loaiza	China ha escalado sus ofrecimientos militares y académicos. Esto incluye becas y cursos de estudio en el continente asiático, generando una competencia directa en la esfera de la formación de élites militares en la región.
Dependencia tecnológica	1. Coronel EP Edgar Concha Loaiza	a integración de la Inteligencia Artificial (IA) nos obliga a utilizar herramientas proporcionadas por empresas externas, lo que inmediatamente implica una pérdida de soberanía. Si una nación, como Perú, no tiene una base de datos soberana que gen
Dependencia tecnológica	1. Coronel EP Edgar Concha Loaiza	El nivel de control que se mantenga estará directamente ligado a los acuerdos de seguridad negociados con el proveedor.
Respuestas regionales	1. Coronel EP Edgar Concha Loaiza	Actualmente, la región se encuentra en un periodo de competencia activa entre ambas potencias.
Respuestas regionales	1. Coronel EP Edgar Concha Loaiza	Las políticas de defensa deberán decidir, en algún momento, el alineamiento estratégico a largo plazo con uno u otro polo de poder.
Autonomía estratégica	1. Coronel EP Edgar Concha Loaiza	Sobre la posibilidad de que la región construya una autonomía estratégica y una agenda hemisférica propia en materia de seguridad y desarrollo tecnológico militar, considero que esta posibilidad es sumamente difícil en el contexto actual.

Agenda hemisférica	1. Coronel EP Edgar Concha Loaiza	La agenda hemisférica de seguridad ya está fuertemente definida por estos nexos. Hay que notar que el alineamiento de algunos países (como Venezuela, Cuba o Bolivia) responde a sus propias ideologías políticas.
Agenda hemisférica	1. Coronel EP Edgar Concha Loaiza	Para construir una capacidad estratégica cohesiva, es imperativo recuperar y fortalecer iniciativas de integración regional como la antigua UNASUR (Unión de Naciones Suramericanas)
Rivalidad China-EE. UU.	2. Gral. EP Dr. Ernesto Castillo Fuerman	Esa experiencia me permite afirmar que América Latina, y particularmente el Perú, se encuentran en una posición intermedia y compleja dentro de esa competencia tecnológica y estratégica entre potencias.
Rivalidad China-EE. UU.	2. Gral. EP Dr. Ernesto Castillo Fuerman	Este enfoque polarizado obstaculiza la cooperación técnica abierta, ya que coloca a los países latinoamericanos en la disyuntiva de alinearse con uno u otro bloque, cuando en realidad cada Estado debería actuar conforme a sus propios intereses estratégicos y de soberanía tecnológica.
Dependencia tecnológica	2. Gral. EP Dr. Ernesto Castillo Fuerman	Contamos con armamento de origen ruso, como los sistemas de artillería BM-21 “Grad”, mientras que la aviación opera equipos de procedencia francesa, entre otros. Cada sistema utiliza plataformas informáticas y protocolos distintos, lo que genera una interoperabilidad muy limitada. Este mosaico de tecnologías de diverso origen nos obliga a definir con claridad qué rumbo o estrategia tecnológica queremos seguir como país y como región.
Dependencia tecnológica	2. Gral. EP Dr. Ernesto Castillo Fuerman	En el caso de Perú, tenemos hoy activos críticos de alta relevancia bajo gestión extranjera. Por ejemplo, el puerto de Chancay, operado por una empresa china, y próximamente la estación espacial de la NASA en Paita. Ambos reflejan cómo nuestra posición geoestratégica puede generar tanto oportunidades de cooperación como riesgos de dependencia tecnológica. Lo ideal sería buscar un equilibrio: alianzas estratégicas amigables y de beneficio mutuo, que fortalezcan nuestras capacidades sin comprometer la soberanía.

Respuestas regionales	2. Gral. EP Dr. Ernesto Castillo Fuerman	Argentina con una nueva línea política, y Perú con sus propios intereses estratégicos. Esa falta de cohesión regional dificulta la posibilidad de establecer una ruta común en materia de autonomía tecnológica y defensa inteligente.
Autonomía estratégica	2. Gral. EP Dr. Ernesto Castillo Fuerman	Personalmente, considero que tenemos el talento humano necesario. He visto el potencial de los ingenieros peruanos: somos capaces de desarrollar nuestros propios algoritmos y software, siempre que se trabaje bajo principios éticos y con una lógica institucional sólida que evite el uso indebido de estas tecnologías. Sin embargo, para que eso ocurra, se requiere una decisión política firme, tanto a nivel nacional como regional
Autonomía estratégica	2. Gral. EP Dr. Ernesto Castillo Fuerman	Lo ideal sería buscar un equilibrio: alianzas estratégicas amigables y de beneficio mutuo, que fortalezcan nuestras capacidades sin comprometer la soberanía.
Agenda hemisférica	3. Gral. EP Hugo Vega Castro	La posibilidad de construir una agenda hemisférica propia en materia de seguridad y desarrollo tecnológico militar existe, pero es limitada si no se acompaña de una verdadera voluntad política colectiva.
Agenda hemisférica	3. Gral. EP Hugo Vega Castro	Sería fundamental también promover la conformación de clústeres tecnológicos y establecer un fondo común regional —por ejemplo, a través del Mercosur u otra instancia hemisférica— destinado a financiar proyectos de investigación en defensa y tecnología avanzada.
Agenda hemisférica	3. Gral. EP Hugo Vega Castro	Es necesario construir una gobernanza común con un marco ético y legal compartido que regule el empleo de la inteligencia artificial, las armas autónomas y el uso militar del ciberespacio.
Agenda hemisférica	3. Gral. EP Hugo Vega Castro	Una de las propuestas concretas sería crear un centro regional de capacitación y especialización técnica en ciberdefensa e inteligencia artificial aplicada a la seguridad.
Agenda hemisférica	3. Gral. EP Hugo Vega Castro	Asimismo, propongo el desarrollo de un centro regional de respuesta ante incidentes cibernéticos (CSIRT) que permita coordinar la defensa digital de los países de la región.

Autonomía estratégica	3. Gral. EP Hugo Vega Castro	Sin esa cooperación regional y sin una visión política compartida de futuro, la región continuará siendo un espacio de competencia entre potencias, más que un actor soberano en el escenario global de la guerra inteligente.
Autonomía estratégica	3. Gral. EP Hugo Vega Castro	el fortalecimiento de la industria militar regional —con una visión de uso dual civil-militar— es clave para reducir la dependencia externa
Autonomía estratégica	3. Gral. EP Hugo Vega Castro	La creación de ecosistemas de investigación, desarrollo e innovación tecnológica (I+D+i) en cada país, y posteriormente a nivel regional, podría convertirse en un motor para alcanzar una soberanía tecnológica compartida.
Respuestas regionales	3. Gral. EP Hugo Vega Castro	Solo mediante una estrategia articulada entre los Estados latinoamericanos, con objetivos comunes y decisiones coordinadas, será posible avanzar hacia una autonomía estratégica real.
Dependencia tecnológica	3. Gral. EP Hugo Vega Castro	Mientras dependamos de tecnologías extranjeras, seguiremos expuestos a vulnerabilidades estructurales y a condicionamientos externos que limitan nuestra capacidad de decisión y respuesta
Dependencia tecnológica	3. Gral. EP Hugo Vega Castro	La dependencia tecnológica implica ceder control sobre infraestructuras críticas y activos estratégicos a potencias o corporaciones extranjeras, lo que puede comprometer seriamente la autonomía estatal y la seguridad nacional.
Rivalidad China-EE. UU.	3. Gral. EP Hugo Vega Castro	China ha incrementado notablemente su presencia en América Latina, no solo desde una perspectiva geopolítica, sino también a través del uso inteligente de su llamado “poder blanco”: la combinación de cultura, cooperación económica y diplomacia blanda. Este enfoque le ha permitido consolidarse como un actor estratégico en la región
Rivalidad China-EE. UU.	3. Gral. EP Hugo Vega Castro	A través de financiamiento y proyectos de desarrollo, China ofrece a los Estados latinoamericanos acceso a tecnología, transferencia de conocimiento y facilidades económicas que contrastan con el enfoque de Estados Unidos, más centrado en la seguridad marítima, la ciberdefensa y el control de las infraestructuras digitales críticas.

Rivalidad China-EE. UU.	3. Gral. EP Hugo Vega Castro	En este contexto, la competencia geoestratégica entre ambas potencias está reconfigurando las políticas de defensa y seguridad de América Latina.
Agenda hemisférica	4. Coronel EP Julio Sebastian Cassareto	Pueden darse reuniones, foros o convenciones donde se discutan estos temas, pero difícilmente se llegará a logros concretos.
Agenda hemisférica	4. Coronel EP Julio Sebastian Cassareto	Si en el futuro algún país de Sudamérica logra una posición económica tan fuerte que le permita asumir un liderazgo regional en materia de defensa y tecnología, quizás podríamos ver algún intento de integración en áreas como la ciberdefensa.
Autonomía estratégica	4. Coronel EP Julio Sebastian Cassareto	la fragmentación política nos impide construir una política de defensa regional sólida frente a la guerra inteligente.
Respuestas regionales	4. Coronel EP Julio Sebastian Cassareto	es muy difícil que América Latina logre unirse frente a este escenario, porque las visiones políticas de los países son muy distintas.
Respuestas regionales	4. Coronel EP Julio Sebastian Cassareto	como Perú y Colombia, las diferencias políticas han impedido articular esfuerzos conjuntos.
Dependencia tecnológica	4. Coronel EP Julio Sebastian Cassareto	dependemos mucho de los proveedores extranjeros, sobre todo en hardware, y también en software
Dependencia tecnológica	4. Coronel EP Julio Sebastian Cassareto	mientras no desarrollemos nuestras propias capacidades tecnológicas, vamos a seguir dependiendo.
Rivalidad China-EE. UU.	4. Coronel EP Julio Sebastian Cassareto	es evidente que existe una competencia muy marcada entre China y Estados Unidos

Rivalidad China-EE. UU.	4. Coronel EP Julio Sebastian Cassareto	esa competencia ha llegado también a América Latina. La vemos, sobre todo, en el ámbito comercial y en la lucha por la influencia política en distintos países de la región.
Rivalidad China-EE. UU.	4. Coronel EP Julio Sebastian Cassareto	Hay países que se alinean más con China, como lo ha sido Bolivia en su momento o Colombia actualmente, y otros, como Argentina, que están más cerca de Estados Unidos.

Tabla 6

Soporte de la categoría 1: Impacto de la guerra inteligente (análisis documental)

Subcategorías	Documentos	Unidades de significado
Arquitectura de seguridad	3. Artificial Intelligence and Information Integrity	Such developments may affect the accuracy, diversity and public interest of the information ecosystem in online spaces, which is especially important during elections
Arquitectura de seguridad	3. Artificial Intelligence and Information Integrity	Elections cannot fulfil their role without a shared reality based on facts
Arquitectura de seguridad	4.América Latina en el nuevo escenario internacional	no solo para promover la integración comercial, sino también para establecer un esquema regional amplio que incluyera cooperación política en seguridad, infraestructura, engería y en distintas agendas sociales, como por ejemplo en salud. Liderada por Brasil, UNASUR fue resultado de un proceso complejo que incluyó negociaciones con otros países de la región, como Argentina y Venezuela
Arquitectura de seguridad	4.América Latina en el nuevo escenario internacional	En América Latina, hoy, desde una perspectiva regional, el entorno institucional exhibe fragmentación, fragilidad y estancamiento, producto de una compleja arquitectura, la superposición de membresías y agendas
Arquitectura de seguridad	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	AI may thus help mitigate offensive actions. It may also help to more effectively attribute cyber-attacks to specific actors by enhancing information and digital evidence collection and by providing probabilistic models to assess contradictory and uncertain data.

Arquitectura de seguridad	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	Enhancing cyber security is becoming increasingly challenging due to the growing number of internet-connected devices and the exponentially increasing volume of data produced that needs securing.
Arquitectura de seguridad	6. AI y políticas públicas en América Latina y el Caribe	While AI en- ables faster and more accurate detection and mitigation of cyber-attacks, it also amplifies the associated risks, such as cy- ber-espionage, information manipulation and the development of advanced surveillance tools.
Arquitectura de seguridad	6. AI y políticas públicas en América Latina y el Caribe	Some of the measures suggested include the creation of regu- latory frameworks that guarantee a responsible use of AI, such as those promoted by the European Union, as well as the devel- opment of specific cybersecurity technologies and skills.
Arquitectura de seguridad	7.Latin American hemispheric security adapted	De esta forma comenzó a cimentarse una arquitectura flexible de Seguridad, con miras al futuro tecnológico y contextualizado en la globalización contemporánea.
Arquitectura de seguridad	7.Latin American hemispheric security adapted	Bajo la triada TIAR–OEA-EE. UU se fue cimentando una noción de Seguridad mucho más amplia y compleja para la región.
Arquitectura de seguridad	9.Artificial intelligence governance challenges	la gobernanza de la inteligencia artificial surge como un profundo proceso de difusión internacional centrado en la gobernanza de datos, la definición de una perspectiva ética y la construcción de marcos regulatorios
Arquitectura de seguridad	9.Artificial intelligence governance challenges	El primer nivel se refiere a una constitución técnica capaz de abordar datos y algoritmos donde se encuentran los procesos de gobernanza de datos

Arquitectura de seguridad	13.Updating cognitive security in a global dimension	The information space of the Earth is a global information system for aerospace monitoring of the Earth (exploration of natural resources, control of man-made accidents and natural disasters, navigation and communication), the primary basis of which was the creation of the global space information and control system of the Russian Aerospace Defence (VKO
Arquitectura de seguridad	13.Updating cognitive security in a global dimension	Countries (members of NATO – I. K., R. V., O. P.) should consider protection from CogWar as an imperative of national and global security
Arquitectura de seguridad	15.Russia´s cooperation with the Latin American	la colaboración entre Rusia y Nicaragua en la esfera de la seguridad que incluye programas de formación y entrenamiento para militares nicaragüenses, así como el funcionamiento del centro para la lucha contra el narcotráfico, construido por Rusia
Arquitectura de seguridad	15.Russia´s cooperation with the Latin American	los acuerdos de Rusia con Brasil y Nicaragua para crear bases e instalaciones destinadas a garantizar el funcionamiento del sistema satelital de navegación global (GLONASS)
Arquitectura de seguridad	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Pueden las armas autónomas diferenciar civiles de combatientes? ¿Pueden respetar los principios del derecho internacional humanitario?
Arquitectura de seguridad	26 Artificial intellrms control in modern warfare (1)	The relevance of AI to security studies has taken multiple dimensions ranging from the dissemination of fake news to surveillance technology and missile defence systems.

Arquitectura de seguridad	26 Artificial intellrms control in modern warfare (1)	AI is the cornerstone of the Chinese national security strategy also and has been employed in terms of quantum technology, which ensures optimal situational awareness through the use of sensors in the battlespace
Arquitectura de seguridad	Investigación sobre las Áreas Clave de Aplicación Militar	En las futuras guerras inteligentes, se desplegarán muchas armas de IA en el campo de batalla, por lo que capturar y proteger los canales de transmisión de información se vuelve crucial
Arquitectura de seguridad	34 Geopolitical Marxism and the Promise of Radical Historicism	the articulation not only of the essential long-term security interests and strategic war objectives of a polity, but combines the concern with how to win major wars with an emphasis on how to win the peace, implying that war-planning is intricately tied to ulterior considerations of a post-war settlement that provides international stability
Arquitectura de seguridad	34 Geopolitical Marxism and the Promise of Radical Historicism	defensive and concerned with security interests versus the continent to prevent the rise of any continental hegemonic state, prosecuted through power-balancing,
Arquitectura de seguridad	35. The Influence of Strategic Culture Components on Bilateral and Regional Relations between Iran and Russia	Strategic ambiguity, deterrence and pragmatism are the basis of Iran's actions in the framework of strategic culture.

Arquitectura de seguridad	35. The Influence of Strategic Culture Components on Bilateral and Regional Relations between Iran and Russia	Geopolitics, pragmatism, historical experiences and Journal of Central Eurasia Studies, Faculty of Law and Political Science, Vol. 15, No. 1, Spring & Summer 2022 389 deterrence against the West are common components of the strategic culture of Iran and Russia
Arquitectura de seguridad	35. The Influence of Strategic Culture Components on Bilateral and Regional Relations between Iran and Russia	Russia's priority is relations with countries that take advantage of their geopolitical position and political and military capacity to interact with the West.
Arquitectura de seguridad	11.Geopolitics in the digital age	Policymakers emphasize the dual nature of AI, presenting transformative opportunities in addressing global challenges alongside significant risks to national security, economic stability, and societal well-being.
Arquitectura de seguridad	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Los sistemas de armas autónomas letales (LAWS) representan un desafío significativo para la seguridad internacional y la humanidad
Arquitectura de seguridad	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	el control de armamentos sobre los LAWS enfrenta múltiples obstáculos, entre ellos: la ambigüedad conceptual, los impedimentos políticos, la atracción militar y las dificultades en materia de rendición de cuentas

Arquitectura de seguridad	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	El sistema de guerra electrónica de inteligencia artificial "Berliana" que pronto equipará el ejército ruso puede analizar la situación en tiempo real, descubrir y clasificar objetivos sin la participación del operador, y puede seleccionar de forma autónoma qué medios de guerra electrónica utilizar, qué mecanismo utilizar y con qué frecuencia y potencia contrarrestar objetivos específicos. En la actualidad, el sistema ha pasado las pruebas integrales y participó en el ejercicio "Oeste-2017".
Arquitectura de seguridad	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	El sistema de confrontación electrónica distribuida basado en el "barco no tripulado de confrontación electrónica" puede convertirse en una forma eficaz de responder a la "matanza distribuida".
Arquitectura de seguridad	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	Se utiliza plenamente la fuerte capacidad de fusión de datos, extracción de información y aprendizaje de características de tecnologías de IA como el aprendizaje profundo y las redes neuronales para lograr una organización y almacenamiento eficientes de datos multimodales heterogéneos.
Arquitectura de seguridad	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	El sistema de asalto inteligente terrestre adopta el nuevo concepto de "agrupación modular, despliegue discreto, aplicación integrada"
Arquitectura de seguridad	20.What do Latin Americans think about the world system	En opinión de los latinoamericanos Estados Unidos ostenta el liderazgo mundial en los temas militares y de seguridad

Autonomía tecnológica	3. Artificial Intelligence and Information Integrity	Algorithmic biases intensify existing forms of exclusion, particularly when AI systems are trained on data sets that do not adequately represent Indigenous communities.
Autonomía tecnológica	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	The Israeli Harpy drone – a loitering munition also known as a 'fire and forget' system – is, judging by its technical specifications alone, a fully-autonomous weapon system.
Autonomía tecnológica	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	We already have AI platforms – such as in the area of missile defense, the Israeli Harpy drone, and automated Russian tanks – that are fully capable of being autonomous, but they have not yet been fully deployed or relied upon.
Autonomía tecnológica	6. AI y políticas públicas en América Latina y el Caribe	EBIA also seeks to empower and educate professionals for the AI ecosystem, stimulate innovation inter- nationally, and foster cooperation between public and private entities, industry and research centers.
Autonomía tecnológica	6. AI y políticas públicas en América Latina y el Caribe	The Chilean policy focuses on empowering citizens in the development and use of AI, promoting participation in debates about its legal, ethical, social and economic implications, and developing enabling factors, such as talent, technological infra structure and data.
Autonomía tecnológica	7.Latin American hemispheric security adapted	la vigilancia estatal sobre las actividades y plataformas públicas y privadas que utilizan el ciberespacio condiciona su efectividad
Autonomía tecnológica	9.Artificial intelligence governance challenges	La posición de América Latina en el concierto global de infraestructura de datos no es significativa y requiere grandes inversiones públicas para construir infraestructura crítica.

Autonomía tecnológica	13.Updating cognitive security in a global dimension	the uncontrolled, in many ways, development of artificial intelligence will pose a serious threa
Autonomía tecnológica	13.Updating cognitive security in a global dimension	Cognitive warfare, which blurs the line between peace and war, includes NBICS technologies for use in specific operations to provide ‘a reliable way of military superiority in the near future
Autonomía tecnológica	15.Russia´s cooperation with the Latin American	los armamentos rusos son de alto rendimiento, seguros y fáciles de manejar, lo cual fue demostrado por su empleo eficaz en conflictos locales, ante todo en Siria
Autonomía tecnológica	21 Sistemas de armas autónomas y DIH	la palabra “autónomo”, la cual hace referencia a un sistema, ya sea de hardware o software capaz de ejecutar una tarea sin intervención humana (Boulanin, 2017, p. 6)
Autonomía tecnológica	21 Sistemas de armas autónomas y DIH	la autonomía de la que hablaremos se entiende como la capacidad de “transformar información del entorno en un plan/acción con propósito” (Boulanin, 2017, p. 7).
Autonomía tecnológica	21 Sistemas de armas autónomas y DIH	un arma que sin intervención humana puede seleccionar (buscar o detectar, identificar y rastrear) y atacar (interceptar, aplicar fuerza, neutralizar, dañar o destruir) objetivos (CICR, 2015).
Autonomía tecnológica	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	La creciente dependencia tecnológica también implica una relación de dominación encubierta de la tecnología sobre los seres humanos
Autonomía tecnológica	26 Artificial intellrms control in modern warfare (1)	Autonomous systems and automated weapons serve different functions, while autonomous weapons are AI-powered weapons designed to work independently and perform tasks without human intervention

Autonomía tecnológica	26 Artificial intellrms control in modern warfare (1)	The future of AI in the military is directly connected to our ability to design autonomous systems.
Autonomía tecnológica	Investigación sobre las Áreas Clave de Aplicación Militar	Con la ayuda de la tecnología de IA, es posible operar mediante equipos no tripulados en cooperación con humanos, o incluso que las máquinas operen de forma completamente autónoma, mejorando la eficiencia y seguridad operativa, como con robots para tuberías, robots de desminado, etc.
Autonomía tecnológica	11.Geopolitics in the digital age	The “world of injustices” narrative emphasizes reducing global technological divides by supporting AI infrastructure in the Global South.
Autonomía tecnológica	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Impulso a la cooperación tecnológica internacional. Participar en proyectos de estándares internacionales en IA y robótica
Autonomía tecnológica	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	personal de la instalación nuclear, si tiene permisos para operar y si está siendo escaneado y detectado por el personal de operación de la computadora, etc., y realizará de forma autónoma acciones de infección, elevación de permisos o evitación,

Autonomía tecnológica	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	la operación inteligente en el campo de la red eléctrica debe innovar la guía de la operación de confrontación de la red eléctrica, confiar en equipos de confrontación de la red eléctrica más autónomos e inteligentes, centrarse en la tecnología inteligente autónoma, la colaboración hombre-máquina y la tecnología de colaboración de grupos para superar las dificultades, mejorar gradualmente el nivel de inteligencia del equipo de confrontación de la red eléctrica y, a través del uso de una arquitectura de sistema abierto, realizar el intercambio de datos, la creación de redes multi máquina, la cooperación coordinada y la conexión perfecta, y finalmente formar un sistema de operación de red eléctrica distribuida, mejorar la capacidad integral de operación de red eléctrica en la era inteligente.
Autonomía tecnológica	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	La tecnología de IA logra la clasificación inteligente de los datos de video masivos del campo de batalla recopilados por enjambres de drones, mejorando enormemente la capacidad de procesamiento y análisis de inteligencia en entornos de batalla complejos
Autonomía tecnológica	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	En este enlace, el sistema no tripulado ejecuta las reglas de comportamiento de "condición-acción", el enlace es más corto, puede lograr el efecto de descubrir y destruir,
Autonomía tecnológica	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	AUGV puede cambiar entre dos estados de colaboración controlada y colaboración autónoma durante el proceso de ataque.

Cooperación regional	4.América Latina en el nuevo escenario internacional	el regionalismo y la cooperación regional en América Latina han estado históricamente ligados al modelo de desarrollo y de inserción internacional
Cooperación regional	4.América Latina en el nuevo escenario internacional	Una vez más, se destaca la región, en este caso, América del Sur, como una «región de paz y cooperación», y se reconoce la importancia del diálogo para promover la integración en América del Sur en la medida en que «la integración regional debe ser parte de las soluciones para afrontar los desafíos compartidos
Cooperación regional	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	There are a number of states developing AI-enabled capabilities that have expressed an interest in maintaining interoperability with allies and partners,
Cooperación regional	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	Developing and deploying AI that is compatible across different branches of the armed forces will be challenging.
Cooperación regional	6. AI y políticas públicas en América Latina y el Caribe	Several regional initiatives seek to foster the exchange of knowledge and best practices, while addressing shared challenges through collaborative efforts. One of the most prominent is fAIr LAC, a project promoted by the Inter-American Development Bank (IDB)
Cooperación regional	6. AI y políticas públicas en América Latina y el Caribe	This collaboration resulted in a standardized public policy for the procurement of AI-based systems by the public sector.

Cooperación regional	6. AI y políticas públicas en América Latina y el Caribe	Thanks to this effort, Chile has become the first country in Latin America to have ethical requirements for the procurement of automated systems (Access Now, 2024).
Cooperación regional	7.Latin American hemispheric security adapted	La OEA ha implementado un número importante de medidas para mejorar la Ciberseguridad en todo el hemisferio.
Cooperación regional	7.Latin American hemispheric security adapted	La cooperación internacional en materia de Ciberseguridad es esencial. Esto hace que las gestiones regionales sean aún más eficaces
Cooperación regional	9.Artificial intelligence governance challenges	las estrategias nacionales de IA en América Latina, excepto Colombia y República Dominicana, no describen ninguna forma de cooperación regional entre los países.
Cooperación regional	15.Russia´s cooperation with the Latin American	la cooperación de Rusia con los países de América Latina y el Caribe pone en riesgo los intereses de Washington en la región
Cooperación regional	26 Artificial intellrms control in modern warfare (1)	Germany and France announced plans to develop the Future Combat Air System (FCAS), a nuclear-capable combat aircraft expected to enter service around 2040, as part of its Next-Generation Weapon Systems plan.
Cooperación regional	27 AI Governance in Latin America	The first regional statement on AI did not come from governments but rather from the tech and academic community. The KHIPU initiative – which mirrored the Af- rican e
Cooperación regional	27 AI Governance in Latin America	In a context of intense global geopo- litical competition, regional coordination might be the best way for Latin America to carve out a role in the AI landscape

Cooperación regional	11.Geopolitics in the digital age	China uses the frames of sovereignty and autonomy as narrative tools to advocate for strengthening international alliances with developing countries.
Cooperación regional	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Promoción de la transparencia y la confianza regional. A través de mecanismos en Asia-Pacífico
Cooperación regional	20.What do Latin Americans think about the world system	Costa Rica, Chile, Uruguay e incluso México tienen buenas o muy buenas relaciones con los tres polos (Estados Unidos, China y la Unión Europea)
Gobernanza tecno-militar	3. Artificial Intelligence and Information Integrity	National AI strategies must explicitly recognize and address deepfakes and other forms of technology-facilitated abuse
Gobernanza tecno-militar	4.América Latina en el nuevo escenario internacional	Asimismo, América Latina es la única región del mundo libre de armas nucleares, desde la firma del Tratado para la Proscripción de las Armas Nucleares en América Latina
Gobernanza tecno-militar	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	Developing common operational standards, requirements and ethical guidelines for AI-enabled capabilities through NATO's Defence Planning Process (NDPP) and Science and Technology Organization (STO), or through the EU's European Defence Fund (EDF), Coordinated Annual Review on Defense (CARD) and Permanent Structured Cooperation (PESCO), will be both necessary and challenging.
Gobernanza tecno-militar	6. AI y políticas públicas en América Latina y el Caribe	It is the obligation of nation states to establish precise regulations regarding the advancement and implementation of autonomous weapons systems to ensure compliance with international legal standards and fundamental human rights principles.

Gobernanza tecno-militar	7.Latin American hemispheric security adapted	La creación de plataformas nacionales multisectoriales sostenibles Es importante tener en cuenta los diferentes aspectos y consecuencias, así como la viabilidad técnica de la promulgación de nuevas regulaciones. Grupos de la sociedad civil, la academia y la comunidad técnica, así como representantes de la industria pueden proporcionar valiosa experiencia
Gobernanza tecno-militar	7.Latin American hemispheric security adapted	la OEA se transformó en el primer organismo regional en adoptar una estrategia en esa materia.
Gobernanza tecno-militar	9.Artificial intelligence governance challenges	La regulación de las tecnologías disruptivas surge en contextos de asimetrías de información, incertidumbres políticas, dinámicas de poder estructural y errores en el diseño de políticas
Gobernanza tecno-militar	9.Artificial intelligence governance challenges	Los gobiernos latinoamericanos defienden el desarrollo técnico y ético sin claridad respecto del nivel regulatorio
Gobernanza tecno-militar	15.Russia´s cooperation with the Latin American	los centros de instrucción y mantenimiento técnico para helicópteros de fabricación rusa que funcionan en México [7], Perú [14, p. 63] y Venezuela
Gobernanza tecno-militar	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Las políticas públicas deben establecer mecanismos coherentes de gobernanza. Propuestas académicas incluyen: Sistemas de decisión tipo “depósito regulatorio”, que mantengan la tecnología bajo la intención human

Gobernanza tecno-militar	26 Artificial intellrms control in modern warfare (1)	The United Nations First Committee, committed to Disarmament and International Security, met in December 2023 to discuss the potential for a comprehensive study of LAWS due to the large grey areassurrounding its ethical, legal and humanitarian consequences
Gobernanza tecno-militar	Investigación sobre las Áreas Clave de Aplicación Militar	Sin embargo, a corto plazo, la tecnología de IA aún no puede reemplazar a los humanos en la toma de decisiones de mando y control, solo puede desempeñar un papel de apoyo. El ejército estadounidense también es cauteloso respecto a la inteligencia del mando y control
Gobernanza tecno-militar	34 Geopolitical Marxism and the Promise of Radical Historicism	developments in military technology collapsed back into geopolitical competition, invoking Realism, without providing a social-relational theory of the early modern permanent war-state. The “military revolution”, the rise of the “permanent war-state”, and the bellicosity of the early modern period are contracted out to Realism or Tilly’s geopolitical-competition-model (T
Gobernanza tecno-militar	35. The Influence of Strategic Culture Components on Bilateral and Regional Relations between Iran and Russia	Russia's strategic culture is aggressive in nature. The threat of the West has provided the basis for the rapprochement of the positions of Iran and Russia,
Gobernanza tecno-militar	11.Geopolitics in the digital age	AI and cyberspace governance should occur within the UN framework, should adhere to multilateralism, and must respect the sovereignty of all nations

Gobernanza tecno-militar	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	La gobernanza global de la inteligencia artificial se ha convertido progresivamente en un tema central, particularmente en relación con los sistemas de armas autónomas letales (LAWS) y su control
Gobernanza tecno-militar	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Promover la transferencia tecnológica responsable y la cooperación en IA para usos civiles y humanitarios
Gobernanza tecno-militar	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	Para abordar los riesgos, se necesita un enfoque diferenciado según la urgencia y gravedad. Se propone una gobernanza basada en clasificación de riesgos, con cooperación global.
Gobernanza tecno-militar	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	Sistemas semi-autónomos: Imponer restricciones en predictibilidad, tipos de objetivo, duración, ámbito geográfico y supervisión humana.
Gobernanza tecno-militar	19.Problemas de Derecho Internacional derivados	Actualmente, las discusiones sobre la gobernanza de la IA bajo el derecho internacional se centran en la regulación de las armas de IA. Por ejemplo, la aplicación de tecnología de reconocimiento facial y drones por ambas partes en el conflicto ruso-ucraniano. La legalidad y la atribución de responsabilidad en el derecho internacional de aplicaciones de IA representadas por "armas autónomas letales" como los "aviones no tripulados" han sido objeto de discusión correspondiente, siendo los desafíos para el derecho internacional humanitario los más prominentes

Gobernanza tecno-militar	19.Problemas de Derecho Internacional derivados	Impulsado por organizaciones no gubernamentales, el foro de la Convención sobre Ciertas Armas Convencionales ha estado discutiendo la prohibición de los sistemas de armas autónomas en Ginebra desde 2013. Los Estados participantes parecen estar de acuerdo en que el uso de la fuerza física, incluido el uso de fuerza letal, en conflictos armados, debe estar siempre bajo un "control humano significativo", y que los sistemas de armas completamente autónomos deberían ser prohibidos por nuevos documentos legales internacionales.
Gobernanza tecno-militar	38 Investigación sobre la tecnología de inteligencia artificial	Su valor real ha superado la comprensión inicial de los investigadores técnicos, y su esencia es la tecnología de procesamiento y producción de información y datos. Esta producción y procesamiento no solo puede proporcionar a las personas una vida más conveniente, sino que también tendrá un impacto fundamental en la forma en que las personas producen y viven en el futuro, y tendrá un impacto de gran alcance en el modo de funcionamiento de la vida económica nacional futura y la estructura organizativa de la sociedad futura.
Gobernanza tecno-militar	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	En los últimos años, con el apoyo de los últimos logros tecnológicos de la información y la inteligencia, el ejército estadounidense ha desarrollado gradualmente el concepto de "operaciones de dominio completo", cuyo objetivo principal es expandirse a dominios como el espacio, el espacio de redes eléctricas, etc.

Gobernanza tecno-militar	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	Entre ellos, el batallón de operaciones multidominio está compuesto por inteligencia, información, redes, guerra electrónica y fuerzas espaciales, y tiene capacidades de análisis y fusión de inteligencia, guerra de opinión pública de información, operaciones de redes eléctricas, coordinación de apoyo espacial, etc.,
Gobernanza tecno-militar	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	Todos los países están acelerando el proceso de despliegue y aplicación de la tecnología de IA en defensa, ámbitos militares y otros campos, esforzándose por ocupar el "punto culminante" de la confrontación de información en futuros sistemas operativos nuevos,
Gobernanza tecno-militar	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	El desarrollo del sistema de concepto de combate involucra muchos elementos como el combate, el mando, el equipo y la tecnología, y pertenece a la categoría de sistemas complejos
Gobernanza tecno-militar	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	DoDAF, como una especificación de arquitectura típica y madura en el mundo, ha sido ampliamente utilizado en el desarrollo de sistemas de conceptos de combate [7-8].
Riesgos emergentes	3. Artificial Intelligence and Information Integrity	Among many imagined risks associated with AI, the possibility of generating content that is impossible to verify stands out as the most alarming.
Riesgos emergentes	3. Artificial Intelligence and Information Integrity	AI technologies have exacerbated the vulnerabilities of Indigenous communities.

Riesgos emergentes	3. Artificial Intelligence and Information Integrity	Automated content generation tools, large-scale bot networks and sophisticated algorithmic targeting can greatly increase the spread, personalization and persistence of disinformation and hate speech
Riesgos emergentes	3. Artificial Intelligence and Information Integrity	These fake personas can be used to help spread narratives and shape alternative realities, as they can better mimic local dialects and language usage or even fake accents. They can also overwhelm fact-checking organizations and make their work much more difficult
Riesgos emergentes	4.América Latina en el nuevo escenario internacional	la COVID-19 de 2020 y la guerra en Ucrania, iniciada en febrero de 2022, han profundizado y amplificado los efectos de estas varias crisis, generando una creciente inestabilidad e incertidumbre.
Riesgos emergentes	4.América Latina en el nuevo escenario internacional	la crisis permanente en Venezuela ha sido el epicentro de la crisis del regionalismo en América Latina
Riesgos emergentes	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	The risks associated with the weaponization of AI have not been outlined systematically27 but include the development of bias within AI systems.
Riesgos emergentes	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	Another significant risk with AI systems is that they can be manipulated, and their integrity altered by malicious actors and evenprogrammed to perform unintended functions.

Riesgos emergentes	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	A related concern is that AI could be used to enhance information operations and target populations with the intent of causing instability or division.
Riesgos emergentes	6. AI y políticas públicas en América Latina y el Caribe	since these systems can copy, perpetuate and amplify discrimination schemes referring to sexual, ethnic, linguistic and religious diversity, just to name some of the most outstanding ones
Riesgos emergentes	7.Latin American hemispheric security adapted	Los riesgos y amenazas son numerosos y dinámicos. Entre ellos destacan, una mayor y más compleja actividad delictual que se desarrolla transnacionalmente
Riesgos emergentes	9.Artificial intelligence governance challenges	(La IA) refuerza los sesgos algorítmicos de una manera que perjudica a las mujeres y personas negras
Riesgos emergentes	9.Artificial intelligence governance challenges	la IA excluye a los más pobres creando áreas de pobreza social y nuevos patrones de jerarquías que profundizan las desigualdades
Riesgos emergentes	13.Updating cognitive security in a global dimension	Cognitive warfare poses global risks of a purely technological and geopolitical, economic, socio-anthropological and existential order.
Riesgos emergentes	13.Updating cognitive security in a global dimension	CogWar poses a threat to national and global stability and security at the economic, geopolitical, social and cultural levels, as it targets the vulnerability of people as a means of creating chaos and confusion in the mass consciousness

Riesgos emergentes	15.Russia´s cooperation with the Latin American	los países de ALC que se empeñan en aplicar políticas independientes ahora se ven en aprietos. Se hallan sometidos a las sanciones económicas y presión política por parte de Washington
Riesgos emergentes	21 Sistemas de armas autónomas y DIH	La falta de un sistema normativo preciso como consecuencia de su novedad, tanto en el ámbito internacional como en el nacional, significa que existe un vacío normativo en la aplicación de dicha tecnología a la realidad y, por ende, una oportunidad para abusar de ella ya sea de parte del Estado o de cualquier grupo que participe activamente en las hostilidades
Riesgos emergentes	21 Sistemas de armas autónomas y DIH	La incapacidad de explicar las decisiones que se toman y, por lo tanto, convertirlas en predecibles, es una característica que bloquea la aplicación de esta tecnología en la vida rea
Riesgos emergentes	21 Sistemas de armas autónomas y DIH	la dimensión de imprevisibilidad eleva el nivel de preocupación sobre la falta de explicabilidad en su toma de decisiones y el posible sesgo al que han sido sometidas durante su programación (CICR, 2021, p. 466).
Riesgos emergentes	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Frente a máquinas inteligentes, el ser humano parece torpe, rígido y se convierte gradualmente en un “componente” subordinado a sistemas inteligentes.
Riesgos emergentes	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	La IA intensifica el riesgo de vulneración de la privacidad debido al almacenamiento masivo de datos personales, el rastreo algorítmico y el procesamiento inteligente

Riesgos emergentes	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	El sesgo algorítmico altera la imparcialidad y la justicia, y plantea preguntas sobre la responsabilidad en los sistemas automatizados:
Riesgos emergentes	26 Artificial intellrms control in modern warfare (1)	While remote control allows for human oversight, AI systems can exhibit unpredictable behaviours or errors that are not fully understood. This unpredictability necessitates additional regulatory measures
Riesgos emergentes	26 Artificial intellrms control in modern warfare (1)	the manipulative power of AI, when mixed with cybersecurity and digital space, can be used to achieve numerous far-fetched objectives in warfare and upset existing peace efforts in volatile environments.
Riesgos emergentes	Investigación sobre las Áreas Clave de Aplicación Militar	La guerra electrónica cognitiva con percepción situacional autónoma toma de decisiones y protección electrónica adaptativa, junto con la tecnología de guerra cibernética, han entrado gradualmente en el escenario de la confrontación.
Riesgos emergentes	34 Geopolitical Marxism and the Promise of Radical Historicism	The effect of more advanced polities on more backward regions could invite “catch-up”, but the result could equally be multiple instances of de-development, non-development, and under-development
Riesgos emergentes	11.Geopolitics in the digital age	The “open world” narrative positions digital technologies, particularly AI, as vital tools for fostering international collaboration to address urgent global challenges such as climate change, global health crises, poverty, inequality, and human rights violations.

Riesgos emergentes	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Sin regulación, esto podría desencadenar una carrera armamentista de armas autónomas, socavando la paz y la estabilidad mundial.
Riesgos emergentes	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Dado el riesgo que suponen los sistemas “human out of the loop”
Riesgos emergentes	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	La proliferación de armas autónomas es una amenaza no tradicional urgente. Especialmente, el riesgo de que estas armas caigan en manos de grupos terroristas está aumentando.
Riesgos emergentes	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	A medio plazo, la IA probablemente afectará negativamente la estabilidad estratégica, con riesgo de guerra nuclear
Riesgos emergentes	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	Además, el uso de la IA en ciberataques, por su velocidad, sigilo, bajo costo y dificultad de rastreo, puede provocar "guerras relámpago" cibernéticas, donde algoritmos automáticos interactúen en tiempo real, escalando conflictos.
Riesgos emergentes	19.Problemas de Derecho Internacional derivados	El rápido desarrollo de la tecnología de Inteligencia Artificial (IA), si bien impulsa la transformación social, también plantea nuevos desafíos al sistema jurídico internacional existente. Además del derecho internacional de la propiedad intelectual, tiene un impacto significativo en principios como la responsabilidad del Estado, la soberanía nacional, el derecho internacional humanitario y el derecho internacional de los derechos humanos

Riesgos emergentes	19.Problemas de Derecho Internacional derivados	La tecnología de IA puede convertirse en un impulso para el bien del desarrollo social, pero si no se considera plenamente su impacto en los derechos humanos durante su uso, también podría producir malas e incluso terribles consecuencias.
Riesgos emergentes	19.Problemas de Derecho Internacional derivados	En la era de la información, el flujo transfronterizo de grandes volúmenes de datos se ha convertido en la norma. Y con la amplia aplicación de las tecnologías de big data e IA, los datos requeridos para el aprendizaje automático y profundo son aún más asombrosos, por lo que la seguridad de los datos se vuelve más urgente.
Riesgos emergentes	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	, la confrontación cognitiva, de información y de energía se entrelazan, se reúnen rápidamente en torno al objetivo bajo el liderazgo de la inteligencia artificial, el tiempo se comprime cada vez más, la velocidad de confrontación es cada vez más rápida, la inversión de la opinión pública, la agitación social, la pérdida de control psicológico y el efecto de encadenamiento del Internet de las cosas, etc., se convertirán en características importantes de la confrontación de la red en la era inteligente [
Riesgos emergentes	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	Los datos de inteligencia militar modernos tienen características como ser masivos, heterogéneos y multidimensionales, lo que complica aún más el proceso de tratamiento de datos de inteligencia
Riesgos emergentes	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	una gran cantidad de información valiosa oculta detrás de los datos de inteligencia no pueda ser descubierta a tiempo, y no se puedan realizar predicciones precisas y en tiempo real de la situación del campo de batalla,

Riesgos emergentes	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	el sistema se enfrentará a una alta intensidad de confrontación y amenazas diversificadas en el combate.
Riesgos emergentes	20.What do Latin Americans think about the world system	el fin de la hegemonía americana en el mundo en general y en Latinoamérica en particular no es homogéneamente percibido por los habitantes de la región.
Transformación doctrinaria	3. Artificial Intelligence and Information Integrity	These actors have weaponized societal divisions, exploiting the new channels and affordances created by digital platforms. They have flooded the digital public sphere with information and narratives, often using inauthentic or illicit techniques, to advance their interests, eroding trust in the electoral process along the way.
Transformación doctrinaria	3. Artificial Intelligence and Information Integrity	This manipulation is creating bespoke realities for certain groups of citizens that are based not on facts or a peaceful exchange of ideas but on manipulated information and narratives that benefit certain political camps.
Transformación doctrinaria	4.América Latina en el nuevo escenario internacional	De esta forma, tanto el entorno institucional como esta idea sobre la región funcionaron como un recurso para los intereses de los actores estatales. En con- junto, esta configuración material, ideacional e institucional tuvo importantes implicaciones a nivel regional.
Transformación doctrinaria	4.América Latina en el nuevo escenario internacional	Ello se tradujo en transformaciones en los proyectos regionales, como en el caso del relanzamiento del Mercosur, así como la transformación de la CSN en la Unión de Naciones Suramericanas (UNASUR)

Transformación doctrinaria	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	Alternatively, the application of AI in the military field, either independently or in conjunction with other emerging technologies such as quantum computing, big data analytics, advanced robotics, human enhancement technologies, and automation, will lead to the development of new doctrines that defy the existing physical and legal boundaries of today's battlefield
Transformación doctrinaria	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	The application of AI into combined armed operations will likely depend more on the national models of inclusion of AI into the military field and the usefulness of this emerging technology, rather than a general set of technical specifications.
Transformación doctrinaria	6. AI y políticas públicas en América Latina y el Caribe	The incorporation of AI into the military domain could cause concerns about technological competition in weaponry. Nations may find it tempting to develop and deploy new tools quickly so as not to fall behind, possibly increasing conflict and disrupting security regionally or even globally.
Transformación doctrinaria	7.Latin American hemispheric security adapted	Desde la conformación de la Conferencia Especial de Seguridad de México de 2003, los Estados Miembros de la OEA acordaron ampliar el concepto de seguridad, adoptando un enfoque multidimensional
Transformación doctrinaria	7.Latin American hemispheric security adapted	El proceso de transformación de un concepto de Seguridad unidimensional a uno multidimensional obedece a esta transformación y tiene una evolución histórica que es importante considerar.
Transformación doctrinaria	9.Artificial intelligence governance challenges	La IA cambia los fundamentos epistémicos de la sociedad a medida que avanza su desarrollo porque trabaja con información amplia y produce predicción, simulación y definición de horizontes para la acción humana

Transformación doctrinaria	9.Artificial intelligence governance challenges	Los algoritmos representan un “libro de reglas” que define cómo los sistemas algorítmicos calculan los cursos de acción social
Transformación doctrinaria	13.Updating cognitive security in a global dimension	In the early 20s of the twenty-first centuries, the issue of the formation of another area (do- main) of military operations – cognitive warfare (a more accurate translation is cognitive operation, Cognitive Warfare) – began to be widely discussed in the NATO military ana- lytic community.
Transformación doctrinaria	13.Updating cognitive security in a global dimension	According to the concept of ‘cognitive warfare,’ another dimension of combat appears on the modern battlefield – the cognitive dimension, which complements the physical (land, sea, air, space) and information dimensions.
Transformación doctrinaria	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Con la tendencia hacia la “guerra ultrarrápida”, los humanos podrían quedar excluidos del ciclo OODA (observar, orientar, decidir, actuar).
Transformación doctrinaria	26 Artificial intellrms control in modern warfare (1)	Throughout history, warfare has undergone significant changes due to revolutionary discoveries and innovative use of technologies. These advancements and revelations have led to significant transformations in military principles, operational strategies, and organisational structures, ultimately altering nature and implementation of military endeavours (Panwar, 2017).
Transformación doctrinaria	26 Artificial intellrms control in modern warfare (1)	The emergence of artificial intelligence is ushering in a cognitive transformation, posing the task of predicting the overarching implications of how this cognitive revolution could reshape the landscape of warfare (Kozyulin, 2019).

Transformación doctrinaria	Investigación sobre las Áreas Clave de Aplicación Militar	La aplicación de tecnología de IA en el mando y control puede comprimir el tiempo de los comandantes en el ciclo, aumentar exponencialmente la velocidad de decisión y lograr el objetivo de mando y control de operaciones conjuntas multidisciplinarias para ganar las guerras futuras.
Transformación doctrinaria	34 Geopolitical Marxism and the Promise of Radical Historicism	We argue that only this final step will ultimately wrest the sphere of international politics from the disciplinary stranglehold of the Realist tradition in IR and in Neo-Weberian Historical Sociology.
Transformación doctrinaria	35. The Influence of Strategic Culture Components on Bilateral and Regional Relations between Iran and Russia	Strategic culture has emerged as an alternative perspective in international relations due to the inability of realism and neorealism theories to explain the behavior of governments during the Cold War.
Transformación doctrinaria	35. The Influence of Strategic Culture Components on Bilateral and Regional Relations between Iran and Russia	The perspective of strategic culture believes that internal factors such as geopolitical situation, historical experiences, political culture and ideology determine the performance of a government and response to challenges.
Transformación doctrinaria	11.Geopolitics in the digital age	The “closed world” narrative emphasizes technological autonomy and sovereignty to enhance national interests and security.

Transformación doctrinaria	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	La militarización de dichas tecnologías ha generado preocupaciones en torno a la seguridad internacional y al humanitarismo, atrayendo una atención global sin precedentes.
Transformación doctrinaria	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	la guerra inteligente es una guerra centrada en el conocimiento, y el núcleo es el "cálculo".
Transformación doctrinaria	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	La tecnología de IA está cambiando constantemente la forma de la guerra futura, generando nuevos modelos de operaciones.
Transformación doctrinaria	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	El desarrollo integrado de la tecnología de IA y la inteligencia mejora esencialmente la capacidad de recopilación de inteligencia y el análisis de minería de datos, e impulsa constantemente la transformación del trabajo de inteligencia hacia una dirección más autónoma e inteligente.
Transformación doctrinaria	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	Actualmente, la guerra inteligente está evolucionando rápidamente desde la previsión teórica hacia la forma de combate real [1

Transformación doctrinaria	20.What do Latin Americans think about the world system	la opinión pública latinoamericana más educada percibe con claridad tres transformaciones del sistema internacional: una disminución de la im- portancia de los Estados Unidos en la región, la irrupción de China a nivel global y regional, y la presencia de otros actores estatales relevantes en el concierto mundial.

Tabla 7

Soporte de la categoría 2: Capacidades estatales (análisis documental)

Subcategorías	Documentos	Contenido de cita
Arquitectura de seguridad Tecnológicas	3. Artificial Intelligence and Information Integrity	AI systems play a crucial role in prioritizing and demoting content in users' feeds based on their profiles and the platforms' business models.
Gobernanza tecno-militar Institucionales	3. Artificial Intelligence and Information Integrity	in December 2024, the Brazilian Senate approved the Brazilian Framework for Artificial Intelligence (Marco Legal da Inteligência Artificial), establishing governance structures for AI development and commercialization
Gobernanza tecno-militar Institucionales	3. Artificial Intelligence and Information Integrity	Global and regional AI policy frameworks must proactively tackle controversial and harmful applications rather than avoiding discussions of malicious or politically disruptive uses.
Autonomía tecnológica Tecnológicas	3. Artificial Intelligence and Information Integrity	Building ethical and inclusive AI demands that we close connectivity and skill gaps, correct algorithmic biases, uphold Indigenous data sovereignty and integrate diverse worldviews.
Institucionales	3. Artificial Intelligence and Information Integrity	Two documents (Peru's National Artificial Intelligence Strategy and the Montevideo Declaration on Artificial Intelligence and Its Impact in Latin America) did not address a single indicator.
Doctrinarias	3. Artificial Intelligence and Information Integrity	AI-powered tools that recommend content are not neutral. Algorithmic curation is shaped by the values and goals of the algorithm's creator
Doctrinarias	3. Artificial Intelligence and Information Integrity	Elections cannot fulfil their role without a shared reality based on facts.

Brechas regionales	3. Artificial Intelligence and Information Integrity	Across Latin America and the Caribbean, Indigenous communities face a pronounced ethnic digital divide, as infrastructure and connectivity often cater primarily to urban areas.
Institucionales	4.América Latina en el nuevo escenario internacional	el entorno institucional exhibe fragmentación, fragilidad y estancamiento, producto de una compleja arquitectura, la superposición de membresías y agendas
Doctrinarias	4.América Latina en el nuevo escenario internacional	el debate sobre la economía política del desarrollo ha estado marcado por una tensión entre las estrategias de mercado internistas dirigidas por el Estado y los enfoques aperturistas dirigidos por el mercado
Tecnológicas	4.América Latina en el nuevo escenario internacional	la región promoverá cadenas de valor regionales, lo cual requerirá de acuerdos políticos entre estados y mercados, incluyendo medidas de facilitación del comercio, de convergencia regulatoria e incluso de infraestructura y conectividad
Brechas regionales	4.América Latina en el nuevo escenario internacional	la participación del comercio intrarregional en las exportaciones totales de la región «sigue siendo una de las más bajas a nivel mundial
Brechas regionales	4.América Latina en el nuevo escenario internacional	una ralentización de las economías de la región, una baja tasa de comercio interregional y un marcado proceso de reprivatización
Preparación y resiliencia	4.América Latina en el nuevo escenario internacional	la pandemia de la COVID-19 supuso una nueva crisis transfronteriza para la región.

Institucionales	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	In the US and Europe, conversely, the challenge will be to develop effective cooperation between the military and private sector in the development of AI, while managing concerns around ethics and privacy.
Institucionales	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	China has already recognized this, as detailed by Elsa Kania in a recent report, and is working to fuse military and state-owned enterprise efforts to enhance China's AI capabilities and technologies
Doctrinarias	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	active measures doctrine in Russia is a type of attrition in that it seeks to deplete the opponents' sources of power
Doctrinarias	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	the application of AI in the military field will affect the balance of power at least through doctrinal changes and adaptations or through the creation of new capabilities
Dependencia tecnológica Tecnológicas	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	AI is a dual-use technology, and as with all dual-use technology its specifications determine the degree to which it is likely to spread in the military or civilian realms.

Tecnológicas	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	Much of historical innovation in technology has been derived from research conducted in private enterprises and research labs, sometimes with government funding.
Brechas regionales	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	Russia has not released a formal strategy for AI and is encumbered in some areas of technology by a lack of industrial and technological innovation
Preparación y resiliencia	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	Mission control has always been based on sensing, perception, comprehension and prediction (battlefield situational awareness) and has always been meant to provide effective real-time decision support
Preparación y resiliencia	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	AI will accentuate the importance of these functions. Trials of these types of battlefield AI have already taken place, such as those developed by the Defence Science and Technology Laboratory (Dstl) and UK industry partners (SAPIENT)
Institucionales	6. AI y políticas públicas en América Latina y el Caribe	In contrast, Latin America presents a fragmentation in its public administrations, with multiple levels of government that often compete with each other, which can generate inefficiencies and lack of coordination.

Doctrinarias	6. AI y políticas públicas en América Latina y el Caribe	AI has the potential to revolutionize the way the military functions, offering strategic benefits, such as the automation of weapons systems, the efficient analysis of large amounts of information to obtain intelligence, and the advancement of sophisticated technologies for surveillance and reconnaissance.
Tecnológicas	6. AI y políticas públicas en América Latina y el Caribe	Two of the most prominent cases are Brazil and Chile, which are leading the deployment of fiber optic networks at the regional level.
Tecnológicas	6. AI y políticas públicas en América Latina y el Caribe	These advances lay the foundations for the growth of innovative digital applications and services that drive digital transformation in both countries.
Brechas regionales	6. AI y políticas públicas en América Latina y el Caribe	However, despite the progress made in recent decades, Latin America and the Caribbean still face challenges related to the disparity in access to technology between urban and rural areas, as well as between different countries, reflecting an urgent need for continued investment and development in digital infrastructure.
Preparación y resiliencia	6. AI y políticas públicas en América Latina y el Caribe	in order to prepare for the changes brought about by AI in the workforce, policy makers and companies can consider several strategies. First, it is important to invest in education and training programs for workers, both to acquire AI-related skills and to improve job adaptability in a changing environment.
Institucionales	7.Latin American hemispheric security adapted	la OEA desde la creación del Comité Interamericano contra el Terrorismo (CICTE) ha impulsado diferentes instancias con el objeto de cohesionar la participación de los gobiernos
Institucionales	7.Latin American hemispheric security adapted	Los países necesitan un órgano de coordinación en las oficinas de la Presidencia o del Primer Ministro para supervisar la aplicación

Doctrinarias	7.Latin American hemispheric security adapted	la noción de "Seguridad Hemisférica", emanada de aquel sistema ha sufrido una notoria evolución
Doctrinarias	7.Latin American hemispheric security adapted	En la Declaración sobre Seguridad en las Américas de la Conferencia Especial de Seguridad de México de 2003, se amplío el concepto de “seguridad hemisférica”
Tecnológicas	7.Latin American hemispheric security adapted	La tendencia, según el Informe de Ciberseguridad 2016, elaborado por la OEA y el BID, asegura que la vigilancia estatal sobre las actividades y plataformas públicas y privadas que utilizan el ciberespacio
Tecnológicas	7.Latin American hemispheric security adapted	la creación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) [5], que se han generalizado en toda la región
Brechas regionales	7.Latin American hemispheric security adapted	A pesar de los esfuerzos, el Informe de Ciberseguridad 2016 demuestra que la región presenta vulnerabilidades "potencialmente devastadoras".
Brechas regionales	7.Latin American hemispheric security adapted	El atraso y desigualdad entre el desarrollo de los países y su acceso a la red ha provocado grandes trabas al avance de la ciberseguridad en la región.
Preparación y resiliencia	7.Latin American hemispheric security adapted	Se apunta a la creación de una red de alerta hemisférica que brinda formación al personal competente en la materia
Preparación y resiliencia	7.Latin American hemispheric security adapted	La mejora de las capacidades nacionales reviste de gran importancia para aumentar la confianza en los servicios digitales públicos y privados

Institucionales	9.Artificial intelligence governance challenges	La heterogeneidad institucional característica de América Latina (Hirschmann, 1958) crea un contexto en el que las decisiones sobre la gobernanza de la IA presentan dilemas propios de la acción colectiva
Doctrinarias	9.Artificial intelligence governance challenges	La inteligencia artificial es una tecnología de propósito general aplicada a una variedad de problemas y tareas.
Doctrinarias	9.Artificial intelligence governance challenges	Como artefacto, la inteligencia artificial es creada por humanos para lograr un propósito
Tecnológicas	9.Artificial intelligence governance challenges	Las infraestructuras de datos comprenden procesos de almacenamiento e intercambio de datos necesarios para que la sociedad opere los servicios e instalaciones
Tecnológicas	9.Artificial intelligence governance challenges	El desarrollo de infraestructura en América Latina es heterogéneo y se inserta en el ámbito global de manera periférica
Brechas regionales	9.Artificial intelligence governance challenges	Solo el 45,5% de los hogares latinoamericanos tienen acceso a banda ancha, y la brecha promedio en el uso de internet entre el quintil superior e inferior de ingresos es de alrededor del 40 por ciento
Brechas regionales	9.Artificial intelligence governance challenges	La región de Centroamérica y el Caribe carece de infraestructuras digitales, lo que refuerza nuevos patrones de desigualdad y exclusión

Preparación y resiliencia	9.Artificial intelligence governance challenges	Las capacidades analíticas fortalecen capacidades estatales más amplias, permitiendo a los gobiernos construir respuestas más sólidas a los problemas públicos
Preparación y resiliencia	9.Artificial intelligence governance challenges	El desarrollo de capacidades implica una capacitación humana acelerada para enfrentar los desafíos del avance de la inteligencia artificial.
Institucionales	13.Updating cognitive security in a global dimension	NATO and its allies should identify acts of cognitive (non-kinetic) warfare and create ‘cognitive organizations within their law enforcement and military organizations with communication channels operating throughout the Alli- ance
Institucionales	13.Updating cognitive security in a global dimension	The implementation of the concept of ‘cognitive warfare’ requires knowledge not only of the natural and technical sciences, but, to the full extent, of the humanities
Doctrinarias	13.Updating cognitive security in a global dimension	Cognitive warfare is interpreted as a war of ideologies, and the essence is to take control of people, organizations, nations, and to manipulate a person's consciousness and subconscious.
Doctrinarias	13.Updating cognitive security in a global dimension	Victory will be determined more from the point of view of capturing psychocultural rather than geographical heights.
Tecnológicas	13.Updating cognitive security in a global dimension	CogWar (as in the text of the report), based on the convergence of cognitive technologies, bio- and neurotechnologies, artificial intelligence technologies and big data processing has become a powerful means of spreading disinformation.

Tecnológicas	13.Updating cognitive security in a global dimension	the development of artificial intelligence, the technological capabilities of big data analysis and the intensive use of achievements in cognitive sciences and technologies
Preparación y resiliencia	13.Updating cognitive security in a global dimension	Education should also play a key role in the development of future critical thinkers
Preparación y resiliencia	13.Updating cognitive security in a global dimension	We must anticipate the impact of new technologies and the intersection of sci-entific fields in order to be effective in our CogWar protection strategy
Institucionales	15.Russia´s cooperation with the Latin American	El gobierno estadounidense está seguro de que la cooperación de Rusia con los países de América Latina y el Caribe pone en riesgo los intereses de Washington
Doctrinarias	15.Russia´s cooperation with the Latin American	los funcionarios de la administración de Joe Biden seguían insistiendo en que China y Rusia representaban una amenaza al dominio de EE. UU.
Doctrinarias	15.Russia´s cooperation with the Latin American	Rusia persigue varios objetivos en América Latina que consisten en: asegurar su presencia en la cercanía de EE.UU. como contrapeso
Doctrinarias	15.Russia´s cooperation with the Latin American	Uno de los propósitos sería desviar los recursos de Washington destinados para oponerse a Rusia en Europa
Brechas regionales	15.Russia´s cooperation with the Latin American	La mayoría de las naciones se ven vulnerables en lo económico como resultado de la pandemia y les resulta difícil acumular los recursos necesarios para llevar a la práctica el proceso de rearme
Brechas regionales	15.Russia´s cooperation with the Latin American	la escasez de recursos ha sido uno de los principales obstáculos para comprar armamentos rusos

Preparación y resiliencia	15.Russia´s cooperation with the Latin American	. La recesión se debe tanto al impacto pandémico como a los cambios políticos en la región.
Institucionales	21 Sistemas de armas autónomas y DIH	El Gobierno peruano, a través de la secretaria de Gobierno Digital de la Presidencia del Consejo de Ministros, ha puesto a disposición de la ciudadanía una Estrategia Nacional de Inteligencia Artificial (ENIA) correspondiente al periodo 2021-2026
Institucionales	21 Sistemas de armas autónomas y DIH	Hacker Laboratory, un laboratorio de innovación dentro de la Cámara de Diputados de Brasil, está utilizando plataformas de inteligencia artificial para facilitar las interacciones entre legisladores y ciudadanos
Tecnológicas	21 Sistemas de armas autónomas y DIH	La Inteligencia Artificial y los sistemas de aprendizaje automático están revolucionando no solamente la forma en la que vivimos y nos relacionamos, sino también la manera en la que aplicamos este tipo de tecnología en conflictos bélicos
Tecnológicas	21 Sistemas de armas autónomas y DIH	El Aprendizaje Automático, como su nombre lo dice, es la capacidad que tiene una máquina para aprender y evolucionar por sí misma.
Tecnológicas	21 Sistemas de armas autónomas y DIH	El reciente éxito y desarrollo acelerado de este tipo de tecnología es consecuencia del aumento de la capacidad de las computadoras y el crecimiento en la cantidad de información que tenemos disponible para su alimentación.
Brechas regionales	21 Sistemas de armas autónomas y DIH	en contextos como el de Sudamérica, se encuentra lejos de poder ser desarrollada a un nivel ‘‘confiable’’ por alguno de esos gobiernos.

Institucionales	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Las políticas públicas deben establecer mecanismos coherentes de gobernanza.
Doctrinarias	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Las Tres Leyes de la Robótica de Asimov ofrecen una base útil para reflexionar sobre la regulación macroética de la IA
Institucionales	26 Artificial intellrms control in modern warfare (1)	the CCW established a Group of Governmental Experts (GGE) on LAWS to formalise its discussions.
Doctrinarias	26 Artificial intellrms control in modern warfare (1)	Clausewitz popularly defined war as a continuation of political intercourse by other means
Doctrinarias	26 Artificial intellrms control in modern warfare (1)	The emergence of guerrilla warfare has also led to an unconventional way of fighting wars.
Tecnológicas	26 Artificial intellrms control in modern warfare (1)	AI refers to codes and algorithms that can perform intricate tasks considered exclusive to humans.
Tecnológicas	26 Artificial intellrms control in modern warfare (1)	The utilisation of Artificial Intelligence (AI) in present-day combat has fundamentally transformed the balance of power in terms of national security among the United States, China, Russia, and the private sector

Brechas regionales	26 Artificial intellrms control in modern warfare (1)	Currently, developed countries possess the authority to allocate substantial resources towards the research and development of AI, which will consequently amplify their capabilities. In contrast, developing nations will continue striving to bridge the gap and catch up in this field
Preparación y resiliencia	26 Artificial intellrms control in modern warfare (1)	These autonomous systems have been beneficial because they have early warning detection systems, alerting military personnel of potential threats and giving decision-makers more time to chart a potential course of action (Fornasier, 2021).
Dependencia tecnológica Institucionales	27 AI Governance in Latin America	the European approach cannot simply be transplanted into the region without the institutional density of the EU, which is fundamentally different from Lat- in America.
Tecnológicas	27 AI Governance in Latin America	. Out of the three pillars (Government, Data, and Technology) of the Government AI Readiness Index 2024, conducted by Oxford Insights, the Technology pillar remains the most significant challenge in the region and demands greater investment.
Brechas regionales	27 AI Governance in Latin America	According to several global rankings and reports on AI governance, worldwide, the trajectory of the Latin American region in this field is medium-to-low, with heterogeneous results across countries.
Preparación y resiliencia	27 AI Governance in Latin America	The scarcity of re- sources underscores the need for a strong role in research and development (R&D) from the private sector in the region, as well as improved efficiency and coordination

Institucionales	Investigación sobre las Áreas Clave de Aplicación Militar	Para desarrollar vigorosamente la tecnología militar inteligente, una de las tareas primordiales es dilucidar el mecanismo de acción y las características de la tecnología de IA, analizar los escenarios de aplicación donde esta tecnología desempeñará un papel importante, juzgar las principales direcciones de desarrollo de las aplicaciones militares y, al mismo tiempo, realizar una evaluación científica del nivel de madurez de los diversos campos tecnológicos y de aplicación, con el fin de proporcionar soporte técnico para el desarrollo de la tecnología militar inteligente
Tecnológicas	Investigación sobre las Áreas Clave de Aplicación Militar	Estados Unidos ya ha situado a la IA en el centro de su estrategia tecnológica para mantener su posición dominante como potencia militar global, siendo también de suma importancia en su "Tercera Estrategia de Compensación", habiendo logrado ya una ventaja significativa en la aplicación militar de la IA. Rusia, por su parte, ha centrado más sus esfuerzos en la transformación inteligente de medios físicos ("hardware"); basándose en una sólida base industrial militar, sus exploraciones prospectivas y disposiciones en el campo militar inteligente no deben subestimarse.
Tecnológicas	Investigación sobre las Áreas Clave de Aplicación Militar	Actualmente, 32 países en todo el mundo han desarrollado más de 150 tipos de UAV, y más de 10 países han equipado o están desarrollando buques de guerra no tripulados y vehículos de combate no tripulados
Institucionales	34 Geopolitical Marxism and the Promise of Radical Historicism	Rational state-building – the conjunction of nationalism, bureaucratization, and de-personalization of the modern state - as opposed to earlier, personal forms of rule is tied to industrialisation.

Dependencia tecnológica Tecnológicas	34 Geopolitical Marxism and the Promise of Radical Historicism	This allows them to adopt the most cutting-edge technologies, institutions, and material practices “pioneered” by the leading states of the international system.
Tecnológicas	34 Geopolitical Marxism and the Promise of Radical Historicism	plus a techno-deterministic account of military technology – separates the “material context” into two: a non-developing productive sector and a developing military sector.
Brechas regionales	34 Geopolitical Marxism and the Promise of Radical Historicism	UCD is conceived as the most general law of world history, developed as a “general abstraction” (Rosenberg 2006). It proceeds from the aprioristic idea of the multiplicity of co-existing polities – “the international” – whose uneven trajectories of development lead to international interactions that reinforce, rather than even out, their individual patterns of development
Brechas regionales	34 Geopolitical Marxism and the Promise of Radical Historicism	those states able to harness the drivers of modernity developed into the current core of the world order, while those states unable or impeded from mobilising them, for example through imperialism, did not
Preparación y resiliencia	34 Geopolitical Marxism and the Promise of Radical Historicism	the articulation not only of the essential long-term security interests and strategic war objectives of a polity, but combines the concern with how to win major wars with an emphasis on how to win the peace

Doctrinarias	35. The Influence of Strategic Culture Components on Bilateral and Regional Relations between Iran and Russia	deterrence against the West are common components of the strategic culture of Iran and Russia. In order to understand the strategic culture of the two countries
Doctrinarias	35. The Influence of Strategic Culture Components on Bilateral and Regional Relations between Iran and Russia	Russia's strategic culture comes from the intersection of political, military and economic culture. It is rooted in the geographic and spiritual parameters of Russian history.
Institucionales	36.Estudio bibliométrico sobre relaciones civiles-militares	La corriente institucional, liderada por Huntington (1957), quien planteó que las relaciones civiles-militares están moldeadas por dos variables principales: el imperativo funcional (amenazas externas) y los imperativos sociales (fuerzas sociales, ideologías e instituciones dominantes dentro de la sociedad).
Institucionales	36.Estudio bibliométrico sobre relaciones civiles-militares	Las teorías institucionales se centran en la influencia perdurable de reglas, patrones y tradiciones organizacionales en el comportamiento individual. Según Pion-Berlin (2001)
Brechas regionales Cooperación regional Respuestas regionales	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Establecer alianzas con países en desarrollo de Asia, África y América Latina para articular posiciones comunes frente a la hegemonía tecnológica del Norte.

Institucionales	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	La más importante es el mecanismo de la Convención sobre Ciertas Armas Convencionales (CCW) de las Naciones Unidas
Institucionales	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	reforzar la revisión nacional previa de nuevos armamentos (Artículo 36 del Protocolo I a los Convenios de Ginebra)
Autonomía estratégica Doctrinarias	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Política de “autonomía responsable”. Formular una doctrina nacional que limite el uso ofensivo de los LAWS
Doctrinarias	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	la posición de China puede caracterizarse como “prudente, cooperativa y equilibrada”
Tecnológicas	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Con el rápido avance de la inteligencia artificial, las plataformas militares no tripuladas han evolucionado aceleradamente.
Tecnológicas	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	El control de armamentos requiere mecanismos de verificación confiables, pero los LAWS complican esta tarea debido a la naturaleza dual (civil y militar) de la inteligencia artificial.
Brechas regionales	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	mecanismos de asistencia técnica para países con menor capacidad

Preparación y resiliencia	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Al mismo tiempo, debe mantener una mentalidad de “línea de base”, preparándose ante la posibilidad de un estancamiento o fracaso en este proceso
Institucionales	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	Estados soberanos: Unidades básicas del sistema internacional, clave en la gobernanza. China ha presentado documentos de posición en la ONU, abogando por "IA para el bien" y la cooperación global. Estados Unidos ha emitido principios éticos de IA.
Institucionales	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	Estados Unidos, Rusia, Reino Unido, India y la OTAN han lanzado estrategias de IA, promoviendo conceptos como "guerra algorítmica" y "guerra en mosaico".
Tecnológicas	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	Impulsados por el gran potencial militar de la IA, los principales países compiten intensamente en una carrera armamentística,
Rivalidad China-EE. UU. Tecnológicas	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	China y EE.UU., como líderes en IA, deben asumir responsabilidad y colaborar para guiar la gobernanza global.
Institucionales	19.Problemas de Derecho Internacional derivados	Por ejemplo, cuando las instituciones estatales y gubernamentales utilizan la IA para sus propios fines, surge la cuestión de si deben asumir la responsabilidad legal por las decisiones y acciones de la IA. Este problema no solo es significativo a nivel nacional, sino también en el derecho internacional.

Tecnológicas	19.Problemas de Derecho Internacional derivados	Las empresas líderes en tecnología de IA obtienen aún más ventajas económicas y estratégicas mediante el control de los recursos de datos y tecnologías inteligentes avanzadas.
Tecnológicas	38 Investigación sobre la tecnología de inteligencia artificial	Los principales países y economías del mundo están intensificando sus esfuerzos para diseñar la investigación y el desarrollo de la tecnología de inteligencia artificial
Tecnológicas	38 Investigación sobre la tecnología de inteligencia artificial	Esta es la primera vez que "inteligencia artificial" se define claramente como "un área clave para formar nuevos modelos industriales" desde el nivel nacional.
Doctrinarias	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	La guerra mecanizada es una guerra centrada en la plataforma, y el núcleo es el "movimiento"; la guerra de la información es una guerra centrada en la red, y el núcleo es la "conexión"; la guerra inteligente es una guerra centrada en el conocimiento, y el núcleo es el "cálculo". "Calcular" requiere reglas y estrategias, que es el algoritmo.
Tecnológicas	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	La cápsula combina algoritmos de aprendizaje automático con informática integrada de alto rendimiento para detectar, relacionar, identificar y rastrear objetivos de forma rápida y precisa.

Tecnológicas	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	Alpha Star" puede analizar, retroalimentar y estimar los resultados de la batalla basándose en la tecnología de redes neuronales para el entorno del campo de batalla. En el caso de que el terreno de la operación sea complejo, el espacio de actividad sea amplio, haya muchos factores desconocidos y el límite de tiempo para la toma de decisiones sea ajustado, la eficiencia de la toma de decisiones
Preparación y resiliencia	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	Quien ata la campana debe desatarla". Para responder a la confrontación de redes eléctricas en la era inteligente, aún se debe romper el problema a partir del concepto de inteligencia en sí mismo.
Institucionales	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	Los gobiernos de países como Estados Unidos y Rusia promulgaron una serie de documentos estratégicos y promovieron activamente la aplicación e investigación de proyectos de IA en defensa, ámbitos militares y otros campos.
Doctrinarias	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	En 2014, el Departamento de Defensa de EE. UU. propuso la "Tercera Estrategia de Compensación" [15], cuyo núcleo es utilizar tecnologías emergentes como big data e IA para lograr avances e innovaciones en conceptos y estilos operativos futuros,
Tecnológicas	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	Con el desarrollo y progreso continuo de tecnologías de IA como el big data, el reconocimiento de imágenes, el procesamiento del lenguaje natural y el aprendizaje profundo, los sistemas de inteligencia de máquinas han comenzado gradualmente a poseer la capacidad de comprensión autónoma, razonamiento y toma de decisiones similar a la humana.

Preparación y resiliencia	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	la mayoría de los sistemas de decisión inteligente tienen la capacidad de percibir autónomamente entornos complejos, comprimiendo enormemente el tiempo de reacción y operación de cada eslabón
Institucionales	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	. El ejército estadounidense planea lograr la agrupación de inteligencia colaborativa tripulada/no tripulada para 2025, realizar operaciones de escolta autónomas para 2030 y lograr la maniobra conjunta de armas combinadas para 2040 [3
Institucionales	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	El ejército ruso comenzó a formular una hoja de ruta para la "Tarea de Formación de Unidades de Robots" en 2020, con planes de formar unidades de robots de combate para 2025 [2].
Doctrinarias	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	Este documento toma el concepto de combate del sistema de asalto inteligente terrestre como objeto de investigación, propone un marco de modelo de concepto de combate y pasos de modelado basados en DoDAF, utiliza Rational Rhapsody para la implementación de modelado específico y utiliza métodos de experimentos de simulación basados en la plataforma Matlab para la validez del concepto de combate.

Tecnológicas	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	El SUAV de retransmisión está diseñado como un tipo atado para aumentar el ancho de banda de comunicación y como un sistema de componentes de MGV, y MGV, AUGV, SUAV de reconocimiento y ataque se configuran en una proporción de 1:2:1 para formar un sistema de combate de ataque tridimensional basado en el sistema de mando y control inteligente, basado en la red de colaboración de combate autoadaptable y con la fuerza terrestre como núcleo. El sistema se puede integrar aún más hacia arriba como una unidad operacional a nivel de pelotón.
Dependencia tecnológica Tecnológicas	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	La limitación de la capacidad de comunicación es un factor importante que debe tenerse en cuenta en el concepto operacional
Preparación y resiliencia	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	el sistema de asalto inteligente terrestre tiene un mejor rendimiento de descubrimiento de objetivos, una velocidad de respuesta de ataque de potencia de fuego más rápida y un tiempo total de finalización de la tarea más corto
Preparación y resiliencia	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	la nueva presión de carga de comunicación está dentro del rango de soporte de capacidad técnica actual
Institucionales	20.What do Latin Americans think about the world system	en países democráticos, como lo son la gran mayoría de los de la región, las preferencias de la opinión pública inciden en los resultados electorales y en la agenda de gobierno.

Doctrinarias	20.What do Latin Americans think about the world system	el Realismo Neoclásico sopesa también las variables endógenas -las percepciones de los tomadores de decisión, la orientación de la cultura estratégica de cada país
Tecnológicas	20.What do Latin Americans think about the world system	China es percibida a la cabeza en los temas vinculados a las ciencias y las tecnologías digitales.
Brechas regionales	20.What do Latin Americans think about the world system	En Brasil la influencia de Estados Unidos y China es casi similar, aunque el primero tiene siete puntos más de preferencias
Preparación y resiliencia	20.What do Latin Americans think about the world system	La encuesta arroja posicionamiento de la opinión pública muy cercanos a los acontecimientos de la realidad, en especial en lo que se refiere a los apoyos en salud y vacunas que la región recibió durante la pandemia.

Tabla 8

Soporte de la categoría 3: Vacíos de gobernanza (análisis documental)

Subcategorías	Documentos	Contenido de cita
Captura tecnológica	4.América Latina en el nuevo escenario internacional	la necesidad de fortalecer las cadenas de valor regionales, la superación de asimetrías y la implementación de medidas de facilitación del comercio e integración financiera.
Captura tecnológica	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	much of the technology is being developed by the private sector, including companies like IBM, Google and Apple in the US, and Baidu, Alibaba and Tencent in China, leaving legislators struggling to regulate, control and mitigate some of AI's associated risks
Captura tecnológica	7.Latin American hemispheric security adapted	se suma el poder que las grandes corporaciones vinculadas a la tecnología ostentan con el dominio de la información en Internet.
Captura tecnológica	7.Latin American hemispheric security adapted	Facebook, Google, Microsoft, Twitter y Yahoo han expresado su preocupación ante el Parlamento sobre dicho proyecto
Captura tecnológica	9.Artificial intelligence governance challenges	"El colonialismo de datos significa que las nuevas relaciones sociales (relaciones de datos que generan insumos brutos para el procesamiento de la información) se convierten en un medio clave mediante el cual se crean nuevas formas de valor económico
Captura tecnológica	9.Artificial intelligence governance challenges	Una vez que las grandes corporaciones controlan los datos, controlan la estructura de la información global

Captura tecnológica	13.Updating cognitive security in a global dimension	cognitive warfare ‘pursues two separate but complementary goals: destabilization and influence… The targets of cognitive warfare attacks can range from entire populations to individual leaders in politics, economics, religion, and academia
Captura tecnológica	13.Updating cognitive security in a global dimension	Its very essence is to seize control over people (civil and military), organizations, nations, as well as ideas, psychology, especially behavioral, thoughts, as well as the environment
Captura tecnológica	15.Russia´s cooperation with the Latin American	Rusia, más que otros socios, está dispuesta a compartir sus tecnologías militares con los compradores
Captura tecnológica	15.Russia´s cooperation with the Latin American	muchos países latinoamericanos poseen armamentos de fabricación soviética o rusa que necesitan mantenimiento técnico adecuado
Captura tecnológica	21 Sistemas de armas autónomas y DIH	la lucha de poder nos lleva a analizar el hipotético caso en el que estas tecnologías sirvan para objetivos más perversos y efectivamente sean usadas en contextos militarizados sin ningún tipo de restricción.
Captura tecnológica	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	. La creciente dependencia tecnológica también implica una relación de dominación encubierta de la tecnología sobre los seres humanos.
Captura tecnológica	26 Artificial intellrms control in modern warfare (1)	The United States has lagged in military technologies and increasingly relies on large technological corporations to keep peace

Captura tecnológica	26 Artificial intellrms control in modern warfare (1)	Secrecy: The rise of ‘AI Competition’ has caused entities to guard their AI algorithms closely to stay ahead (Mittelsteadt, 2021), leading to a culture of secrecy and reluctance to disclose their use of AI systems
Captura tecnológica	11.Geopolitics in the digital age	The ‘closed world’ narrative frames the Act as vital for national security and reducing dependence on foreign – primarily Chinese – supply chains.
Captura tecnológica	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Los algoritmos de aprendizaje automático pueden copiarse y reutilizarse fácilmente para fines militares o civiles
Ético	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	AI is already being weaponized and the debate about banning fully autonomous weapons systems ignores much of the other weaponization processes pertaining to AI that are already in full swing.
Ético	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	Recent reports suggest that the US military is now more trusted to develop AI systems than some of the big tech companies such as Google and Facebook, reflecting recent controversies around social media being used as a platform for AI-enabled information warfare and data privacy breaches
Ético	6. AI y políticas públicas en América Latina y el Caribe	the adoption of AI in the public sector must be done with adequate human oversight, data protection, privacy and prevention of discrimination, which means that AI systems must be understandable and justifiable
Ético	7.Latin American hemispheric security adapted	la conciencia de la intersección entre la Ciberseguridad y los datos personales ha quedado más clara, ya que se trataba de comunicaciones electrónicas diarias.

Ético	7.Latin American hemispheric security adapted	Después de las revelaciones de Snowden [7], en 2013, la conciencia de la intersección entre la Ciberseguridad y los datos personales ha quedado más clara
Ético	9.Artificial intelligence governance challenges	el punto común en todas las estrategias es la definición de principios, generalmente asociados a la difusión de valores éticos por parte de la OCDE y la UNESCO.
Ético	9.Artificial intelligence governance challenges	El objetivo (de La Declaración de Santiago) expresado en la declaración es “promover la inteligencia artificial ética en América Latina y el Caribe”
Ético	15.Russia´s cooperation with the Latin American	Al mismo tiempo, se hace sentir la tradición del “internacionalismo republicano”. Surgido en el siglo XIX, este concepto tuvo una fuerte influencia en la diplomacia latinoamericana, promoviendo el principio de la separación de poderes y el rechazo a la dominación.
Ético	21 Sistemas de armas autónomas y DIH	Si bien es cierto que esto parece una realidad utópica, es necesario empezar a pensar en las implicancias legales y éticas, así como considerar medidas para la supervisión, regulación y conducción responsable por parte de quienes la controlen (De Spiegeleire, 2017, p. 16)
Ético	21 Sistemas de armas autónomas y DIH	Debe existir siempre un elemento de ‘‘humanidad’’ que permita tomar la decisión de si se debe actuar o no luego de recibir este tipo de información

Ético	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	El diseño ético debe integrar mecanismos de explicabilidad, transparencia y supervisión
Ético	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Fortalecer la evaluación y gestión del riesgo ético. Se requiere un sistema de evaluación que combine visiones macro-filosóficas y micro-indicadores operativos, para retroalimentar el desarrollo seguro de la IA
Ético	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	los riesgos éticos derivados de su aplicación se han vuelto cada vez más evidentes
Ético	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Argumentos sobre la Posibilidad de que la Inteligencia Artificial Genere Riesgos Éticos
Ético	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	La comunidad académica coincide en que la IA tiene la capacidad de desencadenar dilemas morales

Ético	26 Artificial intellrms control in modern warfare (1)	. It is recommended that the United Nations First Committee implement proactive measures to ensure the ethical use of these novel artillery weapons.
Ético	26 Artificial intellrms control in modern warfare (1)	Shifting the moral judgement for killing from humans to machines presents a new challenge regarding consequentialist and deontological ethics
Ético	26 Artificial intellrms control in modern warfare (1)	giving a machine the autonomy to kill humans is unethical and can lead to mass killings that will stifle global peace efforts and increase security threats,
Ético	27 AI Governance in Latin America	In a context where il- liberal regimes are on the rise, it would be naïve to underestimate the fact that AI tools can become a powerful weapon for surveillance, privacy violations, and re- strictions on freedom.
Ético	Investigación sobre las Áreas Clave de Aplicación Militar	Sin embargo, a corto plazo, la tecnología de IA aún no puede reemplazar a los humanos en la toma de decisiones de mando y control, solo puede desempeñar un papel de apoyo
Ético	34 Geopolitical Marxism and the Promise of Radical Historicism	Such a radically historicist Geopolitical Marxism is also able to respond to the challenge Postcolonial and Decolonial scholars have mounted against Marxism’s ability to fully comprehend modernity due to its colonial lineages and legacies
Ético	34 Geopolitical Marxism and the Promise of Radical Historicism	Norms, ideas, and culture are privileged by Constructivism, the English School, and Liberalism – institutionalist and ideational – without situating norm-production within the broader confines of socio-economic and political history

Ético	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	¿acepta la conciencia pública global otorgar a máquinas la potestad de quitar la vida humana?
Ético	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Reforzar los programas de investigación en ética de la inteligencia artificial
Ético	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	la prominencia de los sistemas de armas autónomas letales (LAWS) ha generado creciente preocupación por la seguridad, controversias éticas e incluso temores existenciales.
Ético	19.Problemas de Derecho Internacional derivados	Con el rápido desarrollo de la IA en los últimos años, la comunidad internacional también enfrenta una serie de desafíos legales y éticos relacionados con la IA.
Ético	19.Problemas de Derecho Internacional derivados	una serie de principios éticos y directrices formulados por organizaciones e instituciones internacionales. Estos principios éticos y directrices pueden guiar el desarrollo y aplicación de la tecnología de IA para que se ajuste a los principios éticos y mecanismos de derechos humanos. Por ejemplo, el Marco de Ética e Impacto Social de la Inteligencia Artificial de la UNESCO, las Directrices Éticas para la Inteligencia Artificial del Consejo de Europa, etc.
Ético	20.What do Latin Americans think about the world system	la Unión Europea emerge como líder en temas normativos y sociales.

Legal	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	The lack of transparency of most AI algorithms in performing designated tasks is a significant problem and creates obstacles to their deployment in active security and defense roles.
Legal	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	In recent years activists, scientists and governments have sought to place UN-level bans on ‘killer robots’, including Lethal Autonomous Weapons Systems
Legal	6. AI y políticas públicas en América Latina y el Caribe	In Latin America the situation is very different, since, although nineteen countries in the region have sanctioned laws on the protection of personal data, there is no instrument with the characteristics of the GDPR.
Legal	7.Latin American hemispheric security adapted	la creación de una base jurídica armonizada para abordar los delitos cibernéticos. Según su análisis, el mejor medio para dicha cooperación es la Convención de Budapest
Legal	7.Latin American hemispheric security adapted	Esto culminó (Brasil ofrece un caso interesante) en la aprobación del Marco Civil de Internet, que trata temas como la protección de los derechos fundamentales en línea
Legal	9.Artificial intelligence governance challenges	la Carta Iberoamericana sobre Inteligencia Artificial del CLAD no avanza a nivel regulatorio, defendiendo una perspectiva ética.
Legal	9.Artificial intelligence governance challenges	(Chile)Aborda el consumidor, la privacidad y protección de datos, los sistemas de propiedad intelectual y la ciberseguridad.

Legal	21 Sistemas de armas autónomas y DIH	El establecimiento de un marco normativo claro y ajustado a la realidad sobre los medios de guerra que funcionan aplicando la Inteligencia Artificial es poco, por no decir nulo
Legal	21 Sistemas de armas autónomas y DIH	La falta de un sistema normativo preciso como consecuencia de su novedad, tanto en el ámbito internacional como en el nacional, significa que existe un vacío normativo
Legal	21 Sistemas de armas autónomas y DIH	Artículo 36. Armas nuevas Cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable
Legal	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Los estudios proponen enfoques desde la moral y el derecho: Principio de “primacía de lo humano “Límite legal claro frente a decisiones autónomas Legislación temática en campos como privacidad, transporte, medicina o derechos de auto
Legal	26 Artificial intellrms control in modern warfare (1)	Article 36 of Additional Protocol I to the Geneva Conventions, nations must review new weapons and ensure they are not indiscriminate or have the capacity to cause unnecessary injury (Lewis, 2015)
Legal	26 Artificial intellrms control in modern warfare (1)	The Martens Clause also dictates that individuals will remain ‘under the protection and rule of law of nations … from the laws of humanity and the dictates of public conscience’
Legal	34 Geopolitical Marxism and the Promise of Radical Historicism	Westphalia codified this new inter-dynastic state order, transcending papal claims to cosmopolitan rule and lordly claims to parcellated sovereignty

Legal	34 Geopolitical Marxism and the Promise of Radical Historicism	Major international peace settlements – Westphalia 1648, Utrecht 1713, Paris and Hubertusburg 1763, Vienna 1815, Berlin 1885, Versailles 1919 – that reconfigure international order and political geography and establish new principles for international conduct (international regimes) are empirically acknowledged but remain theoretically undigested.
Legal	11.Geopolitics in the digital age	U.S. leaders seek to establish a common international framework for responsible AI use and to re- organize the global governance system of the Internet.
Legal	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	El marco jurídico internacional pertinente es, ante todo, el Derecho Internacional Humanitario (DIH) y el Derecho Internacional de los Derechos Humanos.
Legal	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	la cláusula de la conciencia pública (Martens Clause) como fundamento ético-jurídico.
Legal	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	LAWS abarca muchos riesgos de seguridad, como escalada de conflictos, inestabilidad estratégica y riesgos humanitarios. La definición de LAWS es clave: sistemas letales y autónomos plantean riesgos únicos, ya que las leyes de conflicto armado no pueden responsabilizar a máquinas.
Legal	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	En 2019, la CCW acordó 11 principios rectores, pero no son vinculantes. El progreso es lento debido a desacuerdos entre estados.

Legal	19.Problemas de Derecho Internacional derivados	Los Estados deben cumplir con sus obligaciones internacionales y asumir la responsabilidad estatal que surge de actos estatales que violan obligaciones internacionales. Sin embargo, el problema de la atribución de la responsabilidad estatal es uno de los más importantes sin resolver en el derecho internacional y también se ha convertido en un foco principal de controversia.
Legal	19.Problemas de Derecho Internacional derivados	Actualmente, el derecho internacional no ha formulado un marco legal y normas específicos dirigidos específicamente a los sistemas de armas autónomas.
Operativo	4.América Latina en el nuevo escenario internacional	el SICA y CARICOM generaron un espacio regional para coordinar respuestas concertadas
Operativo	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	AI will Facilitate real-time analysis and improve situational awareness of the battlefield;
Operativo	6. AI y políticas públicas en América Latina y el Caribe	An example of efficiency in the public sphere would be the automation of routine administrative tasks through AI, allowing public employees to focus on more strategic and value-added activities while reducing the time and costs associated with manual processes.
Operativo	7.Latin American hemispheric security adapted	surgen en a nivel nacional los Equipos de Respuesta a Incidentes (CSIRT) de "alerta, vigilancia y prevención" en materia de Ciberseguridad.

Operativo	7.Latin American hemispheric security adapted	los Estados han empezado a aprovechar la capacidad de sus fuerzas armadas nacionales y/o agencias de defensa relacionadas para defender a su país
Operativo	9.Artificial intelligence governance challenges	La algoritmización de las organizaciones burocráticas está arraigada aún más en los cambios en las rutinas de trabajo, racionalizando muchos procesos y alterando la lógica del trabajo organizacional.
Operativo	9.Artificial intelligence governance challenges	La adopción de sistemas algorítmicos codifica procedimientos para los agentes burocráticos, reordenando diversas prácticas burocráticas
Operativo	13.Updating cognitive security in a global dimension	Tactical and operational victories can be achieved in the first five domains; only in the human domain is it possible to achieve a final and complete victory.
Operativo	13.Updating cognitive security in a global dimension	Cognitive operations represent the sixth domain of hybrid warfare
Operativo	21 Sistemas de armas autónomas y DIH	La prueba, debe ser si un humano puede predecir razonablemente que la acción que tomará el AWS cumplirá con el DIH
Operativo	21 Sistemas de armas autónomas y DIH	La decisión de atacar o no a un blanco determinado es tomada por la persona a cargo, quien debe basar su evaluación en la inteligencia e información que razonablemente esté disponible para ella.

Operativo	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	¿Quién asume la responsabilidad de un ataque autónomo descontrolado?
Operativo	26 Artificial intellrms control in modern warfare (1)	AI is integrated into various functions in these aircraft, including navigation and control, taking over in emergencies, acquiring, filtering and fusing data to present the pilot with the most relevant information, suggesting courses of action to execute missions, and coordinating with other platforms
Operativo	26 Artificial intellrms control in modern warfare (1)	The FCAS is designed to fly in a heterogeneous configuration with a swarm of unmanned aerial vehicles (UAVs
Operativo	26 Artificial intellrms control in modern warfare (1)	The FCAS is designed to fly in a heterogeneous configuration with a swarm of unmanned aerial vehicles (UAVs)
Operativo	34 Geopolitical Marxism and the Promise of Radical Historicism	In a third step, it calls for the tracking of the making of statecraft, foreign policy and diplomacy in these dense institutional contexts, succeeded, step four, by a reconstruction of foreign policy encounters in the sphere of international politics,
Operativo	34 Geopolitical Marxism and the Promise of Radical Historicism	It is at this level – the coercive and non-coercive clash and accommodation between plural foreign policy encounters – that differential class interests and power resources may or may not generate international conflicts, which are creatively and decisively resolved and politically settled through international politics with open-ended consequences.

Operativo	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	un sistema de armas autónomas abarca el conjunto de componentes —sensores, módulos de decisión y municiones— que le permiten ejecutar operaciones autónomas
Operativo	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Asegurar trazabilidad y responsabilidad humana en el uso de la fuerza.
Operativo	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	Asegurar que los comandantes supervisen los sistemas de IA y sean responsables.
Operativo	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	Imponer restricciones en predictibilidad, tipos de objetivo, duración, ámbito geográfico y supervisión humana. Prohibir sistemas impredecibles o dirigidos a humanos.
Operativo	19.Problemas de Derecho Internacional derivados	Al ejercer un control "significativo" sobre los sistemas de armas de IA, no solo pueden ser regulados por el derecho internacional humanitario, sino que también puede aliviar hasta cierto punto la preocupación de las personas sobre las armas de IA: es decir, ¿la aparición de armas de IA
Operativo	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	el uso de una formación mixta de "Loyal Wingman" y aviones tripulados engaña y confunde al radar de defensa aérea enemigo, haciendo que el enemigo juzgue mal el modelo, el número de salidas y los atributos de los objetivos aéreos, haciendo que la acción de irrupción sea más engañosa y oculta.

Operativo	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	los drones de "enjambre" pueden usar el equipo de interferencia electrónica que llevan para formar un haz sintético, o interferir con el radar enemigo desde múltiples direcciones y múltiples ángulos al mismo tiempo para garantizar una supresión efectiva, a fin de abrir un corredor aéreo para las fuerzas de operación de seguimiento.
Operativo	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	debido a las limitaciones de las funciones fisiológicas humanas, como la baja eficiencia cognitiva y la consideración limitada de factores, el personal de análisis de inteligencia por sí solo no puede procesar directamente datos no estructurados como imágenes, audio y video.
Operativo	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	Actualmente, el desarrollo de equipos de asalto terrestre inteligentes enfrenta principalmente dos desafíos: primero, varios equipos se desarrollan de forma independiente, con diferentes formas de combate y métodos de aplicación, y no pueden llevar a cabo un intercambio de datos de protocolo eficiente entre sí, lo que dificulta la realización de acciones coordinadas; segundo, el grado de inteligencia de los sistemas de combate no tripulados no es alto, y el método de control se basa principalmente en el tipo de control remoto o el tipo de operación remota, y las características inteligentes y autónomas no se reflejan lo suficiente
Rendición de cuentas	4.América Latina en el nuevo escenario internacional	Esto queda reflejado, por ejemplo, en la persistente falta de respuestas regionales comunes a la crisis multidimensional de Venezuela

Rendición de cuentas	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	The notion that has been often stated on the military side of the LAWS debate, that there will always be an element of human control, appears to be fanciful in the current context.
Rendición de cuentas	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	Trust will be an integral factor – military decision-makers will have to either trust from ignorance or from verification
Rendición de cuentas	6. AI y políticas públicas en América Latina y el Caribe	In this context, government institutions must take responsibility for ADM and be prepared to be accountable for any negative outcomes or unintended impacts
Rendición de cuentas	7.Latin American hemispheric security adapted	esto (la protección de la privacidad en línea y los datos personales) se debe hacer de una manera que no menoscabe estos principios básicos.
Rendición de cuentas	7.Latin American hemispheric security adapted	Grupos de la sociedad civil, la academia y la comunidad técnica, así como representantes de la industria pueden proporcionar valiosa experiencia desde sus perspectivas, y ayudar a diseñar un marco reglamentario racional de una manera sostenible.
Rendición de cuentas	9.Artificial intelligence governance challenges	En cuanto al nivel regulatorio, todas las estrategias nacionales latinoamericanas tienden a reforzar una perspectiva de autorregulación por parte de las empresas

Rendición de cuentas	9.Artificial intelligence governance challenges	(Uruguay)definir mecanismos de transparencia y rendición de cuentas para las soluciones de IA aplicadas en el gobierno.
Rendición de cuentas	15.Russia´s cooperation with the Latin American	los gobiernos latinoamericanos no se han mostrado muy dispuestos a unirse a dichas imposiciones.
Rendición de cuentas	15.Russia´s cooperation with the Latin American	la reacción negativa a las sanciones, a la idea de suministrar armas a Ucrania y críticas a las acciones unilaterales de Washington
Rendición de cuentas	21 Sistemas de armas autónomas y DIH	Esto genera una ‘‘brecha’’ en la responsabilidad o la rendición de cuentas y podría significar un dilema al momento de tomar la decisión de insertar un sistema de este tipo en las hostilidades (Lewis, 2018, p. 13)
Rendición de cuentas	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Especial atención requiere la identificación de responsabilidad en sistemas autónomos: diseñadores, operadores, usuarios o incluso entidades jurídicas nuevas para IA avanzada.
Rendición de cuentas	26 Artificial intellrms control in modern warfare (1)	the core ethical challenges in the implementation of this technology are control and accountability.
Rendición de cuentas	26 Artificial intellrms control in modern warfare (1)	Feeding this technology information from a biased perspective will lead to the assessment of prejudiced data by AI tools, which may be brought to bear by using autonomous weapons in the long ru

Rendición de cuentas	27 AI Governance in Latin America	AI can not only optimize the provision of public services, such as healthcare, education, and transportation, but can also enhance accountability by improving how government explain their use of public funds and justify decision making
Rendición de cuentas	11.Geopolitics in the digital age	U.S. political leaders legitimize their country's central role in shaping the rules and norms for the governance of emerging technologies
Rendición de cuentas	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	El vacío de responsabilidad (accountability gap). Si un arma autónoma causa muertes civiles, ¿quién es responsable?
Rendición de cuentas	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Para evitar el "vacío de responsabilidad" es necesario que las cadenas de mando y los actores —desde diseñadores y fabricantes hasta comandantes y operadores— tengan obligaciones claras de diligencia y rendición de cuentas.
Rendición de cuentas	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	sistemas letales y autónomos plantean riesgos únicos, ya que las leyes de conflicto armado no pueden responsabilizar a máquinas.
Rendición de cuentas	19.Problemas de Derecho Internacional derivados	el proceso de toma de decisiones de los sistemas de armas autónomas hace difícil confirmar y atribuir responsabilidades. Si un sistema de armas autónomas causa una violación de las disposiciones del derecho internacional humanitario, cómo atribuir responsabilidades y garantizar los procedimientos judiciales adecuados sigue siendo un problema. Para los daños causados por los sistemas de armas autónomas de IA, ¿debe ser el fabricante o el usuario el sujeto responsable?

Rendición de cuentas	19.Problemas de Derecho Internacional derivados	Atribuir la responsabilidad internacional a los criminales de guerra ya es difícil en el nivel del derecho internacional, y los sistemas de armas autónomas traídos por el desarrollo de la tecnología artificial hacen que la rendición de cuentas sea aún más difícil
Rendición de cuentas	20.What do Latin Americans think about the world system	Como se puede apreciar, las democracia es valorada en gran parte de los países de la región
Rendición de cuentas	20.What do Latin Americans think about the world system	Los regímenes políticos mejor auto valorados son los Costa Rica y Uruguay

Tabla 9

Soporte de la categoría 4: Competencia geoestratégica (análisis documental)

Subcategorías	**Documentos**	**Contenido de cita**
Agenda hemisférica	3. Artificial Intelligence and Information Integrity	From Argentina to Mexico and from Brazil to El Salvador, the contamination of the information environment represents a defining challenge for democracy across the continent
Agenda hemisférica	3. Artificial Intelligence and Information Integrity	Artificial intelligence (AI) could reshape Latin America's electoral landscape by further exacerbating existing problems with how information is created, curated and disseminated.
Agenda hemisférica	3. Artificial Intelligence and Information Integrity	The issue goes beyond the spread of false or inaccurate information: it involves the manipulation of the information ecosystem to amplify certain political narratives, steer the political agenda and debate, and normalize or legitimize ideas and policies that were, until recently, on the fringes of political discourse.
Agenda hemisférica	4.América Latina en el nuevo escenario internacional	La próxima Cumbre del G-20 en noviembre de 2024, liderada por Brasil, supondrá una prueba tanto para este país como líder regional, como para la capacidad de construcción de consensos mínimos por parte de los países de la región y tener así una voz en la escena internacional.
Agenda hemisférica	6. AI y políticas públicas en América Latina y el Caribe	These regional initiatives not only strengthen Europe's position on the global AI scene but also promote innovation and technological development within the continent.

Agenda hemisférica	6. AI y políticas públicas en América Latina y el Caribe	The ILIA results highlight the diversity in AI development in the region, with countries excelling in specific areas, but showing deficiencies in others. For example, while some nations show high scientific productivity, they lack efficient technology transfer, and others have abundant data available, but lack the infrastructure to take advantage of it. This diversity suggests great potential for cross-learning among countries in the region, where strengths can be leveraged and weaknesses overcome through collaboration.
Agenda hemisférica	7.Latin American hemispheric security adapted	la OEA y el BID, que son los actores más relevantes en la elaboración de parámetros para una política hemisférica de ciberseguridad
Agenda hemisférica	7.Latin American hemispheric security adapted	la Cumbre Mundial sobre la Sociedad de la Información (CMSI) [3] en la que se reunieron por primera vez en igualdad de condiciones
Agenda hemisférica	15.Russia´s cooperation with the Latin American	EE.UU. intentaría presionar económica y políticamente para expulsar a Rusia de la región.
Agenda hemisférica	15.Russia´s cooperation with the Latin American	la presencia de Rusia en el mercado de armas de la región podría disminuir, lo cual se debe a distintos factores, entre ellos a la presión económica y política estadounidense
Agenda hemisférica	11.Geopolitics in the digital age	China’s solidarity will ensure developing countries can gain from technological advancements and will not be marginalized
Agenda hemisférica	20.What do Latin Americans think about the world system	el juego mundial no puede ser pensado exclusivamente como una confrontación sino-americana porque también participan en él otros actores del sistema mundial.

Autonomía estratégica	4.América Latina en el nuevo escenario internacional	como una comunidad de naciones soberanas, capaz de profundizar los consensos en temas de interés común y contribuir al bienestar y desarrollo de la región
Autonomía estratégica	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	China certainly has some advantages, including a productive and innovative economic and industrial base, and the clear articulation of national strategies around AI
Autonomía estratégica	6. AI y políticas públicas en América Latina y el Caribe	ENIA aims to transform and upgrade the national industry and public service through AI, strengthen technological and data sovereignty, and position the country as a regional AI hub.
Autonomía estratégica	7.Latin American hemispheric security adapted	la creación de una capacidad estratégica en Ciberseguridad sigue siendo esencial y todas las naciones se benefician del intercambio de mejores prácticas
Autonomía estratégica	7.Latin American hemispheric security adapted	Brasil, por ejemplo, ya ha desarrollado capacidades avanzadas de defensa cibernética
Autonomía estratégica	9.Artificial intelligence governance challenges	La soberanía digital se refiere a que un Estado (gobierno) o una organización debe establecer su autoridad para ejercer sus poderes en el ciberespacio.
Autonomía estratégica	9.Artificial intelligence governance challenges	países como Brasil y Chile han buscado soluciones para la creación de infraestructuras digitales públicas soberanas

Autonomía estratégica	15.Russia´s cooperation with the Latin American	los países de ALC que se empeñan en aplicar políticas independientes ahora se ven en aprietos.
Autonomía estratégica	26 Artificial intellrms control in modern warfare (1)	The Great Powers of the 21st-century international system are not defined only by large territories, economy or political stability but by technological advancements coupled with military might.
Autonomía estratégica	26 Artificial intellrms control in modern warfare (1)	Each nation strives to outdo itself in developing new techniques for using these weapons and introducing innovative military technology
Autonomía estratégica	27 AI Governance in Latin America	Latin American countries are searching for their place in the AI value chain.
Autonomía estratégica	34 Geopolitical Marxism and the Promise of Radical Historicism	Henceforth, “perfidious Albion” became the offshore balancer of “Westphalian order” without actively transforming continental socio-economic or political relations, reserving military intervention as its ultima ratio
Autonomía estratégica	34 Geopolitical Marxism and the Promise of Radical Historicism	This implied the formation of Realpolitik, resting on a sober calculus of the secular interests of the “political nation”, as opposed to the whims of dynastic interests.

Autonomía estratégica	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	En el futuro, la operación inteligente en el campo de la red eléctrica debe innovar la guía de la operación de confrontación de la red eléctrica, confiar en equipos de confrontación de la red eléctrica más autónomos e inteligentes, centrarse en la tecnología inteligente autónoma, la colaboración hombre-máquina y la tecnología de colaboración de grupos para superar las dificultades, mejorar gradualmente el nivel de inteligencia del equipo de confrontación de la red eléctrica y, a través del uso de una arquitectura de sistema abierto, realizar el intercambio de datos, la creación de redes multi máquina, la cooperación coordinada y la conexión perfecta, y finalmente formar un sistema de operación de red eléctrica distribuida, mejorar la capacidad integral de operación de red eléctrica en la era inteligente.
Autonomía estratégica	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	Aprovechar plenamente estas características ventajosas de la tecnología de IA, corrigiendo y optimizando constantemente las estrategias, busca lograr una decisión global óptima generada al final del trabajo de inteligencia
Autonomía estratégica	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	El sistema de asalto inteligente terrestre adopta el nuevo concepto de "agrupación modular, despliegue discreto, aplicación integrada".
Autonomía estratégica	20.What do Latin Americans think about the world system	la mayoría absoluta de los latinoamericanos opinaba que la Unión Europea actuaba con autonomía respecto a Estados Unidos

Dependencia tecnológica	6. AI y políticas públicas en América Latina y el Caribe	according to the recent global AI index pre- pared by Tortoise (2024), the United States leads the ranking followed by China and Singapore, while Latin America barely manages to rank 30th, with Brazil at the top, followed by Chile (38th), Mexico (45th) and Argentina (47th).
Dependencia tecnológica	7.Latin American hemispheric security adapted	Las economías nacionales que están conectadas a la Internet global y que aprovechan el servicio de Internet crecen más rápidamente
Dependencia tecnológica	9.Artificial intelligence governance challenges	La dependencia tecnológica de los países latinoamericanos se refleja en la disponibilidad de infraestructura de datos
Dependencia tecnológica	9.Artificial intelligence governance challenges	La dependencia surge de las asimetrías en la economía política global en la que los países en desarrollo están subordinados a la producción de materias primas de bajo valor agregado
Dependencia tecnológica	9.Artificial intelligence governance challenges	La inserción de América Latina en un mundo marcado por la inteligencia artificial es dependiente
Dependencia tecnológica	21 Sistemas de armas autónomas y DIH	La cantidad de información que hemos ido volcando como usuarios aumenta diariamente de manera exponencial.
Dependencia tecnológica	24Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la	La creciente dependencia tecnológica también implica una relación de dominación encubierta de la tecnología sobre los seres humanos.

	Inteligencia Artificial	
Dependencia tecnológica	26 Artificial intellrms control in modern warfare (1)	Because AI depends on computers, the devices and the linked databases may be vulnerable to threats from sophisticated computer hacking, and wireless networks linking AI devices may also be vulnerable to electronic jamming.
Dependencia tecnológica	26 Artificial intellrms control in modern warfare (1)	Big data and machine learning are fundamental to the optimal performance of AI algorithms
Dependencia tecnológica	Investigación sobre las Áreas Clave de Aplicación Militar	El principio de funcionamiento de la IA combina grandes volúmenes de datos, una capacidad de cálculo excepcional y algoritmos inteligentes para establecer un modelo que resuelva problemas específicos, permitiendo que el programa aprenda automáticamente patrones o características subyacentes a partir de los datos, logrando así una forma de pensamiento cercana a la humana.
Dependencia tecnológica	11.Geopolitics in the digital age	China’s AI Self-Sufficiency Policy focused on reducing reliance on foreign technologies by investing in domestic innovation.
Dependencia tecnológica	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	El desarrollo militar de la inteligencia artificial ofrece un enorme incentivo estratégico para los Estados.

Dependencia tecnológica	38 Investigación sobre la tecnología de inteligencia artificial	Sin embargo, los recursos de datos que aplican la tecnología de inteligencia artificial todavía enfrentan dos problemas: el estado de la isla de los recursos de datos sigue siendo relativamente obvio y, debido a las limitaciones de la seguridad y el modelo comercial, la apertura de los recursos de datos controlados por varias organizaciones aún necesita promoción;
Dependencia tecnológica	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	la información pública de Internet se ha convertido en una fuente importante de datos para la inteligencia militar.
Dependencia tecnológica	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	El SUAV de retransmisión está diseñado como un tipo atado para aumentar el ancho de banda de comunicación y como un sistema de componentes de MGV, y MGV, AUGV, SUAV de reconocimiento y ataque se configuran en una proporción de 1:2:1 para formar un sistema de combate de ataque tridimensional basado en el sistema de mando y control inteligente, basado en la red de colaboración de combate autoadaptable y con la fuerza terrestre como núcleo. El sistema se puede integrar aún más hacia arriba como una unidad operacional a nivel de pelotón
Respuestas regionales	3. Artificial Intelligence and Information Integrity	Brazil’s main electoral authority, the Superior Electoral Court, issued new regulations before the elections to curb misinformation and the misuse of AI-generated content

Respuestas regionales	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	In 2018, the EU, for example, released a civilian and economy-focused AI strategy, and in the last several years a host of countries, including Canada, China, Denmark, Finland, France, India, Italy, Japan, Mexico, Singapore, South Korea, Sweden, Taiwan, the UAE, and the UK have released strategies to promote the use and development of AI.
Respuestas regionales	6. AI y políticas públicas en América Latina y el Caribe	fAIr LAC works to create regulatory and ethical frameworks that ensure that the use of AI benefits all people, especially those in vulnerable situations, and fosters collaboration between governments, the private sector, academia and civil society to build a shared and coherent vision of AI in the region (Access Now, 2024).
Respuestas regionales	7.Latin American hemispheric security adapted	La OEA ostenta un rol líder a nivel mundial en el desarrollo de la cooperación internacional en materia de Ciberseguridad.
Respuestas regionales	7.Latin American hemispheric security adapted	la región se beneficiaría de una formulación continua de estrategias nacionales en Ciberseguridad.
Respuestas regionales	9.Artificial intelligence governance challenges	Argentina, Brasil, Chile, Colombia, México, Perú, República Dominicana y Uruguay han difundido estrategias nacionales de IA
Respuestas regionales	9.Artificial intelligence governance challenges	Recientemente, veinte países latinoamericanos, excepto Nicaragua, Bolivia, Panamá, firmaron la Declaración de Santiago
Respuestas regionales	15.Russia´s cooperation with the Latin American	los países que ya cooperan con Moscú en los asuntos de la seguridad han sido reacios a dar su apoyo a las políticas de EE.UU. en el mundo

Respuestas regionales	15.Russia´s cooperation with the Latin American	Venezuela, Cuba y Nicaragua se alinearon abiertamente con las acciones de Rusia
Respuestas regionales	27 AI Governance in Latin America	The first regional statement on AI did not come from governments but rather from the tech and academic community
Respuestas regionales	34 Geopolitical Marxism and the Promise of Radical Historicism	the spatio-temporally specific making of international orders. The central point that any account of geopolitical transformations needs to establish is that Europe did not march in lockstep through successive historical phases.
Respuestas regionales	11.Geopolitics in the digital age	China positions itself as an actor advocating for alternative governance models, fostering partnerships with the Global South to expand its influence.
Respuestas regionales	19.Problemas de Derecho Internacional derivados	el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, conocido como la "ley de datos más estricta de la historia"
Respuestas regionales	20.What do Latin Americans think about the world system	América Latina podría constituirse en un actor medianamente relevante del sistema si se consolidara un multipolarismo extendido
Respuestas regionales	20.What do Latin Americans think about the world system	La encuesta muestra que los encuesta- dos asignan a América Latina una importancia media en el mundo (en promedio, 6.6 puntos en 10),

Rivalidad China-EE. UU.	4.América Latina en el nuevo escenario internacional	una crisis global, como consecuencia de la pandemia de la COVID-19, donde se acentúan las reconfiguraciones que se venían dando en el sistema internacional producto del declive relativo de Estados Unidos, del ascenso de China, y la competencia estratégica entre ambos, escenificada en el ámbito multilateral.
Rivalidad China-EE. UU.	4.América Latina en el nuevo escenario internacional	la expansión de las relaciones entre China y América Latina desafía la ya reducida influencia de Estados Unidos y la Unión Europea (UE)
Rivalidad China-EE. UU.	5_Understanding the Strategic Implications of the Weaponization of Artificial Intelligence	By some accounts, an AI arms race is emerging between the great powers, and the US, China and Russia in particular.
Rivalidad China-EE. UU.	6. AI y políticas públicas en América Latina y el Caribe	The inclusion of powers, such as the United States and China, which often have divergent approaches to technology and governance, un- derscores the importance of this agreement as a unifying effort, with the European Union, with its more rigorous approach to technology regulation, bringing its expertise in creating policies that balance innovation with the protection of citizens' rights.
Rivalidad China-EE. UU.	15.Russia´s cooperation with the Latin American	la competitividad entre EE.UU. y Rusia en el mercado de armas y en temas de seguridad de América Latina.
Rivalidad China-EE. UU.	15.Russia´s cooperation with the Latin American	Washington mantendrá su liderazgo en las ventas de armas a las naciones de la región.

Rivalidad China-EE. UU.	21 Sistemas de armas autónomas y DIH	el presidente ruso ha declarado que el país que domine la Inteligencia Artificial será quien mantenga el poder mundial. Es el mismo caso con China, que quiere crear una industria de Inteligencia Artificial de 150 mil millones de dólares.
Rivalidad China-EE. UU.	26 Artificial intellrms control in modern warfare (1)	There appear to be hints at an ongoing Sino-American arms race, as China and America are observed to be heavily committed to proliferating autonomous weapons,
Rivalidad China-EE. UU.	26 Artificial intellrms control in modern warfare (1)	In the AI arms race, China has surpassed the expectations of international observers and analysts, who speculated that Beijing could not be a near competitor with the US
Rivalidad China-EE. UU.	27 AI Governance in Latin America	Amid intense geopolitical competition be- tween the US and China, Latin American countries are searching for their place in the AI value chain.
Rivalidad China-EE. UU.	Investigación sobre las Áreas Clave de Aplicación Militar	Estados Unidos ya ha situado a la IA en el centro de su estrategia tecnológica para mantener su posición dominante como potencia militar global, siendo también de suma importancia en su "Tercera Estrategia de Compensación", habiendo logrado ya una ventaja significativa en la aplicación militar de la IA. Rusia, por su parte, ha centrado más sus esfuerzos en la transformación inteligente de medios físicos ("hardware"); basándose en una sólida base industrial militar, sus exploraciones prospectivas y disposiciones en el campo militar inteligente no deben subestimarse. Israel ha invertido importantes recursos humanos y financieros en la investigación y aplicación militar de la tecnología de IA, y su capacidad en aplicaciones militares de IA ha obtenido un amplio reconocimiento.

Rivalidad China-EE. UU.	11.Geopolitics in the digital age	The intensifying technological competition between the United States and China is reshaping global power dynamics
Rivalidad China-EE. UU.	17.Control de Armamentos de los Sistemas de Armas Autónomas Letales	Potencias como Estados Unidos, Israel, Corea del Sur, Reino Unido y Rusia desarrollan sistemas con altos niveles de autonomía en la selección y ataque de objetivos.
Rivalidad China-EE. UU.	18.Riesgos de Seguridad Internacional y Rutas de Gobernanza	Ejemplos incluyen diálogos entre China y EE.UU. sobre seguridad de la IA.
Rivalidad China-EE. UU.	Nuevas Características y Medidas de Respuesta de la Ciberguerra Electrónica	el despliegue disperso en un amplio espacio geográfico para operaciones independientes en el entorno de fuerte confrontación futuro, y es un concepto operativo diseñado para hacer frente a los principales competidores como China y Rusia, que tendrá un impacto importante en las futuras operaciones de nuestro ejército.
Rivalidad China-EE. UU.	40 Aplicación y desarrollo de la tecnología de inteligencia artificial	En la actualidad, las principales potencias militares del mundo han elevado la IA a una posición estratégica importante a nivel de desarrollo nacional.
Rivalidad China-EE. UU.	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	Entre 2016 y 2021, el ejército estadounidense y los think tanks de defensa impulsaron una serie de estudios como "Squad X", el pelotón de maniobras de operaciones multidominio del ejército de 2028 y el escuadrón de dragones [2].

Rivalidad China-EE. UU.	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	China ha llevado a cabo investigaciones sobre el proyecto "Robot Inteligente Terrestre Militar" durante el "Octavo Plan Quinquenal", y hasta ahora ha experimentado aproximadamente tres etapas de germinación, exploración y madurez.
Rivalidad China-EE. UU.	37 Desarrollo de un Sistema de Concepto Operacional para un Sistema	. China ha llevado a cabo investigaciones sobre el proyecto "Robot Inteligente Terrestre Militar" durante el "Octavo Plan Quinquenal", y hasta ahora ha experimentado aproximadamente tres etapas de germinación, exploración y madurez
Rivalidad China-EE. UU.	20.What do Latin Americans think about the world system	China es un fuerte competidor de Estados Unidos a nivel global pero no lo ha desplazado ni en el mundo ni en América Latina.

4.3 Redes semánticas

4.3.1 Red semántica de la categoría 1: Impacto de la guerra inteligente

La red semántica de la categoría Impacto de la Guerra Inteligente muestra un entramado donde arquitectura de seguridad, autonomía tecnológica, riesgos emergentes, gobernanza tecno-militar, cooperación regional y transformación doctrinaria se entrelazan como partes de un mismo proceso de cambio profundo. La visualización evidencia que la arquitectura de seguridad ocupa una posición estructural, rodeada de múltiples ramificaciones que aluden a vigilancia, coordinación institucional y ciberseguridad, lo que sugiere que los Estados están obligados a reorganizar sus estructuras tradicionales para enfrentar amenazas híbridas y digitales cada vez más complejas. En paralelo, la autonomía tecnológica se presenta como un nodo decisivo, atravesado por ideas de dependencia, desarrollo e independencia, reflejando las tensiones de una región que busca modernizarse, pero que aún se apoya en proveedores externos para tecnologías críticas. En este punto, la red muestra un conflicto entre autonomía y dependencia, lo cual revela uno de los dilemas centrales de la guerra inteligente en América Latina.

Los riesgos emergentes aparecen fuertemente conectados con la autonomía tecnológica, indicando que la dependencia externa aumenta la vulnerabilidad frente a ciberataques, fallas autónomas, desinformación y manipulaciones algorítmicas capaces de afectar infraestructuras esenciales. Esta relación evidencia que los riesgos no surgen solo por la tecnología en sí, sino por las brechas estructurales con las que la región la incorpora. La gobernanza tecno-militar, ubicada entre los nodos principales, funciona como un

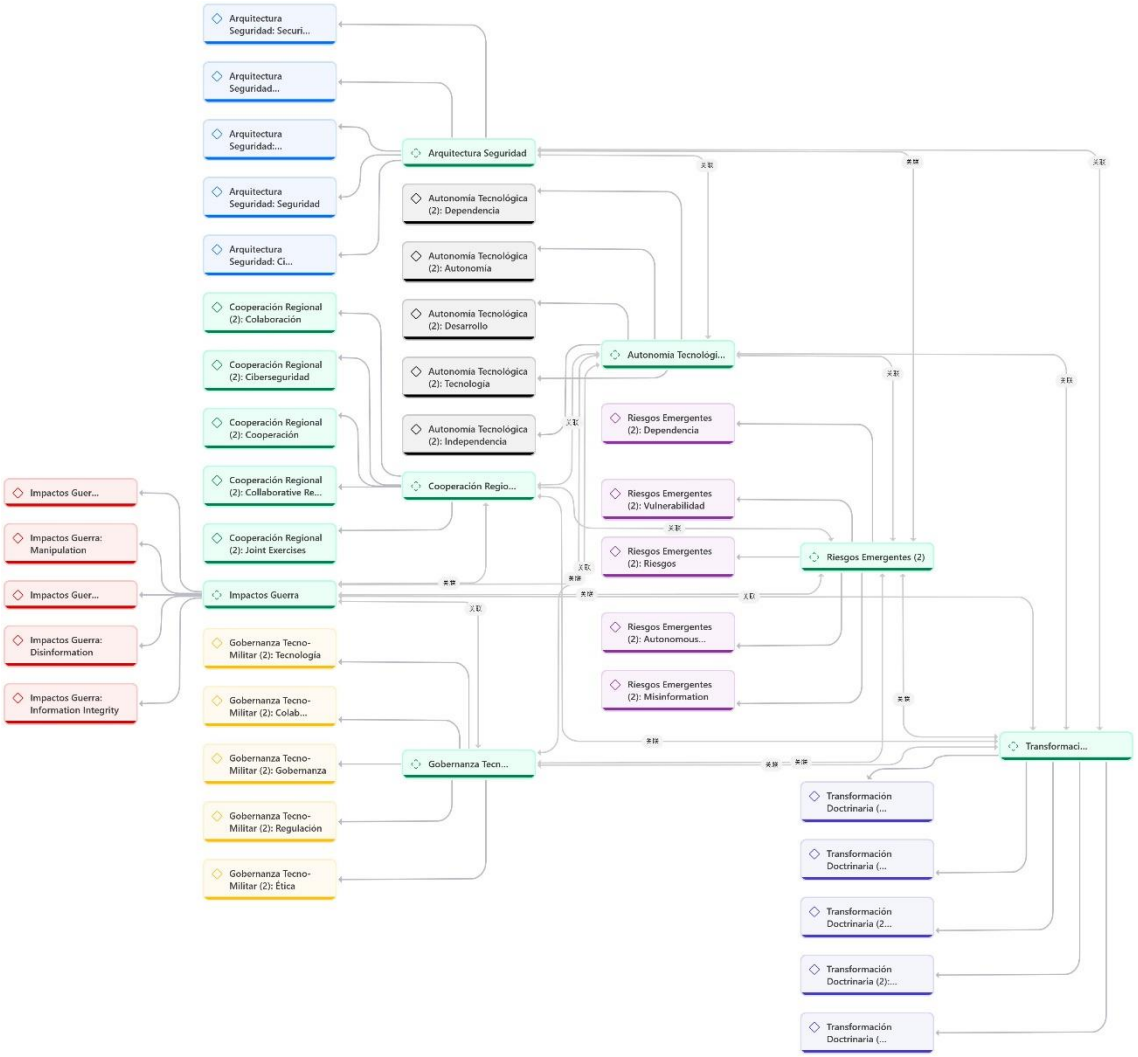
puente que conecta el avance tecnológico con la necesidad de control institucional, regulación, ética y responsabilidad pública. Su posición demuestra que la región no solo enfrenta desafíos técnicos, sino también normativos y políticos, ya que todavía carece de marcos sólidos que regulen el uso militar de la inteligencia artificial o de sistemas autónomos.

Comparativamente, los países latinoamericanos enfrentan la guerra inteligente de manera desigual: Brasil lidera doctrinaria y tecnológicamente con industria militar robusta; Chile destaca por ciberdefensa consolidada y marcos normativos avanzados; Colombia prioriza amenazas híbridas tras experiencias operativas críticas; México avanza de manera fragmentada con capacidades dispersas; Argentina muestra desarrollo técnico moderado pero con limitaciones presupuestarias; y Perú progresa en ciberdefensa, aunque con brechas doctrinarias, dependencia tecnológica y debilidad normativa frente a IA y sistemas autónomos.

Finalmente, la transformación doctrinaria aparece subordinada a los cambios tecnológicos, los riesgos y la gobernanza. La red sugiere que la doctrina militar no está liderando la adaptación, sino respondiendo a presiones externas y a dinámicas tecnológicas que avanzan con mayor rapidez que los ajustes conceptuales. Esto confirma que las fuerzas armadas están revisando sus modelos operativos, pero aún no logran articular un marco doctrinario completamente alineado con el nuevo entorno digital y multidominio.

Figura 1

Red semántica de la categoría: Impacto de la guerra inteligente



Nota. Análisis conceptual-relacional fundamentado en 1659 unidades de significado y siete códigos emergentes, elaborado mediante el proceso de codificación axial.

4.3.2 Red semántica de la categoría 2: Capacidades estatales

La red semántica revela que las capacidades estatales en América Latina funcionan como un eje articulador entre los factores institucionales, tecnológicos y doctrinarios que condicionan la respuesta frente a la guerra inteligente. La presencia simultánea de nodos vinculados a cooperación, seguridad, regulación, gobernanza y adaptación muestra que la preparación estatal no depende únicamente de la disponibilidad de recursos, sino de la capacidad de integrar, coordinar y actualizar estructuras organizacionales que permitan enfrentar amenazas híbridas, cibernéticas y autónomas. Esta interconexión sugiere que los Estados requieren marcos normativos dinámicos, burocracias flexibles y mayor coordinación civil-militar para evitar que los vacíos institucionales amplifiquen vulnerabilidades estratégicas.

En el plano tecnológico, la red evidencia que las capacidades vinculadas a IA militar, sistemas autónomos y ciberseguridad se enlazan de manera directa con los nodos de preparación, resiliencia y adaptación. Esto indica que las tecnologías emergentes no solo transforman las operaciones militares, sino que redefinen las condiciones estructurales de autonomía estratégica, pues la dependencia tecnológica externa incrementa la exposición regional a la competencia entre grandes potencias. La red también sugiere que la brecha tecnológica interna entre países; y dentro de cada país; limita la consolidación de una plataforma regional de defensa capaz de enfrentar amenazas inteligentes con capacidades homogéneas.

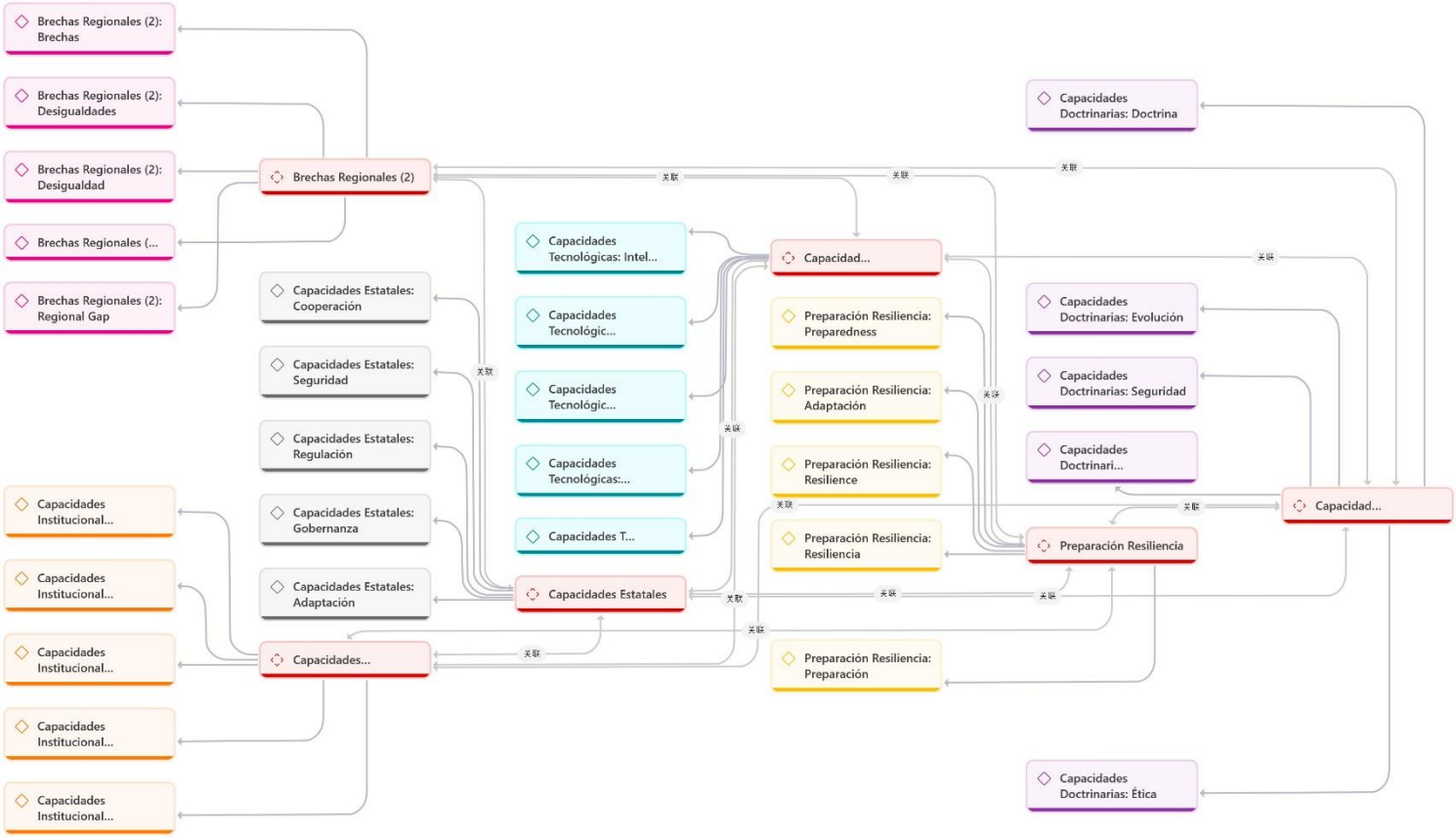
Finalmente, la dimensión doctrinaria aparece vinculada a evolución, seguridad y ética, revelando que la actualización de las doctrinas militares es

insuficiente si no se articula con capacidades institucionales y tecnológicas. La red muestra tensiones entre doctrinas tradicionales basadas en amenazas convencionales y las exigencias de un entorno caracterizado por automatización, toma de decisiones algorítmicas y operaciones cibernéticas. Además, la presencia de nodos normativos y éticos subraya que la región enfrenta vacíos legales críticos respecto al uso de armas autónomas, la responsabilidad en acciones basadas en IA y la gobernanza de datos estratégicos, lo cual condiciona la eficacia y la legitimidad de la defensa en escenarios de guerra inteligente.

Argentina y Chile muestran avances doctrinarios, pero con restricciones tecnológicas y presupuestales; Brasil desarrolla mayor autonomía en IA y ciberdefensa, destacando por capacidades institucionales robustas; Colombia combina modernización tecnológica con cooperación internacional, aunque depende de asistencia externa; México exhibe brechas institucionales y tecnológicas significativas; Perú presenta un desarrollo limitado en IA militar y vacíos normativos. En conjunto, la región evidencia capacidades heterogéneas que dificultan una respuesta cohesionada frente a la guerra inteligente.

Figura 2

Red semántica de la categoría 2: Capacidades estatales



Nota. Análisis conceptual-relacional fundamentado en 2640 unidades de significado y seis códigos emergentes, elaborado mediante el proceso de codificación axial.

4.3.3 Red semántica de la categoría 3: Vacíos de gobernanza

La red semántica evidencia que los vacíos operativos representan la primera línea de fragilidad de los Estados latinoamericanos frente a la guerra inteligente. Los nodos de descoordinación, brechas operativas, ineficiencias, limitaciones e implementación incompleta muestran que las instituciones regionales enfrentan dificultades estructurales para ejecutar estrategias tecnológicas avanzadas. El uso militar de IA, la integración de sistemas autónomos y la defensa cibernética requieren capacidades logísticas, interoperabilidad y sistemas de mando y control actualizados; sin embargo, la red revela un déficit persistente en estos ámbitos, lo que deja a los países expuestos a amenazas rápidas y sofisticadas que superan su capacidad de respuesta inmediata.

En segundo lugar, los vacíos éticos aparecen como un nodo crítico que articula dilemas de responsabilidad humana, supervisión algorítmica y legitimidad del uso de tecnologías inteligentes en operaciones militares. La proliferación de armas autónomas, la toma de decisiones asistida por IA y la vigilancia masiva generan tensiones entre eficiencia militar y respeto a principios éticos universales. Los nodos de consideraciones éticas, omisiones, falta de análisis y ausencia normativa indican que la región carece de marcos de reflexión robustos y comités especializados capaces de evaluar riesgos morales, lo que debilita la gobernanza democrática y agudiza el problema de la rendición de cuentas en acciones militares basadas en IA.

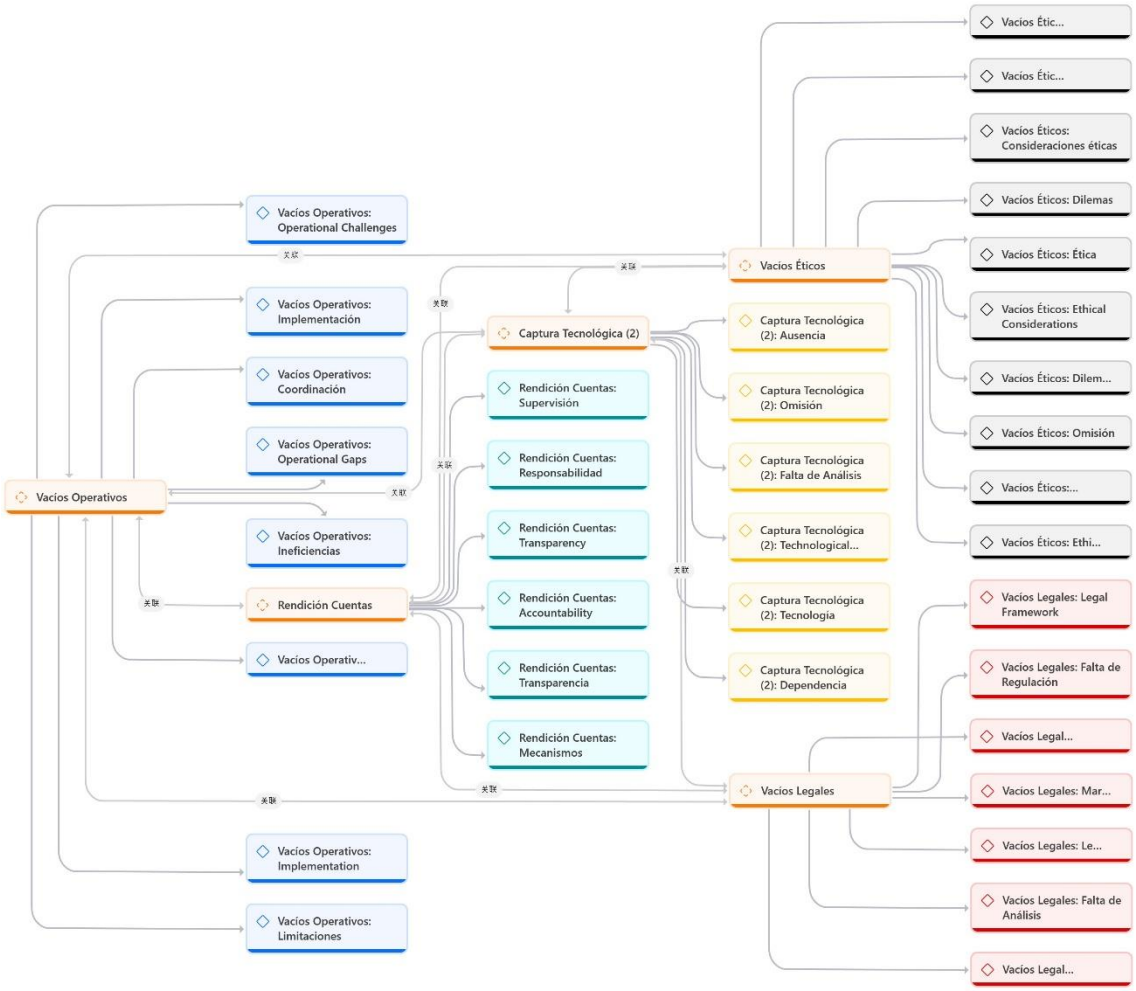
Por lo tanto, los vacíos legales constituyen el eje estructural que vincula la problemática operativa y ética con la gobernanza estratégica regional. La red

muestra que persisten marcos legales incompletos, ausencia de regulación, falta de análisis jurídico y dependencia normativa externa. Esto implica que la región no ha actualizado sus legislaciones para regular IA militar, ciberarmas, responsabilidad por fallos algorítmicos ni evaluación de armas autónomas. La ausencia de reglas claras agrava la dependencia tecnológica de grandes potencias, como Estados Unidos y China, limita la autonomía estratégica y fragmenta las capacidades estatales para actuar de manera coordinada en escenarios de guerra inteligente.

Argentina presenta avances éticos pero limitaciones operativas y legales; Brasil posee mayor desarrollo normativo y capacidades operativas, aunque con dilemas éticos emergentes; Colombia mejora coordinación operativa mediante cooperación internacional, pero depende de marcos externos; Chile exhibe solidez ética y legal, aunque enfrenta brechas operativas; México muestra vacíos estructurales en las tres dimensiones; Perú presenta una débil regulación de IA militar y vacíos operativos persistentes. En conjunto, la región mantiene vacíos heterogéneos y críticos.

Figura 3

Red semántica de la categoría 3: Vacíos de gobernanza



Nota. Análisis conceptual-relacional fundamentado en 4324 unidades de significado y seis códigos emergentes, elaborado mediante el proceso de codificación axial.

4.3.4 Red semántica de la categoría 4: Competencia geoestratégica

La red semántica muestra que la rivalidad geoestratégica entre China y Estados Unidos constituye el eje estructurante que condiciona la inserción de América Latina en la guerra inteligente. Los nodos asociados a seguridad, tecnología, cooperación, competencia e influencia evidencian que la región queda atrapada en una disputa por el control de infraestructuras críticas, cadenas de suministro digitales, plataformas de IA y sistemas de vigilancia estratégica. Esta rivalidad redefine la arquitectura hemisférica al trasladar la competencia tecnológica al espacio militar latinoamericano, incrementando la dependencia de proveedores externos y limitando la capacidad de los Estados para construir autonomía estratégica.

En el centro de la red, la subcategoría de respuestas regionales demuestra que América Latina enfrenta la guerra inteligente de manera fragmentada. Los nodos vinculados a ciberseguridad, gobernanza, regulación, cooperación y estrategias revelan que existe una asimetría marcada entre países, con iniciativas aisladas y sin una agenda de defensa regional articulada. La falta de coordinación limita la capacidad para enfrentar amenazas híbridas transnacionales; como ciberataques, desinformación y espionaje digital; que requieren respuestas conjuntas más allá de las capacidades individuales. La red evidencia un déficit estructural: la región no posee mecanismos sostenidos para el desarrollo conjunto de IA militar ni para la producción regional de sistemas autónomos de defensa.

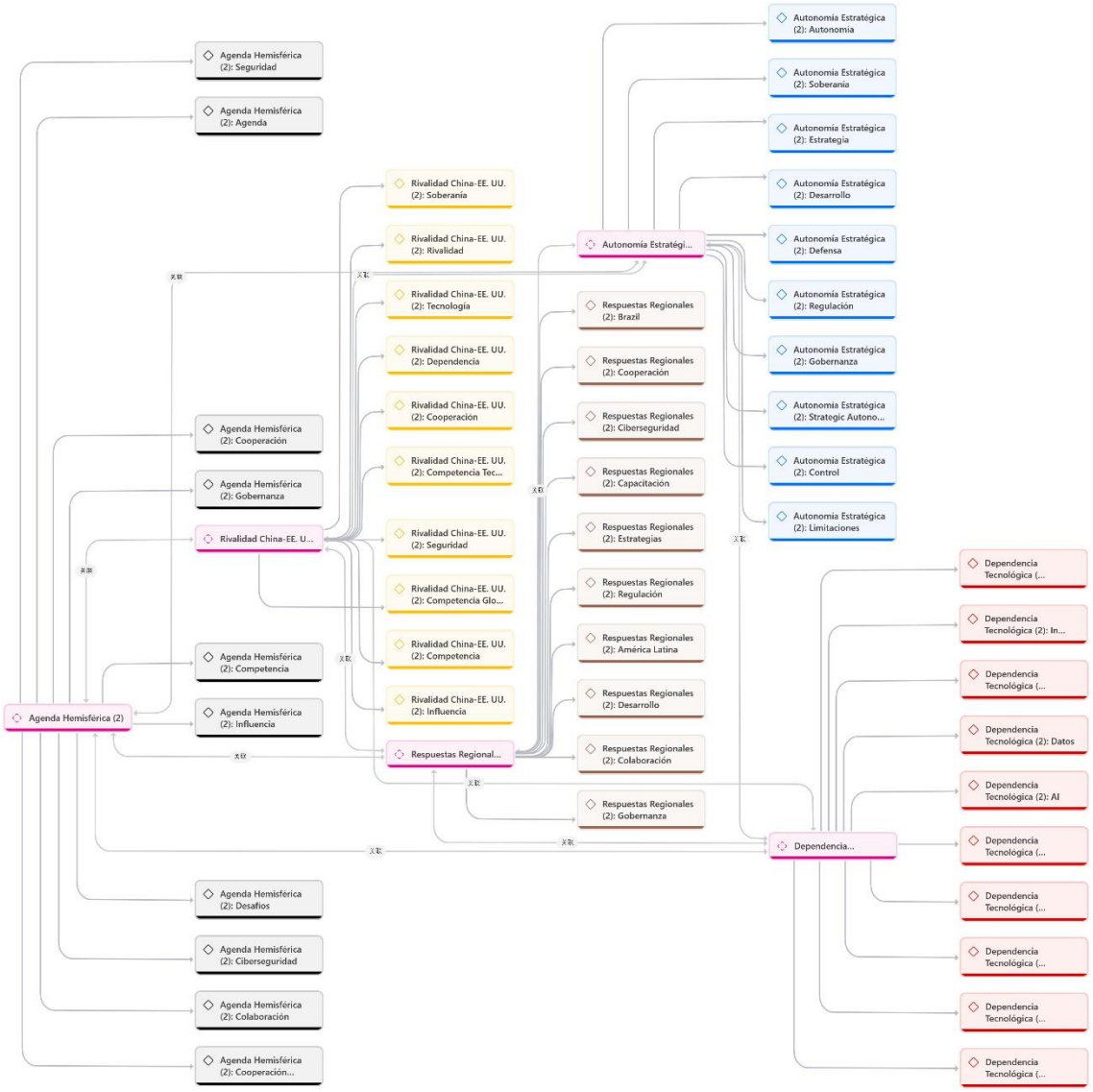
La dimensión de autonomía estratégica se alinea con el conjunto de nodos que apuntan a soberanía, regulación, estrategia, control y desarrollo. La red

muestra que la autonomía latinoamericana depende de tres factores críticos: (1) reducir la dependencia tecnológica de grandes potencias, (2) fortalecer capacidades nacionales de innovación en defensa inteligente, y (3) desarrollar estrategias regulatorias que protejan la soberanía digital. Sin embargo, la presencia dominante de nodos relacionados con dependencia tecnológica (IA, datos, infraestructura, software y capacidades operativas) evidencia profundas vulnerabilidades. La región importa tecnología sensible sin mecanismos robustos de supervisión ni capacidad para auditar sistemas autónomos, lo cual condiciona su toma de decisiones estratégicas y aumenta la subordinación geopolítica.

Argentina enfrenta limitaciones tecnológicas y dependencia externa, pese a esfuerzos por diversificar alianzas; Brasil exhibe la mayor autonomía estratégica regional y capacidad para negociar con EE.UU. y China; Colombia mantiene alineamiento hemisférico con Estados Unidos; Chile combina estabilidad institucional con dependencia tecnológica avanzada; México muestra vulnerabilidades por baja inversión en defensa inteligente; Perú presenta brechas estratégicas y alta dependencia de proveedores externos. En conjunto, la región refleja respuestas geopolíticas dispares y capacidad limitada para construir autonomía estratégica.

Figura 4

Red semántica de la categoría 4: Competencia geoestratégica



Nota. Análisis conceptual-relacional fundamentado en 946 unidades de significado y cinco códigos emergentes, elaborado mediante el proceso de codificación axial

4.3.5 Análisis de coocurrencias

El análisis de coocurrencia es una técnica utilizada en la investigación cualitativa para identificar y analizar las relaciones entre diferentes códigos o categorías dentro de un conjunto de datos (Mardones y García, 2024). Este método ayuda a los investigadores a descubrir patrones e interrelaciones semánticas en los datos, proporcionando una comprensión más profunda de los fenómenos estudiados (Sha y Clarke, 2025).

Los análisis de coocurrencias permiten identificar los patrones de asociación más relevantes entre las subcategorías que estructuran la comprensión regional de la guerra inteligente. A través de estos vínculos se revelan jerarquías, tensiones y núcleos temáticos que no son visibles mediante una lectura aislada de los datos, aportando una visión sistémica sobre cómo se articulan los impactos, capacidades, vacíos y dinámicas geopolíticas en el contexto latinoamericano.

La lectura integrada de estas coocurrencias proporciona una base empírica sólida para interpretar la magnitud de la transformación que la guerra inteligente está generando en los marcos de seguridad y defensa. Cada matriz evidencia relaciones estructurales que permiten comprender la profundidad de los desafíos en materia tecnológica, institucional, normativa y estratégica, ofreciendo insumos esenciales para el análisis comparado y para la formulación de conclusiones en torno a la autonomía y vulnerabilidad de la región.

4.3.5.1 Análisis de coocurrencias asociada a la categoría 1: Impacto de la Guerra Inteligente

La matriz de coocurrencias muestra que “Impactos Guerra” es el núcleo estructurante del mapa semántico: concentra la mayor suma de coocurrencias y se asocia con la arquitectura de seguridad, los riesgos emergentes, la gobernanza tecno-militar y la transformación doctrinaria. El par “Arquitectura de seguridad–Impactos guerra” y “Impactos guerra–Riesgos emergentes” registra los valores más altos, lo que indica que los entrevistados interpretan la guerra inteligente, ante todo, como un fenómeno que reconfigura la arquitectura de defensa y genera nuevos riesgos sistémicos. La fuerte coocurrencia con “Transformación doctrinaria” y “Gobernanza tecno-militar” sugiere que los cambios doctrinarios no son abstractos: aparecen anclados en impactos concretos sobre mandos, estructuras, reglas de empleo de la fuerza y toma de decisiones apoyada en IA. En contraste, “Autonomía tecnológica” y “Cooperación regional” ocupan posiciones más periféricas, lo que revela que, en el discurso experto, la prioridad todavía está en ajustar dispositivos internos de seguridad antes que en construir respuestas regionales o agendas robustas de soberanía tecnológica.

En Argentina, la guerra inteligente se discute más en términos de impactos sobre la arquitectura de seguridad que como doctrina consolidada; Brasil articula efectos operacionales con inversiones en IA y ciberdefensa; Colombia vincula impactos con cooperación militar estadounidense; Chile los conecta con reformas normativas y gestión de riesgos; México muestra impactos dispersos y capacidades fragmentadas; Perú asocia fuertemente impactos y

riesgos emergentes crecientes y persistentes. Las coocurrencias reflejan una región predominantemente reactiva, donde los efectos preceden a la planificación estratégica.

Figura 5

Matriz de coocurrencias de Atlas.Ti 25 asociada a la categoría 1: Impacto de la Guerra Inteligente

	● Arquitectura Seguridad Gr=234	● Autonomía Tecnológica (2) Gr=135	● Cooperación Regional (2) Gr=179	● Gobernanza Tecno-Militar (2) Gr=236	● Impactos Guerra Gr=426	● Riesgos Emergentes (2) Gr=232	● Transformación Doctrinaria (2) Gr=217
● Arquitectura Seguridad Gr=234	0	110	92	159	210	158	190
● Autonomía Tecnológica (2) Gr=135	110	0	73	111	113	109	111
● Cooperación Regional (2) Gr=179	92	73	0	84	97	82	85
● Gobernanza Tecno-Militar (2) Gr=236	159	111	84	0	161	143	160
● Impactos Guerra Gr=426	210	113	97	161	0	210	193
● Riesgos Emergentes (2) Gr=232	158	109	82	143	210	0	146
● Transformación Doctrinaria (2) Gr=217	190	111	85	160	193	146	0

4.3.5.2 Análisis de coocurrencias asociada a la categoría 2: Capacidades estatales

En la matriz de la categoría 2, los grandes *hubs* son Capacidades estatales y Capacidades institucionales, fuertemente coocurrentes entre sí y con las capacidades doctrinarias y tecnológicas. El vínculo más intenso es “Capacidades estatales–Capacidades institucionales”, seguido de las parejas “Capacidades doctrinarias–Capacidades institucionales” y “Capacidades

estatales–Capacidades tecnológicas", lo que indica que los entrevistados conciben la respuesta a la guerra inteligente como un entramado institucional-doctrinario-tecnológico integrado. La preparación y resiliencia aparece densamente conectada con estos cuatro nodos, mostrando que la resiliencia no se entiende solo como gestión de desastres, sino como resultado de la sincronización entre doctrina, tecnología y aparato estatal. "Brechas regionales" coocurre menos, pero funciona como recordatorio permanente de las desigualdades intra e inter-países: allí donde las capacidades institucionales y tecnológicas son débiles, la preparación y resiliencia se erosionan. En conjunto, la matriz muestra un diagnóstico claro: sin reforma institucional, actualización doctrinaria y políticas tecnológicas coherentes, la guerra inteligente desnuda las limitaciones estructurales de los Estados latinoamericanos.

En Argentina, las capacidades institucionales y doctrinarias evolucionan lentamente, con limitadas inversiones tecnológicas; Brasil articula capacidades estatales robustas con desarrollo de industria de defensa inteligente; Colombia depende fuertemente de cooperación y asistencia externas; Chile combina instituciones sólidas y tecnología intermedia, priorizando regulación; México presenta capacidades estatales dispersas y baja resiliencia; Perú evidencia instituciones frágiles y brechas tecnológicas significativas. Las coocurrencias muestran que la resiliencia regional depende de cómo cada país sincroniza doctrina, instituciones y tecnología frente a la guerra inteligente.

Figura 6

Matriz de coocurrencias de Atlas.Ti 25 asociada a la categoría 2: Capacidades estatales

	● Brechas Regionales (2) Gr=238	● Capacidades Doctrinarias Gr=417	● Capacidades Estatales Gr=591	● Capacidades Institucionales Gr=560	● Capacidades Tecnológicas Gr=540	● Preparación Resiliencia Gr=294
● **Brechas Regionales (2)** Gr=238	0	156	198	197	175	124
● **Capacidades Doctrinarias** Gr=417	156	0	398	406	289	255
● **Capacidades Estatales** Gr=591	198	398	0	525	394	282
● **Capacidades Institucionales** Gr=560	197	406	525	0	377	284
● **Capacidades Tecnológicas** Gr=540	175	289	394	377	0	230
● **Preparación Resiliencia** Gr=294	124	255	282	284	230	0

4.3.5.3 Análisis de coocurrencias asociada a la categoría 3: Vacíos de gobernanza

En la categoría 3, la matriz evidencia un bloque de vacíos fuertemente interdependientes. Los nodos de vacíos legales y vacíos operativos presentan las mayores coocurrencias, seguidos muy de cerca por vacíos éticos y rendición de cuentas. El par “Vacíos legales–Vacíos operativos” es el más intenso, lo que sugiere que la ausencia o debilidad normativa se traduce directamente en deficiencias de implementación, coordinación y control en el uso de tecnologías inteligentes. La alta coocurrencia de “Vacíos éticos” con “Vacíos legales” y “Vacíos operativos” indica que los dilemas morales no se abordan de forma sistemática, quedando subsumidos en sistemas institucionales incapaces de

supervisar algoritmos, responsabilizar a actores y garantizar proporcionalidad en el empleo de IA militar. “Rendición de cuentas” aparece como bisagra entre ética, legalidad y operación, revelando que la falta de *accountability* agrava todos los demás vacíos. Finalmente, “Captura tecnológica” se asocia fuertemente con los cuatro núcleos, mostrando el riesgo de que proveedores privados o potencias externas impongan soluciones tecnológicas opacas, aprovechando lagunas legales y debilidades operativas.

En Argentina persisten vacíos legales y éticos sobre IA militar, pese a ciertos mecanismos de control; Brasil ha desarrollado marcos más avanzados, aunque enfrenta riesgos de captura tecnológica; Colombia exhibe fuerte dependencia normativa de socios externos; Chile presenta mejor alineamiento entre legalidad, ética y operación, con brechas moderadas; México reúne graves deficiencias operativas y de rendición de cuentas; Perú combina vacíos legales, operativos y éticos. Las coocurrencias revelan déficits estructurales compartidos que debilitan la gobernanza regional de la guerra inteligente.

Figura 7

Matriz de coocurrencias de Atlas.Ti 25 asociada a la categoría 3: Vacíos de gobernanza

	● Captura Tecnológica (2) Gr=755	● Rendición Cuentas Gr=786	● Vacíos Éticos Gr=790	● Vacíos Legales Gr=1024	● Vacíos Operativos Gr=969
● Captura Tecnológica (2) Gr=755	0	685	676	743	742
● Rendición Cuentas Gr=786	685	0	748	782	776
● Vacíos Éticos Gr=790	676	748	0	789	784
● Vacíos Legales Gr=1024	743	782	789	0	962
● Vacíos Operativos Gr=969	742	776	784	962	0

4.3.5.4 Análisis de coocurrencias asociada a la categoría 4: Competencia geoestratégica

La matriz de la categoría 4 muestra un entramado geopolítico donde Autonomía estratégica, Dependencia tecnológica, Rivalidad China–EE.UU., Respuestas regionales y Agenda hemisférica tienen pesos semejantes, pero roles diferenciados. El lazo más fuerte es “Autonomía estratégica–Dependencia tecnológica”: la autonomía aparece definida negativamente, como capacidad de reducir dependencias en datos, infraestructura e IA de grandes potencias. Casi al mismo nivel se sitúa el par “Dependencia tecnológica–Rivalidad China–EE.UU.”, lo que indica que la competencia entre ambas potencias se materializa en la provisión de tecnologías críticas para defensa, ciberseguridad y vigilancia. “Agenda hemisférica–Respuestas regionales” registra coocurrencias muy altas,

mostrando que buena parte de la agenda latinoamericana se estructura en diálogo o tensión con las prioridades de seguridad definidas desde Washington. La conexión simultánea de “Autonomía estratégica” con “Respuestas regionales” y “Rivalidad China–EE.UU.” evidencia que la región busca márgenes de maniobra, pero lo hace desde posiciones asimétricas y fragmentadas, sin una estrategia latinoamericana común frente a la guerra inteligente.

Argentina oscila entre vínculos con China, Europa y Estados Unidos, buscando equilibrios prudentes; Brasil aprovecha su peso regional para negociar márgenes de autonomía estratégica; Colombia mantiene alineamiento predominante con la agenda de seguridad estadounidense; Chile combina apertura comercial con cautela estratégica; México enfrenta presión geopolítica directa de Estados Unidos; Perú muestra alta dependencia tecnológica externa y respuestas reactivas. Las coocurrencias evidencian una autonomía regional limitada, condicionada por rivalidades globales, inercias históricas y por la falta de una estrategia latinoamericana concertada.

Figura 8

Matriz de coocurrencias de Atlas.Ti 25 asociada a la categoría 4: Competencia geoestratégica

	● Agenda Hemisférica (2) Gr=153	● Autonomía Estratégica (2) Gr=183	● Dependencia Tecnológica (2) Gr=203	● Respuestas Regionales (2) Gr=211	● Rivalidad China-EE. UU. (2) Gr=196
● Agenda Hemisférica (2) Gr=153	0	88	68	115	87
● Autonomía Estratégica (2) Gr=183	88	0	120	101	112
● Dependencia Tecnológica (2) Gr=203	68	120	0	88	115
● Respuestas Regionales (2) Gr=211	115	101	88	0	81
● Rivalidad China-EE. UU. (2) Gr=196	87	112	115	81	0

4.4 Triangulación

4.4.1 Triangulación de resultados de entrevistas semiestructuradas

La guerra inteligente, marcada por la IA militar, los sistemas autónomos y las ciberestrategias, está transformando los marcos de defensa en América Latina. Para comprender este proceso, las entrevistas ofrecen insumos clave que permiten observar cambios doctrinarios, tecnológicos y geopolíticos desde la experiencia de especialistas del sector.

La triangulación de las entrevistas resulta necesaria para identificar patrones comunes, contrastar perspectivas y reconocer brechas en capacidades estatales, gobernanza tecno-militar y autonomía tecnológica. Este procedimiento permite articular un análisis más sólido que trasciende las opiniones individuales y configura una visión comparada del fenómeno regional.

A través de este análisis se evalúan también los vacíos normativos, los riesgos de dependencia tecnológica y el impacto de la competencia estratégica entre China y Estados Unidos. La triangulación, en ese sentido, contribuye a integrar estas dimensiones y a construir un diagnóstico coherente con la complejidad de la guerra inteligente en América Latina.

A partir de las entrevistas analizadas, se observa que los países latinoamericanos enfrentan la guerra inteligente con ritmos y énfasis claramente diferenciados. Brasil aparece como el actor más avanzado, con una industria militar propia, inversiones sostenidas en ciberdefensa y proyectos de IA y sistemas autónomos que le otorgan liderazgo regional. Chile también destaca por su infraestructura digital, la profesionalización de sus centros de ciberseguridad y el fortalecimiento doctrinario orientado a operaciones

multidominio. Colombia, impulsada por la presión del conflicto interno y del crimen organizado, desarrolla capacidades crecientes en ciberinteligencia y combate híbrido, aunque con vulnerabilidades aún visibles. Argentina muestra avances irregulares, ligados a cambios políticos, pero mantiene una base científico-tecnológica importante que impulsa iniciativas en innovación aplicada a defensa. México, aunque con una estructura estatal robusta, concentra su esfuerzo en seguridad interior y enfrenta desafíos para consolidar una doctrina integral de guerra inteligente frente al poder del crimen organizado. Perú, por su parte, ha avanzado en la creación de comandos de ciberdefensa y marcos legales recientes, pero sigue limitado por la dependencia tecnológica externa, presupuestos rígidos y una industria militar incipiente.

En conjunto, la región muestra una brecha evidente: mientras Brasil y Chile consolidan capacidades maduras, países como Perú, México y Argentina avanzan de forma fragmentada, y Colombia se adapta bajo presión, evidenciando que la guerra inteligente profundiza desigualdades doctrinarias, tecnológicas, normativas y geoestratégicas en América Latina.

Tabla 10

Triangulación de resultados de entrevistas semiestructuradas por categoría

Entrevistado	Categorías de Análisis				Síntesis integradora
	Impacto de la guerra inteligente	**Capacidades estatales**	**Vacíos de gobernanza**	**Competencia geoestratégica**	
CRL EP Edgar Concha Loaiza	La guerra inteligente redefine doctrinas y capacidades latinoamericanas mediante ciberdefensa, IA emergente y cooperación regional impulsada por la JID.	Las capacidades estatales avanzan lentamente, limitadas por presupuestos rígidos, débil industria militar y amenazas híbridas crecientes del crimen organizado.	Persisten vacíos legales y éticos en IA militar, dificultando control, estandarización operativa y responsabilidad frente a decisiones algorítmicas.	La rivalidad China–Estados Unidos condiciona elecciones tecnológicas latinoamericanas, generando presiones estratégicas y dilemas de alineamiento futuro.	El coronel Concha describe una región que avanza en ciberdefensa y cooperación vía la JID, pero sin guía doctrinaria unificada ni presupuestos robustos para IA. Identifica como amenaza central al crimen organizado transnacional, denuncia vacíos legales específicos para el empleo militar de IA y advierte que la competencia China–Estados Unidos empuja a

					Latinoamérica hacia decisiones tecnológicas pragmáticas que condicionarán su autonomía estratégica.
GRAL EP Dr. Ernesto Castillo Fuerman	La guerra inteligente transforma doctrina y operaciones mediante simulación avanzada, IA táctica, ciberataques y redefinición total del entorno operacional.	Las capacidades regionales siguen siendo incipientes, evidenciadas por ataques como “Guacamaya” y la escasa cooperación estructurada en ciberdefensa.	Las normas sobre IA militar y ciberdefensa son incompletas, generando confusiones institucionales y retrasos significativos en regulación operativa.	La competencia China–Estados Unidos presiona decisiones tecnológicas, revelando heterogeneidad regional e impacto directo sobre la autonomía estratégica.	Castillo muestra cómo la guerra inteligente transforma la doctrina mediante simulación táctica con IA y evidencia vulnerabilidades regionales a partir de ciberataques como “Guacamaya”. Señala capacidades aún incipientes, marcos legales incompletos y una gobernanza que se retrasa frente a la velocidad tecnológica, mientras la rivalidad China–Estados Unidos y la protección

					de la soberanía digital redefinen las prioridades estratégicas latinoamericanas hacia 2030.
GRAL EP Hugo Vega Castro	La guerra inteligente redefine poder estatal incorporando IA, ciberespacio y operaciones multidominio como eje central de seguridad regional.	Existen avances desiguales, con brechas estructurales marcadas entre países y limitada inversión en investigación y desarrollo militar.	La región carece de regulaciones claras sobre armas autónomas e IA, generando incertidumbre ética y jurídica significativa.	China expande su influencia mediante cooperación tecnológica, mientras Estados Unidos mantiene predominio militar, fragmentando respuestas latinoamericanas.	Vega concibe la guerra inteligente como un cambio de era, donde el poder se mide por control del ciberespacio, datos y algoritmos. Reconoce capacidades estatales bajas a medias, grandes asimetrías regionales y falta de regulación sobre IA y armas autónomas, mientras China expande su “poder blanco” y Estados Unidos conserva influencia militar, obligando a América

					Latina a replantear soberanía tecnológica y formación de talento especializado.
CRL EP Julio Sebastian Cassareto	La región adopta lentamente ciberdefensa e IA, con estructuras incipientes y cooperación limitada por fuertes divergencias políticas.	Las capacidades varían drásticamente: Brasil lidera, mientras países con menos recursos mantienen vulnerabilidades críticas frente a amenazas híbridas.	La ausencia de normas regionales y la dependencia tecnológica debilitan estándares, protocolos y soberanía defensiva latinoamericana.	La rivalidad China–Estados Unidos acentúa fracturas políticas regionales, dificultando agendas comunes y reduciendo posibilidades de autonomía estratégica.	Cassareto subraya que, pese a la creación de comandos de ciberdefensa y apoyos de países como Brasil, la región sigue fragmentada políticamente, con capacidades muy desiguales y fuerte dependencia tecnológica externa. La ausencia de gobernanza regional efectiva y la competencia China–Estados Unidos dificultan construir una agenda hemisférica propia,

					haciendo del conocimiento, la capacitación y el desarrollo de tecnología propia el principal desafío estratégico hacia 2030.
Síntesis interpretativa global	Las entrevistas evidencian que la guerra inteligente reconfigura doctrinas, capacidades y arquitecturas de seguridad, profundiza vacíos normativos, incrementa la dependencia tecnológica y, bajo la rivalidad China–Estados Unidos, tensiona la autonomía estratégica latinoamericana y su resiliencia frente a amenazas híbridas.				

4.4.2 Triangulación de resultados del análisis documental por categoría

La revisión documental realizada integra un conjunto de estudios estratégicos, doctrinarios, geopolíticos, éticos y normativos que permiten comprender cómo la guerra inteligente, basada en inteligencia artificial, sistemas autónomos, ciberestrategias y nuevas arquitecturas de control, está reconfigurando los marcos de seguridad y defensa en América Latina. Los documentos analizados, que abarcan desde evaluaciones sobre integridad de la información y gobernanza de la IA hasta investigaciones sobre guerra cognitiva, sistemas de armas autónomas, cooperación internacional y cultura estratégica, ofrecen un panorama multidimensional sobre las transformaciones tecnológicas que afectan el entorno hemisférico.

En conjunto, estas fuentes permiten identificar patrones convergentes respecto a las capacidades institucionales, doctrinarias y tecnológicas de los Estados latinoamericanos, así como divergencias en materia de preparación, resiliencia y adaptación estratégica frente a amenazas emergentes. Además, revelan los vacíos normativos, éticos y operativos que caracterizan a la región ante la proliferación de tecnologías disruptivas, desde la automatización letal hasta la guerra cognitiva y los riesgos asociados a la desinformación, evidenciando la asimetría entre los avances tecnológicos globales y la respuesta estatal regional.

Por lo tanto, los documentos ofrecen claves para comprender el papel de la competencia geoestratégica entre grandes potencias, especialmente China, Estados Unidos y Rusia, en la configuración de la gobernanza de la guerra inteligente en América Latina. Esta dinámica influye tanto en los modelos de cooperación, como en las tensiones en torno a la autonomía tecnológica, la

dependencia estratégica y las oportunidades de integración regional. Sobre esta base, la triangulación documental permitirá sintetizar los principales aportes, tensiones y regularidades que emergen del corpus analizado, estableciendo un marco sólido para la interpretación de los resultados en relación con las preguntas de investigación planteadas.

Desde una perspectiva comparativa, los documentos también permiten identificar cómo Argentina, Brasil, Colombia, Chile, México y Perú enfrentan la guerra inteligente desde enfoques doctrinarios, tecnológicos, normativos y geoestratégicos diferenciados. Brasil aparece como el actor con mayor proyección tecnológica y doctrinaria, impulsado por su industria de defensa y su visión de autonomía estratégica; Chile y Colombia destacan en modernización doctrinaria y capacidades cibernéticas, aunque con limitaciones industriales; México avanza en marcos normativos y cooperación internacional, pero mantiene rezagos operativos; mientras que Argentina y Perú evidencian importantes brechas tecnológicas y regulatorias pese a esfuerzos recientes de actualización institucional. Esta heterogeneidad revela que la región no enfrenta un proceso uniforme, sino un mosaico de capacidades y prioridades que condiciona la posibilidad de construir respuestas regionales coherentes ante la evolución de la guerra inteligente.

Tabla 11

Triangulación de resultados del análisis documental por categoría

Documento	Categorías de Análisis				Síntesis integradora
	Impacto de la guerra inteligente	**Capacidades estatales**	**Vacíos de gobernanza**	**Competencia geoestratégica**	
Artificial Intelligence and Information Integrity	El documento muestra cómo la desinformación algorítmica erosiona infraestructuras críticas, altera percepciones estratégicas y reconfigura la guerra inteligente.	Evidencia capacidades estatales desiguales para monitorear plataformas digitales, coordinar agencias y proteger procesos electorales ante campañas coordinadas.	Identifica vacíos de gobernanza en regulación de contenidos, responsabilidad de plataformas y transparencia algorítmica frente a operaciones de influencia hostil.	Subraya cómo potencias globales utilizan ecosistemas informativos y plataformas digitales para disputar narrativas estratégicas dentro de sociedades latinoamericanas.	El documento muestra cómo la manipulación algorítmica y las campañas de desinformación reconfiguran la guerra inteligente, tensionando capacidades estatales para proteger procesos democráticos. Los vacíos regulatorios sobre plataformas y contenidos favorecen operaciones de influencia hostil en un contexto de competencia geoestratégica por el

					control del espacio informativo.
América Latina en el nuevo escenario internacional	Analiza cómo la guerra inteligente reconfigura correlaciones de poder, vulnerabilidades regionales y márgenes de maniobra de América Latina.	Describe capacidades estatales dispares para adaptar doctrinas, modernizar fuerzas armadas y construir instituciones especializadas en ciberdefensa y seguridad digital.	Señala vacíos normativos y éticos frente a nuevas tecnologías militares, particularmente en ciberoperaciones y vigilancia masiva de poblaciones.	Discute cómo la rivalidad entre potencias introduce presiones contradictorias sobre alianzas, compras militares y posicionamiento diplomático latinoamericano.	Se describe una región atravesada por la guerra inteligente, con impactos profundos en sus arquitecturas de seguridad y márgenes de maniobra. Las capacidades estatales son desiguales y los marcos normativos incompletos, mientras la rivalidad entre potencias condiciona alianzas, compras militares y agendas diplomáticas latinoamericanas.
Understanding the Strategic Implications of the Weaponization of Artificial	Explora cómo la militarización de la inteligencia artificial transforma ciclos de	Evalúa capacidades estatales para integrar algoritmos en mando	Advierte vacíos regulatorios sobre responsabilidad por decisiones algorítmica	Discute cómo la carrera por armas basadas en IA intensifica competenc	El texto muestra que la militarización de la IA transforma doctrinas, escalamien

Intelligence	decisión, letalidad, escalamiento y disuasión en conflictos contemporáneos.	y control, inteligencia operativa y sistemas autónomos de apoyo al combate.	s, transparencia técnica y control humano significativo en contextos bélicos.	ia geoestratégica y multiplica riesgos de inestabilidad sistémica.	to y disuasión, exigiendo nuevas capacidades estatales de integración tecnológica. Los marcos jurídicos y éticos resultan insuficientes ante decisiones algorítmicas letales, en un escenario donde la carrera armamentista basada en IA incrementa riesgos geoestratégicos globales.
AI y políticas públicas en América Latina y el Caribe	Muestra cómo la expansión de IA en políticas públicas permea seguridad ciudadana, defensa, vigilancia y gestión de infraestructuras estratégicas.	Analiza capacidades estatales para diseñar estrategias nacionales de IA, coordinando ministerios, agencias de ciberseguridad y sectores	Identifica vacíos de gobernanza sobre uso de datos, supervisión algorítmica y protección de derechos fundamentales frente a tecnologías inteligentes.	Sugiere que la cooperación y asistencia internacional condicionan agendas nacionales de IA, afectando márgenes de autonomía estratégica regional.	El documento evidencia cómo la expansión de la IA en políticas públicas permea seguridad, defensa y gestión de infraestructuras críticas. Las capacidades estatales para

		de defensa.			gobernar estos procesos son incipientes y fragmentadas, con vacíos de protección de derechos, en un contexto de cooperación internacional que condiciona autonomía estratégica.
Latin American hemispheric security adapted	Relaciona la guerra inteligente con la adaptación de arquitecturas hemisféricas de seguridad, incorporando amenazas cibernéticas, híbridas e informacionales.	Describe capacidades diferenciadas entre Estados para participar en mecanismos hemisféricos, compartir inteligencia y desarrollar ejercicios conjuntos de ciberdefensa.	Señala vacíos de gobernanza regional respecto a normas comunes sobre ciberoperaciones, armas autónomas y protección de infraestructuras críticas transnacionales.	Analiza cómo la agenda hemisférica se ve tensionada por agendas de Estados Unidos, potencias extrahemisféricas y demandas de autonomía latinoamericana.	Se analiza la adaptación de la seguridad hemisférica ante amenazas híbridas y cibernéticas asociadas a la guerra inteligente. Las capacidades estatales para participar en esquemas de inteligencia y ciberdefensa son heterogéneas; los marcos regionales

					de gobernanza resultan incompletos y tensionados por la influencia de Estados Unidos y actores extrahemisféricos.
Artificial intelligence governance challenges	Aborda cómo la expansión de sistemas inteligentes introduce nuevas superficies de riesgo para seguridad nacional, ciberdefensa y estabilidad institucional.	Examina capacidades estatales para regular, auditar y supervisar sistemas de IA empleados en defensa, vigilancia y gestión de crisis.	Destaca vacíos de gobernanza en marcos legales, estructuras regulatorias y mecanismos de control democrático sobre tecnologías de alto impacto.	Sugiere que la fragmentación regulatoria global profundiza asimetrías entre potencias tecnológicas y países periféricos, incluyendo América Latina.	El texto expone cómo la incorporación masiva de sistemas inteligentes introduce nuevos riesgos para la seguridad nacional, demandando instituciones capaces de regular, auditar y supervisar la IA. Persisten vacíos legales y de control democrático, mientras la fragmentación regulatoria global refuerza asimetrías entre potencias

					tecnológicas y países dependientes.
Updating cognitive security in a global dimension	Plantea que la guerra inteligente amplía el campo cognitivo del conflicto, afectando percepciones, emociones colectivas y toma de decisiones estratégicas.	Analiza capacidades estatales para desarrollar doctrinas de seguridad cognitiva, combinando ciberdefensa, comunicación estratégica y resiliencia social.	Señala vacíos éticos y operativos respecto al uso de técnicas de manipulación psicológica apoyadas en datos masivos y algoritmos predictivos.	Discute cómo actores estatales y no estatales compiten globalmente por influir ecosistemas informativos, afectando márgenes de autonomía regional.	Aquí la guerra inteligente aparece centrada en la dimensión cognitiva, donde percepciones y decisiones estratégicas son blanco de operaciones algorítmicas. Las capacidades estatales para articular seguridad cognitiva son limitadas, con serios vacíos éticos, mientras actores globales compiten por influir ecosistemas informativos que afectan directamente a regiones periféricas.

Russia´s cooperation with the Latin American	Describe cómo la cooperación militar rusa introduce tecnologías avanzadas, entrenamiento y doctrinas asociadas a guerra informacional y capacidades cibernéticas.	Analiza capacidades estatales latinoamericanas para absorber asistencia rusa, integrarla en estructuras de defensa y manejar dependencias tecnológicas resultantes.	Advierte vacíos de gobernanza sobre transparencia, control parlamentario y alineamiento con normas internacionales en acuerdos de cooperación militar tecnológica.	Interpreta la cooperación rusa como instrumento de competencia geoestratégica, diversificación de alianzas y ampliación de márgenes frente a Estados Unidos.	El documento muestra que la cooperación militar rusa introduce tecnologías y doctrinas asociadas a guerra informacional y capacidades cibernéticas, ampliando capacidades estatales de algunos países. Sin embargo, persisten opacidades y debilidades de control civil, mientras esta cooperación se inscribe en la competencia geoestratégica con Estados Unidos en la región.
Sistemas de armas autónomas y DIH	Analiza cómo los sistemas de armas autónomas transforma	Evalúa capacidades estatales para integrar,	Identifica vacíos jurídicos del DIH respecto a responsabil	Discute posiciones divergentes entre potencias y países	Se examina cómo los sistemas de armas autónomas transforma

	n operaciones militares, distribución de riesgos y modalidades de empleo de la fuerza.	probar y supervisar estos sistemas dentro de doctrinas existentes y estructuras de mando.	idad, proporcionalidad y control humano significativo sobre funciones críticas de letalidad.	periféricos sobre prohibición, regulación o moratoria de armas autónomas letales.	n operaciones militares y distribución de riesgos, exigiendo nuevas capacidades doctrinarias y técnicas. El DIH presenta importantes lagunas sobre responsabilidad y control humano, mientras las posiciones divergentes entre potencias y países periféricos reflejan una competencia geoestratégica sin consenso regulatorio robusto.
Revisión de la Investigación sobre los Riesgos Éticos en la Aplicación de la Inteligencia Artificial	Muestra cómo la expansión de IA en ámbitos militares y de seguridad genera impactos estructurales sobre derechos y libertades	Analiza capacidades institucionales para incorporar evaluaciones éticas, comités especializados y marcos de riesgo en proyectos	Sistematiza vacíos éticos recurrentes, como opacidad algorítmica, sesgos, discriminación automatizada y delegación excesiva	Sugiere que marcos éticos globales emergen en tensión con intereses estratégicos nacionales y competenc	Este trabajo evidencia que la expansión de la IA a seguridad y defensa genera impactos estructurales sobre derechos, frente a

	fundamentales.	de IA aplicada.	de decisiones sensibles.	ia tecnológica entre grandes potencias.	capacidades institucionales aún débiles para gestionar riesgos éticos. La opacidad algorítmica y los sesgos persisten en un escenario donde marcos éticos globales chocan con intereses estratégicos nacionales.
Artificial intellrms control in modern warfare	Explora cómo la incorporación de IA en sistemas de armas modifica dinámicas de control, verificación y estabilidad estratégica internacional.	Examina capacidades estatales y multilaterales para diseñar regímenes de control de armamentos adaptados a tecnologías inteligentes emergentes.	Identifica vacíos de gobernanza en tratados existentes, incapaces de abarcar autonomía, aprendizaje automático y decisiones algorítmicas en combate.	Argumenta que la competencia geopolítica dificulta acuerdos robustos, pues potencias buscan ventajas asimétricas mediante sistemas impulsados por IA.	El documento plantea que la integración de IA en sistemas de armas altera la estabilidad estratégica y los regímenes de verificación, requiriendo nuevas capacidades institucionales de control de armamentos. Los tratados

					existentes muestran vacíos frente a autonomía y aprendizaje automático, mientras la competencia geopolítica obstaculiza la construcción de acuerdos efectivos.
AI Governance in Latin America	Vincula la gobernanza de IA con impactos sobre seguridad, vigilancia estatal y potencial militarización de infraestructuras digitales en la región.	Caracteriza capacidades institucionales latinoamericanas para formular estrategias, organismos reguladores y marcos intersectoriales de gobernanza algorítmica.	Identifica vacíos legales, debilidad regulatoria y escaso control democrático sobre proyectos de IA impulsados por seguridad y defensa.	Discute cómo agendas de cooperación con potencias condicionan estándares, proveedores y prioridades estratégicas en la gobernanza regional de IA.	Se analiza cómo la gobernanza de IA en la región impacta seguridad y vigilancia, con capacidades institucionales desiguales para diseñar estrategias y organismos reguladores. Los marcos legales son débiles, especialmente en ámbitos de seguridad y defensa, y la cooperación

					internacional condiciona estándares, proveedores y prioridades estratégicas regionales.
Investigación sobre las Áreas Clave de Aplicación Militar	Mapea cómo la inteligencia artificial y sistemas inteligentes se insertan en áreas críticas de aplicación militar, transformando capacidades operativas.	Evalúa niveles de desarrollo tecnológico, infraestructura y recursos humanos especializados requeridos para implementar aplicaciones militares avanzadas.	Advierte carencias de marcos regulatorios y supervisión sobre experimentación, pruebas y uso operacional de estas aplicaciones militares emergentes.	Ubica estas áreas de aplicación dentro de la competencia global por ventajas militares, condicionando alianzas, transferencia tecnológica y dependencias.	El texto mapea áreas donde IA y tecnologías inteligentes potencian capacidades militares, redefiniendo el impacto de la guerra inteligente. La implementación exige infraestructuras, talento especializado y marcos de prueba aún insuficientes; estos desarrollos se inscriben en una competencia global por ventajas militares que condiciona transferencias y dependencias

					tecnológicas.
Geopolitical Marxism and the Promise of Radical Historicism	Interpreta la guerra inteligente como expresión de nuevas formas de acumulación, control y dominación en el sistema capitalista global.	Cuestiona capacidades estatales periféricas para contrarrestar estructuras de poder tecnocientífico dominadas por bloques hegemónicos del Norte global.	Sugiere que vacíos de gobernanza reflejan relaciones de dependencia, captura tecnológica y subordinación de marcos normativos periféricos.	Analiza competencia geoestratégica como lucha entre fracciones de capital, reconfigurando periferias y espacios de autonomía latinoamericana.	Desde una perspectiva crítico-marxista, la guerra inteligente se interpreta como forma avanzada de dominación tecnocientífica, frente a capacidades periféricas limitadas. Los vacíos de gobernanza expresan relaciones de dependencia y captura tecnológica, mientras la competencia geoestratégica reorganiza periferias y restringe las posibilidades de autonomía latinoamericana.
The Influence of Strategic Culture	Muestra cómo la cultura estratégica de Irán y	Analiza capacidades institucionales y	Sugiere que vacíos de gobernanza	Interpreta la relación Irán–Rusia como nodo dentro de	El documento muestra cómo culturas

Components on Bilateral and Regional Relations between Iran and Russia	Rusia orienta usos de tecnologías militares avanzadas y guerra inteligente.	doctrinarias resultantes, relevantes para comprender posibles aprendizajes o transferencias hacia contextos latinoamericanos.	internacional permiten cooperación militar tecnológica con impactos potenciales en regiones periféricas, incluyendo América Latina.	competencia geoestratégica más amplia, que reconfigura alineamientos globales emergentes.	estratégicas específicas orientan la adopción de tecnologías militares avanzadas, ofreciendo claves comparativas para otros contextos. Destaca capacidades institucionales y doctrinarias construidas fuera del núcleo occidental, en un escenario de vacíos regulatorios internacionales y competencia geoestratégica que reconfigura alineamientos emergentes, incluidos vínculos con América Latina.
Estudio bibliométrico sobre relacione	Evidencia que la guerra inteligente introduce tensiones	Muestra capacidades institucionales heterogéne	Identifica vacíos de gobernanza vinculados a	Sugiere que la competencia geoestratégica	Este estudio evidencia que la guerra inteligente

s civiles-militares	adicionales en relaciones civiles–militares, especialmente por militarización de funciones tecnológicas críticas.	as para ejercer control civil efectivo sobre agendas de innovación militar y ciberdefensa.	opacidad, debilidad parlamentaria y concentración tecnomilitar en ciertos aparatos de seguridad.	incentiva autonomización de élites militares, dificultando agendas de democratización en defensa.	introduce tensiones adicionales en las relaciones civiles–militares, por la concentración tecnomilitar de funciones críticas. Las capacidades estatales para ejercer control civil efectivo son desiguales; la opacidad institucional revela vacíos de gobernanza que, en un contexto de competencia geoestratégica, pueden reforzar autonomización militar.
Geopolitics in the digital age	Analiza cómo infraestructuras digitales, datos y algoritmos se convierten en componentes centrales	Examina capacidades estatales para proteger soberanía digital, desarrollar industrias tecnológicas propias y controlar	Señala vacíos regulatorios sobre plataformas, datos transfronterizos y ciberoperaciones ofensivas, dificultando gobernanz	Interpreta la competencia geoestratégica principalmente como disputa por control de redes, estándares, nubes y	El texto analiza cómo datos, redes y algoritmos se vuelven recursos centrales de la guerra inteligente, exigiendo

	de la guerra inteligente contemporánea.	flujos estratégicos de información.	a democrática del poder digital.	cadenas de valor digitales.	capacidades estatales para proteger soberanía digital. Persisten vacíos normativos sobre plataformas y ciberoperaciones, mientras la competencia geoestratégica se expresa como disputa por estándares, infraestructuras y cadenas de valor digitales.
Control de Armamentos de los Sistemas de Armas Autónomas Letales	Estudia cómo los sistemas de armas autónomas letales modifican equilibrios estratégicos, costos de intervención y riesgos de escalamiento involuntario.	Evalúa capacidades estatales y multilaterales para negociar, verificar y hacer cumplir regímenes de control específicos sobre estas tecnologías.	Señala vacíos legales en DIH y tratados de desarme, incapaces de abordar plenamente autonomía, responsabilidad y rendición de cuentas.	Discute cómo divergencias entre grandes potencias y países menores bloquean avances hacia un marco robusto de prohibición o regulación.	Se examina el impacto de las armas autónomas letales en los equilibrios estratégicos y en los costos políticos de la intervención armada. Las capacidades estatales y multilaterales para regularlas

					siguen siendo limitadas; los marcos de desarme presentan grandes lagunas, en un escenario de fuertes divergencias geopolíticas sobre prohibición o control.
Riesgos de Seguridad Internacional y Rutas de Gobernanza	Analiza la guerra inteligente como catalizador de nuevos riesgos sistémicos, afectando estabilidad internacional, disuasión y vulnerabilidades de infraestructuras críticas.	Evalúa capacidades actuales de organismos internacionales y Estados para gestionar amenazas tecnológicas y crisis complejas interconectadas.	Identifica profundos vacíos de gobernanza global, fragmentación normativa y ausencia de mecanismos efectivos de supervisión sobre tecnologías disruptivas.	Discute cómo la competencia entre potencias dificulta acuerdos, pero también impulsa propuestas parciales de regulación y confianza mutua.	El documento presenta la guerra inteligente como catalizador de nuevos riesgos sistémicos que ponen a prueba capacidades estatales e institucionales globales. Los vacíos de gobernanza, la fragmentación normativa y la débil supervisión internacional se combinan con una competencia entre

					potencias que simultánea mente dificulta e impulsa iniciativas parciales de regulación.
Problema s de Derecho Internaci onal derivados	Aborda cómo la guerra inteligente tensiona principios clásicos del derecho internacion al, particularm ente en uso de la fuerza y responsabi lidad.	Examina capacidad es de los Estados y tribunales para interpretar normas existentes frente a tecnología s autónomas , ciberopera ciones y armas inteligentes .	Identifica lagunas jurídicas significativ as relativas a atribución, jurisdicción , diligencia debida y regulación de actores privados tecnológico s.	Sugiere que la competenc ia geoestraté gica inhibe reformas profundas del derecho internacion al, priorizando flexibilidad es interpretati vas para potencias.	Se muestra cómo la guerra inteligente tensiona el derecho internacion al en atribución, uso de la fuerza y responsabil idad estatal, frente a capacidade s interpretativ as limitadas. Importantes lagunas jurídicas en ciberoperac iones y autonomía tecnológica persisten, mientras la competenci a geoestratég ica favorece interpretaci ones flexibles antes que reformas estructurale

					s del orden jurídico internacional.
Investigación sobre la tecnología de inteligencia artificial	Expone cómo desarrollos generales en inteligencia artificial crean nuevas posibilidades de aplicación militar, cibernética y de vigilancia estratégica.	Analiza capacidades científicas, infraestructuras de investigación y ecosistemas de innovación necesarios para sostener proyectos de IA de alta complejidad.	Señala vacíos de gobernanza tempranos en ética de la investigación, acceso a datos y control sobre transferencias tecnológicas sensibles.	Ubica el desarrollo de IA dentro de competencia geoestratégica por liderazgo científico, inversión y captación de talento especializado.	El texto evidencia que los avances generales en IA habilitan nuevas aplicaciones militares y de vigilancia, reforzando el impacto de la guerra inteligente. Las capacidades científicas y de innovación resultan decisivas, pero se enfrentan a vacíos éticos y regulatorios tempranos, en un contexto de competencia global por liderazgo tecnológico.
Nuevas Características y Medidas de Respuesta de la Cibergue	Describe cómo la ciberguerra electrónica redefine escenarios de	Analiza capacidades estatales para detectar, mitigar y responder	Identifica vacíos operativos en interoperabilidad, coordinación	Sitúa la ciberguerra como dimensión clave de competencia geoestraté	Aquí la guerra inteligente se expresa en ciberoperaciones avanzadas

rra Electrónica	confrontación, priorizando ataques a redes, sensores, comunicaciones y entornos informacionales.	a operaciones cibernéticas avanzadas mediante doctrinas, unidades especializadas y cooperación técnica.	interagencial y protocolos de respuesta rápida ante incidentes cibernéticos complejos.	gica, donde potencias experimentan tácticas y prueban capacidades sobre terceros.	contra redes, sensores y comunicaciones, requiriendo doctrinas y unidades especializadas. Las capacidades estatales para responder siguen siendo desiguales y operativamente frágiles, con importantes vacíos de interoperabilidad, mientras potencias experimentan tácticas y capacidades en escenarios que involucran a terceros países.
Aplicación y desarrollo de la tecnología de inteligencia artificial	Analiza aplicaciones de IA que, aunque civiles, poseen potencial de doble uso relevante para	Examina capacidades industriales y de innovación para escalar estas aplicaciones hacia sectores	Señala vacíos regulatorios sobre usos secundarios, exportaciones, protección de datos y supervisión	Ubica estas trayectorias tecnológicas dentro de cadenas globales de valor, condicionadas por estándares	El documento muestra cómo aplicaciones de IA, en principio civiles, adquieren relevancia dual para seguridad,

	vigilancia, control social y defensa.	estratégicos, incluyendo seguridad y gestión de riesgos.	del despliegue empresarial de IA avanzada.	, patentes y dependencia de plataformas extranjeras.	control social y defensa. Las capacidades industriales y de innovación determinan el aprovechamiento estratégico, pero existen vacíos regulatorios sobre usos secundarios, exportaciones y protección de datos, en cadenas globales dominadas por plataformas extranjeras.
Desarrollo de un Sistema de Concepto Operacional para un Sistema	Describe el impacto operacional de un sistema inteligente específico, redefiniendo tareas, roles humanos y ciclos de decisión táctica.	Detalla capacidades doctrinarias y organizacionales requeridas para integrar el sistema en estructuras de mando, entrenamiento y logística.	Evidencia vacíos operativos en protocolos, reglas de enfrentamiento y mecanismos de supervisión sobre decisiones asistidas por el sistema.	Sugiere que el desarrollo del sistema responde a dinámicas de competencia tecnológica y necesidad de mantener relevancia estratégica.	Se analizan los efectos concretos de un sistema inteligente en la organización operacional, redefiniendo tareas humanas y ciclos de decisión. Su integración requiere

					capacidades doctrinarias, de entrenamiento y logística aún en construcción, con vacíos en reglas de empleo y supervisión, mientras su desarrollo responde directamente a dinámicas competitivas tecnológicas.
What do Latin Americans think about the world system	Muestra percepciones ciudadanas sobre poder global, tecnología y seguridad, condicionando legitimidad social de respuestas frente a guerra inteligente.	Refleja evaluaciones sociales de capacidades estatales para proteger soberanía, garantizar seguridad humana y gestionar riesgos tecnológicos emergentes.	Evidencia desconfianza hacia gobernanza global, percepción de desigualdad normativa y dudas sobre control democrático de tecnologías estratégicas.	Registra cómo la competencia entre potencias es percibida como fuente simultánea de amenazas, oportunidades y dependencias para la región.	El documento recoge percepciones latinoamericanas sobre poder global, tecnología y seguridad, condicionando la legitimidad de respuestas frente a la guerra inteligente. La ciudadanía evalúa críticament

					e capacidades estatales, percibe vacíos en la gobernanza global y lee la competencia entre potencias como fuente simultánea de amenazas, oportunidades y dependencias.
Síntesis interpretative global	La literatura analizada revela que la guerra inteligente transforma doctrinas, capacidades y gobernanzas en América Latina, profundizando brechas tecnológicas y normativas mientras la rivalidad entre potencias condiciona autonomía regional, incrementa riesgos emergentes y redefine los márgenes estratégicos de seguridad y defensa entre 2015 y 2025.				

4.4.3 Triangulación de síntesis integradoras según técnicas de acopio de información

Las tablas de triangulación que se presentan a continuación articulan, de manera sistemática, los resultados obtenidos a partir de las entrevistas semiestructuradas, el análisis documental y la síntesis integrada por categorías. Este dispositivo permite contrastar y complementar las perspectivas empíricas y teóricas sobre la evolución de la guerra inteligente y sus efectos en los marcos de seguridad y defensa en América Latina.

Al disponer los hallazgos por categorías analíticas, impacto de la guerra inteligente, capacidades estatales, vacíos de gobernanza y competencia geoestratégica, las tablas hacen visible la convergencia, las tensiones y las brechas entre los distintos insumos de información. Así, la triangulación no solo valida los resultados, sino que también aporta un diagnóstico más robusto y coherente con la complejidad del fenómeno estudiado en el período 2015–2025.

Desde una perspectiva comparada, la triangulación entre entrevistas y análisis documental evidencia que Argentina, Brasil, Colombia, Chile, México y Perú enfrentan la guerra inteligente desde trayectorias profundamente diferenciadas. Brasil se consolida como el actor más avanzado, articulando doctrina multidominio, industria militar propia y proyectos sostenidos de IA y ciberdefensa; Chile destaca por su institucionalidad técnica, modernización doctrinaria y capacidades cibernéticas estables; Colombia desarrolla respuestas aceleradas por su conflicto interno y la presión del crimen organizado, fortaleciendo ciberinteligencia y operaciones híbridas; Argentina combina capacidad científico-tecnológica con avances irregulares condicionados por inestabilidad política; México prioriza seguridad interior y marcos normativos, aunque con rezagos operativos en guerra inteligente; mientras que Perú

avanza en ciberdefensa y normativa reciente, pero sigue limitado por dependencia tecnológica externa y capacidades industriales incipientes. En conjunto, esta comparación revela un mosaico de capacidades asimétricas que condiciona la autonomía estratégica regional e impide la construcción de una respuesta latinoamericana coherente frente a los desafíos doctrinarios, tecnológicos, normativos y geoestratégicos de la guerra inteligente.

Tabla 12

Triangulación de síntesis integradoras según técnicas de acopio de información

Categorías	Entrevista Semiestructurada	Análisis Documental	Síntesis integradora
Impacto de la guerra inteligente	Las entrevistas muestran que la guerra inteligente redefine doctrinas, operaciones y arquitecturas de seguridad, desplazando el centro de gravedad hacia el ciberespacio, los datos y los algoritmos, con énfasis en ciberdefensa, simulación táctica, armas autónomas y guerra cognitiva.	Los documentos evidencian que la guerra inteligente reconfigura estructuralmente los marcos de seguridad y defensa, transformando disuasión, escalamiento, control de armamentos y soberanía digital, e introduciendo nuevas superficies de vulnerabilidad en infraestructuras críticas e información estratégica.	En conjunto, ambas fuentes coinciden en que la guerra inteligente opera como cambio de época: altera los fundamentos doctrinarios, tecnológicos y geopolíticos de la seguridad y defensa en América Latina, desplazando el poder hacia el dominio informacional-cibernético y profundizando asimetrías entre la región y las principales potencias tecnológicas.
Capacidades estatales	Los entrevistados describen capacidades	La literatura confirma una fuerte disparidad	La triangulación revela un mosaico de

	estatales heterogéneas: Brasil y Chile aparecen más avanzados; Colombia se adapta bajo presión; México, Argentina y Perú muestran progresos fragmentados, limitados por presupuestos rígidos, débil industria militar y escasa inversión sostenida en investigación y desarrollo.	en capacidades institucionales, doctrinarias y tecnológicas entre países latinoamericanos, con avances puntuales en estrategias de IA, ciberdefensa y vigilancia, pero con brechas persistentes en resiliencia, preparación para crisis y articulación interagencial efectiva.	capacidades: algunos Estados configuran núcleos de modernización y otros permanecen rezagados, mostrando que la región enfrenta la guerra inteligente con recursos, ritmos y prioridades desiguales, lo que condiciona la posibilidad de respuestas coordinadas y de construcción de resiliencia estratégica regional.
Vacíos de gobernanza	Las entrevistas subrayan la ausencia de marcos claros sobre IA militar, armas autónomas y ciberdefensa, la debilidad del control civil, la dependencia tecnológica y la falta de normas regionales que orienten estándares, protocolos de empleo y responsabilidad por decisiones algorítmicas.	Los documentos identifican vacíos legales, éticos y operativos en DIH, derecho internacional, regulación de plataformas digitales y gobernanza algorítmica, además de fragmentación normativa global, opacidad institucional y escasa rendición de cuentas sobre proyectos tecno-militares de alto impacto.	Integradas, ambas fuentes muestran que la gobernanza de la guerra inteligente es claramente insuficiente a nivel nacional, regional y global, generando amplias zonas grises que facilitan captura tecnológica, opacidad decisional y vulneración de derechos, y dejando a América Latina reactiva frente a la velocidad del cambio tecnológico-militar.

Competencia geoestratégica	Los entrevistados coinciden en que la rivalidad China–Estados Unidos, sumada a la presencia de Rusia, condiciona elecciones tecnológicas, cooperación militar y agendas de ciberdefensa, generando dilemas de alineamiento, riesgos de dependencia y tensiones crecientes sobre la autonomía estratégica latinoamericana.	Los documentos muestran cómo la competencia entre grandes potencias se expresa en carrera armamentista basada en IA, disputa por estándares digitales, control de redes, acuerdos de cooperación militar y configuraciones hemisféricas de seguridad que colocan a América Latina como escenario periférico de confrontación indirecta.	La triangulación evidencia que la guerra inteligente se inscribe en una competencia geoestratégica que reduce márgenes de maniobra regional, pero también abre opciones de diversificación de alianzas; sin embargo, la ausencia de una agenda latinoamericana propia limita la conversión de esta disputa en verdadera autonomía estratégica.
Síntesis interpretativa global	En síntesis, la integración de entrevistas y análisis documental muestra que la guerra inteligente reconfigura doctrinas, capacidades, marcos de gobernanza y posicionamientos geoestratégicos en América Latina, profundizando brechas internas y dependencia tecnológica, mientras la rivalidad entre potencias tensiona la autonomía regional y obliga a repensar modelos de seguridad y defensa hacia 2015–2025.		

CAPÍTULO V: DIÁLOGO TEÓRICO-EMPÍRICO

El examen integrado entre los fundamentos conceptuales y los hallazgos empíricos permite comprender de manera profunda cómo la guerra inteligente está reconfigurando los marcos de seguridad, defensa y gobernanza en América Latina. Este capítulo articula ambas dimensiones —teoría y evidencia— para evaluar el impacto estratégico de la inteligencia artificial militar, los sistemas autónomos, la ciberdefensa y la competencia geoestratégica. A través del análisis de entrevistas especializadas y de la revisión teórica, se identifican patrones comunes, brechas estructurales y tensiones regionales que permiten responder a las preguntas y objetivos de investigación. Sobre esta base, se desarrollan las cinco secciones siguientes, iniciando con el impacto de la guerra inteligente en las doctrinas, capacidades y arquitecturas de seguridad latinoamericanas.

5.1 Impacto de la guerra inteligente

El diálogo entre teoría y evidencia empírica muestra que la guerra inteligente constituye una transformación estructural, doctrinaria y geopolítica que redefine las capacidades estratégicas de América Latina. Las bases teóricas revisadas en los capítulos anteriores destacan que la inteligencia artificial, los sistemas autónomos, la ciberdefensa avanzada y la guerra cognitiva alteran los umbrales del uso de la fuerza, incrementan la velocidad y complejidad de las decisiones militares y reconfiguran la competencia entre potencias globales (Long & Xu, 2022; Zhao et al., 2023; Osimen et al., 2024)

Esta comprensión teórica se articula de manera directa con los hallazgos empíricos, en los cuales los entrevistados coinciden en que la evolución tecnológica

está modificando profundamente la arquitectura de seguridad regional y los modelos de defensa de los Estados.

La transformación doctrinaria emerge como una de las consecuencias más evidentes de la guerra inteligente. De acuerdo con las entrevistas, los países suramericanos han iniciado la actualización de manuales y reglamentos para incorporar el empleo de IA, ciberdefensa y operaciones multidominio, aunque sin una guía doctrinaria unificada (entrevistado 1; entrevistado 4).

Este diagnóstico empírico dialoga con lo expuesto en el marco teórico sobre la tensión entre innovación tecnológica y rigidez doctrinaria, especialmente en contextos donde las fuerzas armadas aún mantienen estructuras operativas tradicionales que no se adaptan al ritmo acelerado de la automatización bélica (Tao & Yang, 2024; Wang et al., 2023)

La evidencia demuestra que la doctrina regional avanza, pero lo hace de forma fragmentada, parcial y sin interoperabilidad normativa.

En relación con la arquitectura de seguridad, la teoría anticipa que los Estados requieren estructuras flexibles, interagenciales y multidominio. Los testimonios corroboran esta perspectiva: las Fuerzas Armadas de varios países han creado comandos de ciberdefensa y unidades especializadas, aunque aún dependen de diseños institucionales pensados para amenazas convencionales. Los entrevistados enfatizan que la región mantiene arquitecturas centradas en el intercambio de información, sin una integración real de capacidades digitales ni una doctrina robusta de ciberoperaciones (entrevistado 1; entrevistado 4).

Esta desconexión confirma lo planteado por Saavedra (2024) y Filgueiras (2023), quienes advirtieron que la ciberseguridad latinoamericana carece de estructuras estables y de políticas interagenciales que integren defensa, inteligencia y gobernanza tecnológica.

Respecto a los riesgos emergentes, la convergencia entre teoría y evidencia es contundente. La literatura revisada plantea que los ciberataques de alta escala, la manipulación algorítmica, la autonomía letal y la guerra cognitiva son amenazas centrales del nuevo paradigma bélico (Zhang et al., 2022; Luo et al., 2023)

En la evidencia empírica, los entrevistados coinciden en que un ciberataque coordinado podría paralizar servicios esenciales sin necesidad del uso físico de la fuerza (entrevistado 1; entrevistado 3, entrevistado 4).

Asimismo, se revela que organizaciones criminales, como el narcotráfico y la minería ilegal, ya están incorporando tecnologías de IA y drones, lo que confirma la advertencia teórica sobre la difusión tecnológica hacia actores no estatales.

La gobernanza tecno-militar también muestra un fuerte diálogo entre teoría y práctica. Las bases teóricas señalan que la supervisión civil, la ética algorítmica, la auditoría tecnológica y los marcos de responsabilidad son esenciales para evitar abusos, errores letales y capturas tecnológicas (Lu, 2024; Macher, 2021)

Las entrevistas corroboran esta preocupación: los países latinoamericanos carecen de legislación específica sobre IA militar y sistemas autónomos, lo que genera vacíos éticos y operativos que afectan la toma de decisiones y la interoperabilidad institucional (entrevistado 1; entrevistado 3).

Finalmente, la autonomía tecnológica y la cooperación regional aparecen como dimensiones críticas. Teóricamente, América Latina enfrenta una “dependencia tecnológica estructural” que limita su soberanía digital y su capacidad de disuasión (Krivolapov & Stepanova, 2023; Bianculli, 2024)

Los entrevistados confirman que la región sigue siendo compradora más que productora de tecnología militar avanzada, con una industria militar débil y capacidades de innovación fragmentadas. Del mismo modo, la cooperación regional se mantiene limitada a intercambios bilaterales o vínculos con la Junta Interamericana de Defensa, sin mecanismos sostenidos de desarrollo tecnológico conjunto (entrevistado 1; entrevistado 2; entrevistado 4).

En conjunto, el diálogo teórico–empírico revela que el impacto de la guerra inteligente en América Latina se expresa en doctrinas incompletas, arquitecturas institucionales insuficientes, riesgos amplificados, gobernanza precaria y autonomía tecnológica restringida, configurando un escenario de vulnerabilidad estratégica que coincide plenamente con los objetivos y preguntas de la investigación.

5.2 Capacidades estatales

El análisis de capacidades estatales evidencia una profunda correspondencia entre los postulados teóricos y los hallazgos empíricos. Las bases conceptuales señalan que la respuesta efectiva a la guerra inteligente depende del fortalecimiento institucional, doctrinario y tecnológico, así como de la reducción de brechas regionales y del desarrollo de resiliencia estratégica (Saavedra, 2024; Campos, 2025)

Los testimonios confirman que estos elementos son precisamente las áreas más críticas y desiguales de América Latina.

En el plano institucional, las fuentes teóricas destacan que la integración entre defensa, inteligencia, innovación y ciberseguridad debe ser sistémica y articulada. Sin embargo, los entrevistados describen estructuras descoordinadas, procesos fragmentados y una insuficiente comprensión política del dominio cibernético, lo cual retrasa la formulación de políticas y la asignación de recursos (entrevistado 2; entrevistado 3). Estos hallazgos coinciden con el diagnóstico teórico de que la región carece de sistemas integrados de mando y control digital capaces de anticipar, mitigar y responder a amenazas híbridas.

Las capacidades doctrinarias también muestran una fuerte convergencia entre teoría y evidencia. La literatura reconoce que la adaptación doctrinaria es un requisito para operar en entornos multidominio y altamente tecnológicos. Las entrevistas sostienen que algunos países han iniciado procesos de actualización doctrinal, pero lo hacen a ritmos distintos y sin estándares comunes. La ausencia de una doctrina regional compartida, mencionada reiteradamente por los entrevistados, confirma la advertencia teórica de que la falta de interoperabilidad doctrinal incrementa la vulnerabilidad continental y limita la cooperación.

En cuanto a las capacidades tecnológicas, la literatura identifica una brecha estructural entre países desarrollados y América Latina, especialmente en IA militar, ciberdefensa avanzada y sistemas autónomos. Las entrevistas corroboran esta brecha, revelando limitaciones en infraestructura digital, hardware estratégico, centros de datos soberanos, algoritmos propios y especialistas en guerra inteligente (entrevistado 1; entrevistado 4). Del mismo modo, se evidencia que la dependencia de proveedores extranjeros genera problemas de interoperabilidad, mantenimiento, soberanía y seguridad, confirmando lo señalado por Krivolapov & Stepanova (2023).

La categoría brechas regionales es donde la coincidencia teoría–empiria es más marcada. Las fuentes teóricas plantean que América Latina avanza de forma heterogénea, con países como Brasil en la vanguardia tecnológica y otros como Haití o Honduras prácticamente sin capacidades digitales. Los testimonios reproducen exactamente esta segmentación regional, destacando que los avances son asimétricos, desorganizados y vulnerables a cambios políticos, lo que dificulta la construcción de una agenda continental coherente.

Finalmente, la dimensión preparación y resiliencia es identificada tanto en la teoría como en la evidencia como la principal carencia estratégica. La teoría subraya que la resiliencia digital es equivalente a la soberanía tecnológica en la guerra contemporánea. Las entrevistas coinciden al afirmar que la región tiene una capacidad limitada para identificar amenazas, responder a ataques y recuperarse de incidentes cibernéticos. La ausencia de inversiones en innovación, hardware soberano y formación de especialistas refuerza este diagnóstico, alineándose plenamente con los objetivos de la investigación sobre la interpretación de capacidades estatales frente a la guerra inteligente.

5.3 Vacíos de gobernanza

La literatura teórica plantea que los vacíos de gobernanza (legales, éticos, operativos, institucionales y tecnológicos) son uno de los principales factores que incrementan el riesgo estratégico de la guerra inteligente (Lu, 2024; Macher, 2021; Pomares, 2024)

El análisis empírico confirma la existencia de estos vacíos y los ubica en el centro de la vulnerabilidad regional.

El vacío legal aparece como un componente transversal. Teóricamente, la falta de normas específicas sobre armas autónomas, responsabilidad algorítmica, ciberoperaciones y uso militar de datos genera incertidumbre y riesgo. Las entrevistas corroboran esta situación: la mayoría de los países no tiene leyes de IA aplicadas a defensa, por lo que las fuerzas armadas quedan sujetas a normativas civiles insuficientes (entrevistado 1). De esta manera, la teoría y la práctica convergen en la afirmación de que la región enfrenta una desregulación crítica que limita la adopción segura de tecnologías emergentes.

El vacío ético también presenta una alta correspondencia entre teoría y evidencia. Los estudios revisados enfatizan que el uso de IA y la autonomía letal plantean dilemas morales inéditos, especialmente en la atribución de decisiones de vida o muerte a algoritmos. Las entrevistas advierten que, al no contar con doctrinas éticas claras, los Estados se exponen a sesgos algorítmicos, decisiones automatizadas sin supervisión humana y riesgos en la legitimidad del uso de la fuerza. Esto confirma la preocupación teórica sobre la opacidad tecnológica y la necesidad de establecer principios de control humano significativo.

En el plano operativo, los hallazgos empíricos señalan que la ausencia de estándares, protocolos y procedimientos específicos dificulta la integración de tecnología avanzada. La teoría ya anticipaba que, sin marcos operativos claros, las fuerzas armadas operan bajo reglas inestables que afectan la interoperabilidad, la capacidad de respuesta y la certificación de procesos. El diálogo entre teoría y empírea coincide, por tanto, en que los vacíos operativos constituyen un obstáculo estructural para la modernización militar.

La captura tecnológica es uno de los elementos más sensibles del diálogo teórico–empírico. Teóricamente, depender de proveedores extranjeros condiciona la soberanía digital y limita la capacidad estatal de auditoría, mantenimiento y control. Los testimonios confirman que la región depende casi por completo de hardware y software extranjeros, que no existen mecanismos de auditoría algorítmica ni de seguridad tecnológica, y que la dependencia puede comprometer incluso la atribución de responsabilidades ante fallas o ataques.

Finalmente, la rendición de cuentas es un vacío coincidente en teoría y evidencia. Tanto los estudios teóricos como las entrevistas resaltan que no existe un sistema regional de supervisión tecno-militar, ni marcos robustos de transparencia, ni mecanismos de fiscalización sobre el uso de IA y sistemas autónomos. Esta carencia refuerza la tesis central de que la gobernanza latinoamericana está rezagada respecto a la velocidad de la innovación, lo que amplía los riesgos y limita las capacidades estatales, cumpliendo así con el tercer objetivo de la investigación.

5.4 Competencia geoestratégica

El diálogo teórico–empírico evidencia que la rivalidad entre China y Estados Unidos es un factor determinante para comprender la evolución de la guerra inteligente en América Latina. Las bases teóricas sostienen que la competencia por tecnologías críticas (5G, IA, ciberseguridad, satélites, drones, puertos estratégicos) está redefiniendo las relaciones hemisféricas y generando tensiones entre autonomía y alineamiento (Krivolapov & Stepanova, 2023; Zhang et al., 2022).

Los entrevistados confirman que esta competencia ya se expresa en la asistencia militar, la provisión tecnológica, los convenios académicos y la infraestructura crítica (E1; E3; E4)

En la subcategoría rivalidad China–EE. UU., la teoría plantea que ambas potencias buscan posicionarse como líderes de la carrera tecnológico-militar, influyendo en las decisiones de defensa de terceros países. Las entrevistas indican que China ofrece becas, cooperación militar y desarrollo de infraestructuras estratégicas, mientras que Estados Unidos enfatiza ciberseguridad, control marítimo y estándares digitales. Este patrón confirma el marco teórico sobre la disputa por influencia geopolítica basada en tecnología militar e infraestructura digital.

La dependencia tecnológica es un punto donde teoría y evidencia convergen con fuerza. Las fuentes teóricas señalan que la dependencia de proveedores extranjeros limita la soberanía estatal y condiciona la capacidad operativa. Las entrevistas muestran que la región opera con sistemas rusos, franceses, estadounidenses y chinos, sin interoperabilidad técnica. Infraestructuras como el Puerto de Chancay o estaciones espaciales administradas por potencias ilustran esta dependencia, confirmando el diagnóstico teórico.

Las respuestas regionales también muestran coherencia entre teoría y evidencia. Teóricamente, América Latina presenta respuestas fragmentadas y orientadas por intereses políticos particulares. Los entrevistados coinciden en que no existe una estrategia regional común, y que las divisiones ideológicas dificultan la convergencia en defensa, gobernanza tecnológica o autonomía digital. Esto confirma el cuarto objetivo de investigación, relativo a cómo la competencia entre potencias condiciona las respuestas regionales.

La autonomía estratégica aparece como una aspiración más que una realidad. La teoría sostiene que la autonomía requiere capacidades tecnológicas, industriales y políticas, además de liderazgo e integración regional. La evidencia empírica

demuestra que, pese al talento humano presente en la región, las decisiones políticas, la falta de inversión y la dependencia tecnológica obstaculizan cualquier avance hacia la autonomía. La teoría, por tanto, encuentra en los testimonios una confirmación empírica de que la región corre el riesgo de convertirse en escenario de competencia más que en actor autónomo.

Finalmente, la agenda hemisférica revela que la gobernanza de seguridad sigue siendo definida desde los marcos interamericanos donde la influencia de Estados Unidos es predominante. Los entrevistados advierten que, aunque existen foros, no se consolidan mecanismos concretos de cooperación en IA militar, ciberdefensa o armas autónomas. Esto confirma la brecha entre la agenda teórica de una defensa regional soberana y la práctica empírica de una región dependiente de marcos externos.

5.5 Latinoamérica ante la guerra inteligente

Brasil lidera doctrinas multidominio e integración tecnológica; Chile y Colombia avanzan moderadamente; Argentina y México muestran avances parciales; Perú adapta doctrinas lentamente, con fuerte dependencia. La región conserva brechas tecnológicas, arquitecturas fragmentadas y baja interoperabilidad.

Brasil posee mayores capacidades institucionales, tecnológicas e industriales; Chile y Colombia mantienen desarrollos medios; Argentina y México exhiben progresos discontinuos; Perú fortalece ciberdefensa, pero carece de autonomía. Las brechas regionales perpetúan vulnerabilidades estratégicas compartidas.

Brasil desarrolla normativas más robustas; Chile y Colombia avanzan en ciberseguridad; Argentina y México mantienen marcos parciales; Perú carece de

regulación específica en IA militar. La región exhibe vacíos legales, éticos y operativos persistentes.

Brasil equilibra cooperación con China y Estados Unidos; Colombia favorece vínculos estadounidenses; Argentina oscila políticamente; México mantiene pragmatismo; Chile prioriza estabilidad; Perú gestiona dependencias crecientes. América Latina continúa siendo terreno de disputa tecnológica y estratégica.

5.6 Conclusión integradora del diálogo teórico–empírico

El conjunto del diálogo teórico–empírico muestra que la guerra inteligente constituye una transformación estructural que rebasa lo meramente tecnológico y redefine la seguridad, la defensa, la gobernanza y la geopolítica en América Latina. La teoría anticipa estos cambios, y la evidencia empírica confirma que la región responde con capacidades desiguales, vacíos regulatorios persistentes, dependencia tecnológica crítica y una inserción geoestratégica condicionada por la rivalidad entre potencias globales. Así, las cuatro categorías analíticas confluyen en un diagnóstico compartido: la región enfrenta un escenario donde la modernización militar es imprescindible, pero requiere gobernanza sofisticada, autonomía tecnológica gradual, cooperación regional efectiva y decisiones estratégicas que permitan enfrentar los riesgos emergentes de la guerra inteligente sin renunciar a la soberanía y la estabilidad regional.

CONCLUSIONES

La investigación demuestra que la evolución de la guerra inteligente está reconfigurando de manera profunda y acelerada los marcos de seguridad y defensa en América Latina. La incorporación de inteligencia artificial militar, sistemas autónomos, ciberestrategias, tecnologías de fusión hombre–máquina y operaciones cognitivas redefine los modos de disuasión, mando y control, así como la arquitectura institucional del poder militar. Las entrevistas analizadas confirman que esta transformación no es abstracta ni lejana: la región ya experimenta impactos concretos en la doctrina, la estructura organizacional, la gestión del riesgo y la toma de decisiones estratégicas, coincidiendo con la literatura especializada recogida en los documentos proporcionados. Sin embargo, este impacto ocurre de manera desigual, fragmentada y con un rezago estructural respecto al ritmo de innovación global.

En relación con la primera pregunta de investigación, los resultados muestran que la guerra inteligente está alterando los marcos de seguridad mediante la expansión del dominio cibernético, la adopción parcial de operaciones multidominio, la creación de comandos de ciberdefensa y la incorporación incipiente de IA en simulaciones, vigilancia y operaciones tácticas. Argentina, Chile, Colombia y Perú avanzan con niveles distintos de adaptación; México mantiene una estrategia fragmentada; y Brasil se consolida como el actor más adelantado doctrinaria y tecnológicamente. No obstante, la región sigue caracterizada por la fragmentación en doctrina digital, la ausencia de interoperabilidad regional, la alta dependencia de proveedores externos y la debilidad de la industria militar local. Esto configura un escenario donde los desafíos estratégicos se concentran en la gobernanza tecno-

militar, la autonomía tecnológica limitada y la insuficiente cooperación regional, tal como señalan las entrevistas y la literatura analizada en los archivos.

Respecto a la segunda pregunta de investigación, la evidencia revela que las capacidades institucionales, doctrinarias y tecnológicas latinoamericanas son insuficientes y profundamente desiguales. Brasil destaca por su industria militar, inversión en ciberdefensa y madurez doctrinaria; Chile y Colombia presentan capacidades medias con avances importantes en ciberseguridad; Argentina oscila según los ciclos políticos; México avanza lentamente; y Perú desarrolla comandos especializados, pero con fuertes limitaciones tecnológicas y presupuestales. De acuerdo con las entrevistas, las brechas tecnológicas (hardware soberano, centros de datos propios, especialistas en IA militar) son críticas y condicionan la resiliencia estratégica de la región. Estas variaciones explican por qué América Latina no puede aún sostener una respuesta conjunta o coordinada frente a amenazas de guerra inteligente.

En relación con la tercera pregunta de investigación, los hallazgos permiten concluir que los vacíos normativos, éticos y operativos constituyen la principal vulnerabilidad estratégica frente a la guerra inteligente. La región carece de leyes específicas sobre IA militar, armas autónomas, algoritmos de decisión letal, auditoría tecnológica y ciberoperaciones ofensivas. Los archivos analizados muestran que, incluso cuando existen leyes de inteligencia artificial (como en Perú), estas no contemplan el ámbito de defensa y seguridad. En el plano ético, persiste la ausencia de protocolos para el control humano significativo, la responsabilidad algorítmica, la neutralización de sesgos y la protección de derechos fundamentales en contextos militares. Operativamente, las fuerzas armadas latinoamericanas carecen de

estándares, certificaciones, manuales, interoperabilidad y mecanismos de adquisición tecnológica seguros, lo cual incrementa los riesgos de fallas, mal uso o captura tecnológica, según advierten los entrevistados. Estos vacíos evidencian una gobernanza desfasada respecto a la aceleración tecnológica de la guerra contemporánea.

Finalmente, respecto a la cuarta pregunta de investigación, la competencia geoestratégica entre China y Estados Unidos influye decisivamente en las respuestas regionales y condiciona la autonomía estratégica latinoamericana. Los archivos muestran que China amplía su presencia mediante infraestructura crítica, cooperación tecnológica, diplomacia de defensa y formación de cuadros militares; mientras que Estados Unidos sostiene su presencia a través de interoperabilidad militar, ciberseguridad hemisférica y control de infraestructuras digitales. Las entrevistas confirman que esta rivalidad sitúa a los países latinoamericanos ante dilemas de alineamiento estratégico. Brasil intenta equilibrar ambas potencias; Colombia privilegia la alianza con Estados Unidos; Argentina oscila según el ciclo político; Chile y México mantienen pragmatismo; y Perú gestiona dependencias crecientes ligadas a proyectos estratégicos administrados por potencias externas. Esta configuración evidencia que la región continúa siendo más un espacio de competencia que un actor autónomo, y que la ausencia de una cooperación regional sólida limita la posibilidad de construir una soberanía tecnológica compartida.

En síntesis, la investigación concluye que América Latina enfrenta la guerra inteligente desde una posición de vulnerabilidad estructural, marcada por capacidades fragmentadas, gobernanza insuficiente, dependencia tecnológica profunda y presiones geopolíticas externas crecientes. Estos factores limitan la

autonomía estratégica, amplifican los riesgos y dificultan la construcción de un marco regional coherente frente a la transformación bélica del siglo XXI. Superar estas brechas requiere fortalecer la industria militar regional, consolidar doctrinas tecnológicas compartidas, diseñar marcos ético-normativos robustos y articular una cooperación regional capaz de integrar la innovación soberana, la resiliencia digital y la estabilidad geoestratégica continental.

RECOMENDACIONES

Las transformaciones derivadas de la guerra inteligente; caracterizadas por la integración acelerada de inteligencia artificial militar, sistemas autónomos, ciberestrategias y operaciones cognitivas; plantean para América Latina un conjunto de desafíos estratégicos que trascienden lo tecnológico y alcanzan dimensiones doctrinarias, institucionales, normativas y geopolíticas. Los hallazgos teóricos y empíricos de esta investigación evidencian brechas sustantivas en capacidades estatales, vacíos regulatorios críticos, dependencias tecnológicas profundas y una inserción internacional marcada por la competencia entre grandes potencias. Frente a este escenario, resulta imprescindible formular recomendaciones orientadas a fortalecer la resiliencia regional, promover la autonomía tecnológica, modernizar las doctrinas militares y consolidar marcos de gobernanza que permitan responder de manera eficaz y soberana a las amenazas emergentes de la guerra inteligente. Las siguientes recomendaciones buscan, por tanto, ofrecer lineamientos estratégicos, realistas y aplicables que contribuyan al desarrollo de capacidades nacionales y regionales acordes con las exigencias de la defensa contemporánea.

1. Fortalecimiento doctrinario y modernización operativa

Es indispensable que los Estados latinoamericanos desarrollen doctrinas de guerra inteligente, integrando IA militar, ciberdefensa, operaciones multidominio y armas autónomas en sus procesos de planeamiento. Se recomienda crear manuales regionales armonizados, actualizar las reglas de enfrentamiento y fortalecer la formación profesional en entornos de combate automatizado. Cada país debe consolidar Centros de Simulación Avanzada con IA, replicando modelos exitosos como los registrados en las entrevistas (p. ej., el Centro de Simulación Táctica del

Ejército del Perú). Una doctrina común permitiría mejorar la interoperabilidad regional, reducir asimetrías y anticipar amenazas híbridas y cognitivas, conforme sugieren la teoría y los hallazgos empíricos.

2. Desarrollo de autonomía tecnológica y ecosistemas de innovación

Se recomienda establecer programas nacionales y regionales de I+D+i militar, orientados a desarrollar algoritmos propios, sensores, drones, ciberarmamento defensivo y plataformas de vigilancia inteligente. La región debe reducir su dependencia tecnológica mediante fabricación local, transferencia tecnológica equilibrada y alianzas estratégicas supervisadas, priorizando hardware soberano y centros de datos nacionales. Países como Brasil pueden liderar clústeres tecnológicos regionales, creando cadenas de valor militar en IA, ciberseguridad y sistemas autónomos. Asimismo, se propone la creación de un Banco Latinoamericano de Innovación en Defensa, financiado por consorcios público–privados, para sostener proyectos de largo plazo.

3. Construcción de marcos legales, éticos y operativos robustos

Es urgente desarrollar leyes específicas de inteligencia artificial militar, armas autónomas y defensa digital, incorporando principios como control humano significativo, responsabilidad algorítmica y estándares de auditoría tecnológica. Cada Estado debe establecer agencias de supervisión tecno-militar para fiscalizar adquisiciones, procesos algorítmicos y operaciones de ciberdefensa, reduciendo riesgos de captura tecnológica. A nivel regional, se recomienda promover un Marco Interamericano de Gobernanza Algorítmica en Defensa, que homologue la legislación, estandarice protocolos y defina principios éticos aplicables a la guerra inteligente. Asimismo, se deben diseñar protocolos de interoperabilidad para

operaciones conjuntas, certificación de ciberunidades y manejo de infraestructura crítica.

4. Desarrollo de resiliencia estratégica y capacidades institucionales

Los Estados deben consolidar sistemas de resiliencia digital capaces de anticipar, responder y recuperarse de ciberataques, fallas algorítmicas y operaciones cognitivas. Esto incluye la creación de Centros Nacionales de Respuesta a Incidentes Cibernéticos (CSIRT) interconectados regionalmente, así como la inversión en laboratorios de ciberseguridad, redes redundantes, simuladores de crisis y protocolos de continuidad estatal. Se recomienda priorizar la formación de especialistas en guerra inteligente, ampliando la cooperación académica, el entrenamiento interagencial y la profesionalización en IA, ciberseguridad, robótica militar y análisis de datos. Las Fuerzas Armadas deben adoptar una cultura estratégica del conocimiento, tal como lo señalan los entrevistados, fortaleciendo el capital humano como base de la soberanía tecnológica.

5. Impulso de cooperación regional en defensa tecnológica

América Latina necesita construir una arquitectura de cooperación regional que trascienda los intercambios bilaterales y los foros declarativos. Se recomienda: i) Crear un Comando Regional de Ciberdefensa, con participación inicial de Brasil, Chile, Colombia, Argentina, México y Perú; ii) Establecer una Red Latinoamericana de Academias Militares en IA y Guerra Inteligente para compartir doctrina, formación y ejercicios simulados; iii) Diseñar programas de desarrollo tecnológico conjunto (drones, sensores, software de ciberdefensa); y, iv) Impulsar acuerdos de interoperabilidad técnica y compartición de inteligencia algorítmica.

Estas iniciativas permitirían responder de manera colectiva a amenazas híbridas y superar la fragmentación geopolítica que caracteriza actualmente a la región.

6. Gestión estratégica de la competencia China–Estados Unidos

Los países latinoamericanos deben adoptar estrategias de equilibrio inteligente, evitando alineamientos automáticos con cualquiera de las potencias. Se recomienda evaluar cada acuerdo tecnológico según criterios de soberanía digital, dependencia crítica, riesgos de acceso a datos y compatibilidad doctrinaria. La región debe promover una agenda autónoma de seguridad tecnológica, negociando con ambos polos desde intereses propios y no desde presiones geopolíticas externas. Asimismo, se recomienda fortalecer organismos multilaterales capaces de gestionar esta disputa, proponiendo una Agenda Latinoamericana de Autonomía Estratégica que incluya infraestructura crítica, IA, ciberseguridad y sistemas autónomos.

7. Consolidación de una visión hemisférica de seguridad inteligente

Es necesario que América Latina transite de una seguridad tradicional a una seguridad inteligente, integrando IA, ciberdefensa, resiliencia digital y autonomía tecnológica en la arquitectura hemisférica. La OEA y la JID pueden liderar una iniciativa hemisférica para IA militar y ciberseguridad, promoviendo estándares comunes, entrenamiento avanzado y monitoreo de riesgos. Para ello, se recomienda impulsar la creación de un Centro Hemisférico de Innovación Tecnológica Militar, que articule capacidades de Estados, academia e industria. Esto contribuiría a reducir asimetrías, fortalecer la interoperabilidad y mejorar la estabilidad geopolítica regional.

Estas recomendaciones se orientan a fortalecer la autonomía estratégica latinoamericana y reducir las vulnerabilidades derivadas de la guerra inteligente. La región posee talento humano, capacidades emergentes e instituciones con potencial; sin embargo, convertir estas ventajas en poder estratégico exige visión política, inversión sostenida, gobernanza tecnológica moderna y una cooperación regional efectiva. La guerra inteligente no es un fenómeno futuro: ya está configurando el presente. La respuesta estratégica debe construirse ahora.

PROPUESTA PARA ENFRENTAR LA REALIDAD PROBLEMÁTICA

La investigación demuestra que América Latina enfrenta la guerra inteligente desde una posición de vulnerabilidad estructural marcada por la dependencia tecnológica, la fragmentación doctrinaria, los vacíos normativos y la presión geoestratégica ejercida por potencias tecnológicas globales. Superar esta realidad problemática exige una propuesta regional integral que articule capacidades estatales, innovación soberana, gobernanza tecnológica y cooperación estructurada. A continuación, se plantea una propuesta estratégica orientada a fortalecer la resiliencia continental y garantizar la autonomía regional frente a los desafíos de la guerra inteligente.

1. Construcción de una Doctrina Regional de Guerra Inteligente

Los países latinoamericanos deben avanzar hacia una doctrina conjunta que incorpore conceptos modernos de operaciones multidominio, ciberdefensa, autonomía algorítmica, guerra cognitiva y mando inteligente. Esta doctrina debe armonizar lineamientos actualmente fragmentados y establecer estándares mínimos de interoperabilidad, inspirándose en los avances de Brasil y los marcos interamericanos existentes. Una visión doctrinaria compartida permitirá mejorar la respuesta regional ante amenazas híbridas y reducir asimetrías operativas entre países.

2. Desarrollo de una Base Tecnológica Regional Soberana

La región necesita transitar de una posición de compradora tecnológica hacia un modelo productor–desarrollador, fortaleciendo industrias militares locales y capacidades de I+D+i. La propuesta considera:

- creación de clústeres regionales de innovación militar (liderados inicialmente por Brasil, Chile y Colombia);
- diseño de proyectos tecnológicos conjuntos (drones, sensores, software defensivo, IA militar propia);
- establecimiento de centros de datos soberanos y reglas de protección algorítmica;
- incentivos para empresas y universidades en tecnologías estratégicas.

Esta estrategia busca reducir la dependencia de proveedores externos (China, EE. UU. y Europa) y construir una plataforma regional de autonomía digital.

3. Implementación de un Marco Normativo y Ético de Alcance Continental

La ausencia de regulación en IA militar, armas autónomas y ciberoperaciones exige la creación de un Marco Latinoamericano de Gobernanza de Tecnologías de Defensa que considere:

- legislación unificada sobre IA militar y sistemas autónomos;
- estándares éticos para control humano significativo;
- protocolos de responsabilidad algorítmica y auditoría tecnológica;
- normativas sobre protección de infraestructuras críticas;
- regulaciones para evitar captura tecnológica y vulnerabilidad institucional.

Este marco debe ser impulsado por los ministerios de defensa, organismos regionales y la Junta Interamericana de Defensa (JID).

4. Fortalecimiento de la Resiliencia Institucional y del Capital Humano

Ninguna transformación estratégica es posible sin capacidades humanas sólidas. La propuesta plantea:

- creación de Escuelas Regionales de Inteligencia Artificial Militar, integrando Argentina, Brasil, Chile, Colombia, México y Perú;
- formación avanzada en ciberseguridad, robótica militar, análisis de datos e ingeniería algorítmica;
- simuladores regionales para entrenar escenarios de guerra inteligente;
- generación de una cultura estratégica basada en conocimiento, innovación y anticipación.

Este eje permitiría enfrentar la brecha de especialistas, uno de los desafíos más críticos identificados.

5. Arquitectura Regional de Ciberdefensa y Cooperación Estratégica

La región necesita una estructura concreta y operativa. Se propone:

- creación del Comando Latinoamericano de Ciberdefensa (CLAC), encargado de coordinar respuestas ante amenazas cibernéticas regionales;
- construcción de una Red Regional de CSIRT militares para proteger infraestructura crítica;
- mecanismos permanentes de intercambio de inteligencia algorítmica;
- realización de ejercicios multilaterales anuales de guerra inteligente;
- fortalecimiento del Consejo Sudamericano de Defensa o su equivalente actualizado.

Este nivel de cooperación permitiría a los estados actuar de manera conjunta ante crisis, evitando respuestas aisladas e ineficientes.

6. Estrategia Regional frente a la Competencia China–Estados Unidos

La propuesta sugiere que la región adopte una estrategia de equilibrio inteligente, basada en decisiones soberanas y no en alineamientos automáticos. Para ello se requiere:

- mecanismos regionales de evaluación de riesgos geoestratégicos ante acuerdos tecnológicos;
- negociaciones multilaterales que reduzcan dependencia crítica de cualquier potencia;
- acuerdos de transferencia tecnológica supervisada y equilibrada;
- fortalecimiento de la autonomía decisional en proyectos de infraestructura digital, espacial y logística;
- posicionamiento de América Latina como actor autónomo, no como espacio de disputa.

Este enfoque permitirá gestionar la rivalidad geopolítica sin comprometer la soberanía regional.

7. Consolidación de una Agenda Hemisférica de Seguridad Inteligente

Finalmente, la región debe construir una agenda hemisférica que integre IA, ciberseguridad y operaciones autónomas como pilares centrales de la defensa. Se propone la creación del:

- Centro Hemisférico para la Innovación en Guerra Inteligente, articulado con la JID y la OEA;
- “Libro Blanco de Seguridad Inteligente” para América Latina;
- programas regionales de anticipación estratégica y análisis prospectivo;
- mesas permanentes de coordinación entre fuerzas armadas, academias militares y sectores tecnológicos.

Esta agenda permitirá superar la fragmentación geopolítica y fortalecer la estabilidad estratégica continental.

Esta propuesta integral busca convertir la vulnerabilidad tecnológica y doctrinaria de América Latina en una oportunidad para la construcción de capacidades soberanas, marcos normativos modernos y alianzas estratégicas regionales. La guerra inteligente ya forma parte del presente; enfrentarla exige coordinación, innovación y visión de largo plazo. Solo mediante una articulación regional sólida y un compromiso político sostenido la región podrá garantizar su autonomía estratégica, estabilidad y seguridad en un escenario global dominado por la competencia tecnológica y la automatización del poder militar.

REFERENCIAS BIBLIOGRÁFICAS

Banta, B., & Kaufman, S. J. (2022). Integrative pluralism and security studies: The implications for International Relations theory. European Journal of International Security. https://www.scopus.com/pages/publications/85126744989?origin=scopusAI

Batista, R., Villar, O., González, H. & Milián, V. (2020). Cultural challenges of the malicious use of artificial intelligence in Latin American regional balance. *Proceedings of the 2nd European Conference on the Impact of Artificial Intelligence and Robotics, ECIAIR 2020* (pp. 7–13). Academic Conferences International https://doi.org/10.34190/EAIR.20.029

Becker Castellaro, S., Carvalho, M., Fernandez Gibaja, A., Grassi, A., Hammar, C., Muller, J., Pereira, L., Piaia, V., & Ruediger, M. A. (2025). Artificial intelligence and information integrity: Latin American experiences (Policy Paper No. 34). International IDEA & Fundação Getulio Vargas. https://doi.org/10.31752/idea.2025.39

Bianculli, A. (2024). América Latina en el nuevo escenario internacional: ¿qué espacio hay para el regionalismo y la cooperación regional? *Revista CIDOB d'Afers Internacionals, 136*, 89–110. https://doi.org/10.24241/rcai.2024.136.1.89

Burton, J. & Soare, S. (2019). Understanding the Strategic Implications of the Weaponization of Artificial Intelligence. En T. Minarik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga & G. Visky (Eds.), *Proceedings of the 11th International Conference on Cyber Conflict: Silent Battle, CyCon 2019* (art. No. 8756866). NATO CCD COE Publications. https://doi.org/10.23919/cycon.2019.8756866

Campos Ríos, M. (2025). Artificial intelligence and public policy in Latin America and the Caribbean: Experiences and contributions toward shaping a regional roadmap. SELA & CLAD.

Castro Valdebenito, H. J., & Monteverde Sánchez, A. (2018). Latin American hemispheric security adapted to new technologies: Cybersecurity and advances in regional and international cooperation for the sanction of cybercrime. Espacios. https://www.scopus.com/pages/publications/85053776043?origin=scopusAI

Ding, G., Ge, B., Li, M., (...), Yang, Z. (2024). Conceptual Research on Intelligent Urban Combat System Based on SysML. Lecture Notes in Electrical Engineering. https://www.scopus.com/pages/publications/85218491977?origin=scopusAI

Filgueira, F. (2023). Artificial intelligence governance challenges in Latin America. infrastructure, decolonization and new dependency. *Revista del CLAD Reforma y Democracia, 87*, 44–70. https://doi.org/10.69733/clad.ryd.n87.a3

Flores, D. F., & Vergara, J. J. B. (2025). A constructivist approach to the geopolitics of Latin American regionalism: The case of ALBA-TCP. In International Relations in Times of Transition: Concepts, Debates and Regional Perspectives. https://www.scopus.com/pages/publications/85213920025?origin=scopusAI

Gatica, J. P. S. (2025). Geopolitics in the digital age: the U.S.-China competition through their narratives on digital technologies. Revista de Internet, Derecho y Política. https://www.scopus.com/pages/publications/105003834733?origin=scopusAI

Gómez, O. A. (2015). Alternative views of security in Latin America: Towards a global contribution to human security. Regions and Cohesion. https://www.scopus.com/pages/publications/84962409112?origin=scopusAI

Kefeli, I. F., Vykhodets, R. S., & Plebanek, O. V. (2025). Updating cognitive security in a global dimension. Journal of Globalization Studies. https://www.scopus.com/pages/publications/105011933908?origin=scopusAI

Kosevich, E. (2023). Theoretical foundations of the foreign policy of Latin American nations: The evolution of the concept of autonomy and the role of integration. Mezhdunarodnye Protsessy. https://www.scopus.com/pages/publications/85175246022?origin=scopusAI

Krivolapov, O. & Stepanova, N. (2023). Russia´s cooperation with the Latin American countries in security field. *Iberoamerica, 1*, 31–52. https://doi.org/10.37656/s20768400-2023-1-02

Lash, J. (2022). Economic Security: Conceptual and Operational Intersection of Trade Policy and National Security. In Handbook of Security Science. https://www.scopus.com/pages/publications/85159443323?origin=scopusAI

Long, K., & Xu, N. (2020). Control de armamentos de sistemas de armas autónomas letales: dilemas, salidas y estrategias de participación. International Outlook, 2, 78–98. https://doi.org/10.13851/j.cnki.gjzw.202002005

Long, K., & Xu, N. (2022). Artificial intelligence military applications: International security risks and governance paths. International Security Studies, 5, 123–141. https://doi.org/10.13851/j.cnki.gjzw.202205007

Lu, L. (2024). The challenges of artificial intelligence development on international law and response. International Journal of Humanities and Social Sciences Research, 5(6), 76–88. Shenzhen Polytechnic University.

Luján, C. A. (2023). What do Latin Americans think about the world system? Estudos Internacionais. https://www.scopus.com/pages/publications/85200829468?origin=scopusAI

Luo, J., Zhang, W., Xiang, F., Jiang, C., & Chen, J. (2023). Survey on Intelligent Wargaming: Tactical & Campaign Wargame and Strategic Game from Game-Theoretic Perspective. Journal of System Simulation, 35(9), 1871–1894. https://doi.org/10.16182/j.issn1004731x.joss.23-0300

Macher Reyes, M. (2021). Sistemas de armas autónomas y Derecho Internacional Humanitario: Advertencia de un futuro cercano. IUS ET VERITAS, (63), 179–188. https://doi.org/10.18800/iusetveritas.202102.009

Mares, D. R., & Kacowicz, A. M. (2015). Routledge handbook of Latin American security. Routledge. https://www.scopus.com/pages/publications/84942307445?origin=scopusAI

Meza Rivas, M. J. (2019). El desarrollo y el uso de los sistemas de armas autónomas letales en los conflictos armados internacionales [Tesis doctoral, Universidad de Barcelona]. Universitat de Barcelona.

Miao, C., & Wang, R. (2022). Artificial intelligence application ethical risk research review. Journal of Chongqing University of Technology (Social Science), 36(4), 198–206. https://doi.org/10.3969/j.issn.1674-8425(s).2022.04.018

Mirzekhanov, V. (2025). The Legacy of the Congress of Vienna as a Factor in International Relations from the 19th to the Early 21st Century. Istoriya. https://www.scopus.com/pages/publications/105018518941?origin/scopusAI

Osimen, G., Newo, O. & Fulani, O. M. (2024). Artificial intelligence and arms control in modern warfare. *Cogent Social Sciences, 10*(1). https://doi.org/10.1080/23311886.2024.2407514

Pomares, J. (2024). AI governance in Latin America: Towards a new “Brussels Effect” or a distinct regional approach? Global Solutions Journal, (11), 156–164.

Rivera-Rodríguez, H.-A., Beltrán Duque, A., & Sánchez-López, J. C. (2025). What characterizes strategy research in Latin America? A bibliometric analysis for the 1990–2023 period. Journal of Management History. https://www.scopus.com/pages/publications/85199435947?origin=scopusAI

Saavedra, B. (2004). Confronting terrorism in Latin America: building up cooperation in the andean ridge region. *Low Intensity Conflict & Law Enforcement, 12*(3), 156–171. https://doi.org/10.1080/09662840500072847

Saavedra, B. (2024). Cybersecurity in Latin America: Challenges, concerns and opportunities.

Sharmila, C., Baiju, B. V., Gino Sophia, S. G., (...), Kirubha, D. (2025). Artificial intelligence framework for ISTAR missions in tactical networks using autonomous vehicles. In Battery-Free Sensor Networks for Sustainable Next-Generation IoT Connectivity. https://www.scopus.com/pages/publications/105007711327?origin=scopusAI

Slaughter, A.-M. (2004). International law and international relations theory: A prospectus. In The Impact of International Law on International Cooperation: Theoretical Perspectives. https://www.scopus.com/pages/publications/84916962367?origin=scopusAI

Tao, R., & Yang, Z. (2024). Research on key areas and maturity evaluation of AI military applications. Command Control & Simulation, 46(2), 63–68. https://doi.org/10.3969/j.issn.1673-3819.2024.02.009

Teschke, B., & Pfaler, L. V. (2024). Quo Vadis, Historical International Relations? Geopolitical Marxism and the Promise of Radical Historicism. Uluslararası

İlişkiler. https://www.scopus.com/pages/publications/85197726721?origin=scopusAI

Valizadeh, A., & Kazemi, S. (2022). The Influence of Strategic Culture Components on Bilateral and Regional Relations between Iran and Russia. Central Eurasia Studies. https://www.scopus.com/pages/publications/85138644563?origin=scopusAI

Velandia Pardo, E. F., & Betancur Montoya, M. A. (2025). Bibliometric study on civil-military relations in Latin America in the last 30 years. Revista Científica General José María Córdova. https://www.scopus.com/pages/publications/105000951454?origin=scopusAI

Wang, C., Ji, H., Guo, Q., Dong, Z., Tan, Y., & Mu, G. (2023). Development of combat concept of intelligent land assault system based on DoDAF. Journal of System Simulation, 35(11), 2397–2409. https://doi.org/10.16182/j.issn1004731x.joss.22-0628

Wang, Z., & Yang, Z. (2017). Research on artificial intelligence technology and the future intelligent information service architecture. Telecommunications Science, 33(5), 1–11. https://doi.org/10.11959/j.issn.1000-0801.2017134

Zhang, D., Deng, S., & Li, Z. (2022). Nuevas características y contramedidas de la confrontación cibernético-electrónica en la era de la inteligencia]. New Generation of Information Technology, 5(9), 32-35. https://doi.org/10.3969/j.issn.2096-6091.2022.09.007

Zhao, Y., Huang, Y., Li, H., & Meng, J. (2023). Application and development of artificial intelligence technology in military intelligence field. Command Control & Simulation, 45(4), 36–43. https://doi.org/10.3969/j.issn.1673-3819.2023.04.006

Mardones, P. C., & García, M. G. (2024). Unión de dos unidades léxicas: Uso de co-ocurrencias para investigar el desarrollo y autoevaluación de la lengua oral en profesorado. *Fronteiras, 13*(1), 291–302. https://doi.org/10.21664/2238-8869.2024v13i1p.291-302

Sha, Y., & Clarke, I. (2025). Using ATLAS.ti to interpret keyword co-occurrence analysis: A case study on the representation of vaccin∗ across pseudoscience and conspiracy websites. Linguistics Vanguard. *Advance online publication*. https://doi.org/10.1515/lingvan-2024-0066

Anexo 1. Matriz de Consistencia

Evolución de la Guerra Inteligente y Desafíos Estratégicos para la Seguridad y Defensa Nacional en América Latina, 2015-2025

Problemas	Objetivos	Categorías y Subcategorías	Metodología
- ¿Cómo está impactando la evolución de la guerra inteligente, incluyendo el uso militar de inteligencia artificial, armas autónomas y ciberestrategias, en los marcos de seguridad y defensa nacional de los países de América Latina, y qué desafíos estratégicos plantea en términos de gobernanza, autonomía tecnológica y cooperación regional? - ¿Qué capacidades institucionales, doctrinarias y tecnológicas poseen los Estados latinoamericanos para responder a las amenazas emergentes de la guerra inteligente, y cómo varían dichas capacidades entre países? - ¿Cuáles son los vacíos normativos, éticos y operativos más críticos en los	- Interpretar cómo la guerra inteligente transforma los marcos de defensa y seguridad en América Latina y qué desafíos plantea en gobernanza, autonomía y cooperación. - Analizar las capacidades institucionales, doctrinarias y tecnológicas de los Estados latinoamericanos frente a la guerra inteligente y sus variaciones entre países. - Identificar los vacíos normativos, éticos y operativos en la gobernanza latinoamericana ante el avance de tecnologías de guerra inteligente. - Comprender cómo la competencia entre grandes potencias influye en las respuestas regionales y en la construcción de autonomía	**Categoría 1:** Impacto de la guerra inteligente Subcategorías: - Transformación doctrinaria - Arquitectura de seguridad - Riesgos emergentes - Gobernanza tecno-militar - Autonomía tecnológica - Cooperación regional **Categoría 2:** Capacidades estatales Subcategorías: - Institucionales - Doctrinarias - Tecnológicas - Brechas regionales - Preparación y resiliencia **Categoría 3:** Vacíos de gobernanza Subcategorías: - Legal - Ético	- **Enfoque de Investigación:** cualitativo - **Tipo de Investigación:** teórico-empírico - **Método de Investigación:** estudio de caso múltiple comparativo - **Escenario de Estudio:** sistemas nacionales de defensa y seguridad de América Latina. En el plano conceptual, el estudio se sitúa en la intersección entre geopolítica, estrategia y gobernanza digital. - **Diseño Muestral:** intencional. Seis unidades de análisis principales: Brasil, Argentina, Chile, Colombia, México y Perú. La muestra documental comprende aproximadamente 40 fuentes especializadas.

marcos legales y de gobernanza de América Latina frente a la proliferación de tecnologías de guerra inteligente? - ¿Cómo influye la competencia geoestratégica entre grandes potencias, como China y Estados Unidos, en la configuración de las respuestas regionales frente a la guerra inteligente, y qué implicancias tiene ello para la autonomía estratégica de América Latina?	estratégica en América Latina.	- Operativo - Captura tecnológica - Rendición de cuentas **Categoría 4:** Competencia geoestratégica Subcategorías: - Rivalidad China-EE. UU. - Dependencia tecnológica - Respuestas regionales - Autonomía estratégica - Agenda hemisférica	- **Técnicas e Instrumentos de Recolección de Información** **Técnicas:** Análisis documental, revisión bibliográfica sistemática y análisis comparativo **Instrumentos:** Guía de análisis documental, ficha de registro bibliográfico, matriz comparativa de países - **Validación de los Instrumentos:** juicio de expertos. Cinco especialistas en geopolítica, defensa y análisis estratégico. - **Técnicas para el Procesamiento de la Información:** Transcripción y organización de la información; codificación abierta y axial; y, análisis interpretativo y triangulación - **Aspectos Éticos:** integridad académica, confidencialidad, transparencia y respeto a la propiedad intelectual.

Anexo 2: Validación del Instrumento

Validación de Instrumento

Chorrillos, 13 de noviembre de 2025

Informe N.º 001

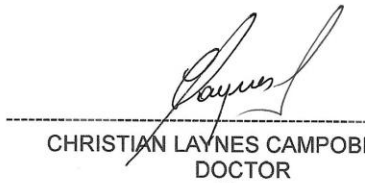
De : CHRISTIAN LAYNES CAMPOBLANCO
Para : Cmdte he wang
Cmdte yan houyi

Me dirijo a Ustedes respetuosamente para saludarlos y agradecer la designación para la evaluación de la Validez de Contenido de la Guía de entrevista semiestructurada, instrumento de recolección de información para la tesis titulada: "...".

Después de la evaluación correspondiente se determina que:

a. El Instrumento cumple en su totalidad con los criterios, por lo que es válido para proceder a la recolección de la información (SI)

b. El Instrumento no cumple en su totalidad con los criterios, por lo que deberá levantar las observaciones siguiendo las sugerencias propuestas ( )



CHRISTIAN LAYNES CAMPOBLANCO
DOCTOR
Firma

Validación de Instrumento

Chorrillos, 13 de noviembre de 2025

Informe N.º 002

De : MIGUEL ANGEL CHIMA CERDAN
Para : Cmdte he wang
Cmdte yan houyi

Me dirijo a Ustedes respetuosamente para saludarlos y agradecer la designación para la evaluación de la Validez de Contenido de la Guía de entrevista semiestructurada, instrumento de recolección de información para la tesis titulada: "...".

Después de la evaluación correspondiente se determina que:

a. El Instrumento cumple en su totalidad con los criterios, por lo que es válido para proceder a la recolección de la información (SI)

b. El Instrumento no cumple en su totalidad con los criterios, por lo que deberá levantar las observaciones siguiendo las sugerencias propuestas ( )

MIGUEL ANGEL CHIMA CERDAN
DOCTOR
Firma

Validación de Instrumento

Chorrillos, 13 de noviembre de 2025

Informe N.º 003

De : HEIDY LUANNA CASTILLO MORMONTOY
Para : Cmdte he wang
Cmdte yan houyi

Me dirijo a Ustedes respetuosamente para saludarlos y agradecer la designación para la evaluación de la Validez de Contenido de la Guía de entrevista semiestructurada, instrumento de recolección de información para la tesis titulada: "...".

Después de la evaluación correspondiente se determina que:

a. El Instrumento cumple en su totalidad con los criterios, por lo que es válido para proceder a la recolección de la información (SI)

b. El Instrumento no cumple en su totalidad con los criterios, por lo que deberá levantar las observaciones siguiendo las sugerencias propuestas ( )

HEIDY LUANNA CASTILLO MORMONTOY
DOCTORA
Firma

Anexo 3: Instrumentos de Recolección de información

3.1 Guía de Análisis Documental

Objetivo: Orientar la revisión sistemática de literatura científica, documentos estratégicos y marcos doctrinarios sobre guerra inteligente, capacidades estatales, vacíos de gobernanza y competencia geoestratégica.

Sección	Descripción	Observación
Identificación del documento	Datos bibliográficos y tipo de documento	
Eje temático	Categoría principal a la que se adscribe el documento	
Dimensión analítica	Subcategoría analizada (doctrinaria, tecnológica, ética, etc.)	
Ideas clave	Síntesis de los principales aportes del documento	
Implicancias	Consecuencias teóricas o estratégicas del contenido	
Evidencia textual	Fragmento relevante o cita clave	
Análisis y lectura crítica	Interpretación o inferencia del investigador	

3.2 Ficha de Registro Bibliográfico

Objetivo: Sistematizar las fuentes revisadas, integrando datos técnicos y analíticos para construir la base documental de la investigación.

Campo	Contenido
Referencia completa (APA 7ma. ed.)	
DOI / URL	
Año / País / Idioma	
Tipo de fuente	Artículo científico / Documento de defensa / Libro / Informe institucional
Categoría analítica	(Impacto / Capacidades / Vacíos / Competencia)
Subcategoría	(Transformación doctrinaria, dependencia tecnológica, etc.)
Resumen analítico (5 líneas)	Síntesis del aporte y su relación con la categoría.
Palabras clave	
Vacío identificado	
Posible aporte para el estudio	Cómo puede fortalecer la comprensión teórica o empírica del fenómeno.

Escuela Superior de Guerra del Ejército
XVI Programa de Alto Mando del Ejército-PAME 2025
Maestría en Geopolítica y Estrategia
Evolución de la Guerra Inteligente y Desafíos Estratégicos para la Seguridad y Defensa Nacional en América Latina, 2015-2025

3.3 Guía de Entrevista Semiestructurada

Objetivo: Comprender cómo la evolución de la guerra inteligente está reconfigurando las doctrinas, capacidades y estructuras de seguridad en América Latina, y qué desafíos estratégicos genera en términos de autonomía, gobernanza y cooperación regional.

Categoría 1. Impacto de la Guerra Inteligente

1. Desde su experiencia, ¿cómo ha transformado la guerra inteligente (incluyendo la inteligencia artificial, los sistemas autónomos y las ciberestrategias) las doctrinas, estructuras y arquitecturas de seguridad de los Estados latinoamericanos?

2. ¿Qué desafíos emergen en términos de autonomía tecnológica, gobernanza tecno-militar y cooperación regional frente a esta nueva configuración de poder y amenaza?

Categoría 2. Capacidades Estatales

3. ¿Cómo evalúa las capacidades institucionales, doctrinarias y tecnológicas de los Estados latinoamericanos para responder a los escenarios de guerra inteligente y amenazas híbridas?

4. ¿Qué brechas regionales o debilidades estructurales identifica en materia de preparación, innovación y resiliencia ante los nuevos desafíos tecnológicos de defensa?

Categoría 3. Vacíos de Gobernanza

5. ¿Cuáles considera que son los principales vacíos legales, éticos y operativos en la gobernanza de las tecnologías militares inteligentes en América Latina?

6. ¿Qué riesgos supone la dependencia o captura tecnológica en términos de soberanía, control civil y rendición de cuentas sobre las decisiones de defensa inteligente?

Categoría 4. Competencia Geoestratégica

7. ¿Cómo influye la competencia geoestratégica entre China y Estados Unidos en la configuración de las políticas de defensa y seguridad de América Latina frente a la guerra inteligente?

8. ¿Qué posibilidades existen para que la región construya una autonomía estratégica y una agenda hemisférica propia en materia de seguridad y desarrollo tecnológico militar?

Cierre de la entrevista

9. Desde su perspectiva, ¿cuál será el principal desafío estratégico que enfrentará América Latina en el escenario de guerra inteligente hacia 2030?

10. ¿Desea agregar alguna reflexión sobre el futuro de la guerra inteligente y sus implicaciones para América Latina?

11. ¿Qué recomendaciones formularía para fortalecer la capacidad estratégica de los Estados de la región?

Anexo 4: Matriz Analítica-Comparativa de Países de América Latina, 2015-2025

Objetivo: Analizar comparativamente cómo distintos países latinoamericanos enfrentan la guerra inteligente en términos doctrinarios, tecnológicos, normativos y geoestratégicos.

País	Categoría 1	Categoría 2	Categoría 3	Categoría 4	Sentido
Argentina	Modernización limitada; IA en fase incipiente; dependencia tecnológica alta; vulnerabilidad informacional creciente. Arquitectura de seguridad fragmentada.	Instituciones con capacidades desiguales; doctrina parcialmente actualizada; brechas tecnológicas críticas; resiliencia media.	Vacíos legales y éticos amplios; falta de protocolos para IA militar; dependencia de proveedores externos.	Dependencia elevada de EE. UU. y China; baja autonomía; respuestas regionales mínimas.	Rezago tecnológico estructural; postura reactiva; vulnerabilidad estratégica frente a guerra cognitiva y ciberamenazas.
Brasil	Mayor avance regional; integración de IA en ciberdefensa; comando cibernético maduro; transformación doctrinaria en	Fortalezas institucionales; doctrina en actualización; capacidades tecnológicas robustas; menor brecha regional.	Vacíos operativos en regulación de IA militar; desafíos éticos moderados; riesgo de captura tecnológica limitada.	Actor bisagra en la rivalidad China–EE.UU.; diversificación tecnológica; búsqueda activa de autonomía estratégica.	Liderazgo regional; capacidad de influir en gobernanza hemisférica; mejor preparado para guerra inteligente.

	curso; liderazgo en cooperación JID.				
Colombia	Avances en ciberseguridad aplicados a conflicto interno; adopción de tecnologías de vigilancia; arquitectura de seguridad orientada al combate híbrido.	Instituciones fuertes; doctrina adaptada a amenazas híbridas; capacidades tecnológicas intermedias; resiliencia alta.	Vacíos éticos y legales en vigilancia algorítmica; dependencia de empresas extranjeras; limitada fiscalización civil.	Cooperación intensa con EE.UU.; dependencia tecnológica alta; baja autonomía frente a IA militar.	Capacidad operativa alta pero autonomía limitada; adaptación doctrinaria superior a la media regional.
Chile	Avances significativos en digitalización; doctrina sólida; infraestructura crítica protegida; arquitectura de ciberdefensa establecida.	Capacidades institucionales estables; doctrina moderna; desarrollo tecnológico medio-alto; resiliencia fortalecida.	Vacíos éticos moderados; marco legal en actualización; dependencia tecnológica persistente.	Cooperación equilibrada con potencias; autonomía técnica moderada; integración regional activa.	Perfil de país estable, con gobernanza ordenada y capacidad de absorción tecnológica destacada.
México	Impacto fuerte de desinformación y guerra cognitiva; vulnerabilidad en integridad informacional;	Instituciones fragmentadas; capacidades tecnológicas limitadas; doctrina	Amplios vacíos legales y operativos; débil gobernanza algorítmica; captura	Competencia EE.UU.–China intensa; alta dependencia de	Vulnerabilidad alta en guerra cognitiva; riesgo estratégico elevado por

	arquitectura de seguridad tensionada.	poco actualizada; resiliencia desigual.	tecnológica evidente.	proveedores norteamericanos.	debilidad normativa y tecnológica.
Perú	Impacto creciente de IA en vigilancia, ciberdefensa y gestión de crisis; arquitectura de seguridad en transición.	Capacidades institucionales en desarrollo; doctrina desactualizada, pero en proceso de modernización; brecha tecnológica severa; resiliencia media.	Vacíos legales y éticos profundos; inexistencia de regulación de IA militar; dependencia crítica de proveedores externos.	Dependencia estructural de EE.UU. y China; débil agenda regional; autonomía estratégica baja.	Vulnerabilidad elevada; urgencia de modernización doctrinaria, tecnológica y regulatoria; riesgo de dependencia estructural.
Integración interpretativa	La Matriz Analítica-Comparativa de Países de América Latina revela tres patrones regionales: **1. Asimetría marcada en capacidades y nivel de impacto** - Brasil es el país mejor posicionado para transitar hacia la guerra inteligente. - Chile y Colombia muestran capacidades intermedias con marcos institucionales más estables. - Argentina, México y Perú exhiben rezagos estructurales, alta dependencia tecnológica y limitados avances doctrinarios. **2. Amplios vacíos de gobernanza tecnológica** - En los seis países predominan vacíos legales, éticos y operativos ante la IA militar, las armas autónomas y la guerra cognitiva. - La región carece de estándares para control humano significativo, rendición de cuentas y regulación de algoritmos militares.				

	3. Dependencia estructural en la competencia China–Estados Unidos - Ningún país logra autonomía tecnológica plena. - Brasil muestra la mayor diversificación; México y Perú la mayor dependencia. - La región carece de respuestas regionales coordinadas frente al avance de tecnologías críticas.
Conclusiones comparativas	La evolución de la guerra inteligente profundiza las asimetrías estratégicas en América Latina, revelando tres niveles diferenciados de preparación: i) un único país con capacidades avanzadas y liderazgo regional (Brasil); ii) un grupo intermedio que muestra avances parciales y arquitecturas relativamente estables (Chile y Colombia); y, iii) un conjunto de países con rezagos estructurales en doctrina, tecnología, marcos regulatorios y autonomía estratégica (Argentina, México y Perú). Estas brechas condicionan la capacidad regional para responder colectivamente a amenazas basadas en IA, ciberoperaciones y guerra cognitiva. El impacto de la guerra inteligente es heterogéneo, pero todos los países experimentan transformaciones significativas en sus arquitecturas de seguridad. Mientras Brasil y Chile integran progresivamente IA y ciberdefensa en sus doctrinas, Argentina, México y Perú muestran un impacto más reactivo, marcado por la dependencia tecnológica y la vulnerabilidad informacional. Colombia destaca por adaptar sus capacidades a amenazas híbridas vinculadas al conflicto interno y al crimen organizado. En términos de capacidades estatales, Brasil se posiciona como el país con mayor solidez institucional, doctrinaria y tecnológica, seguido por Chile y Colombia, que exhiben arquitecturas estables y resilientes. En contraste, Argentina, México y Perú presentan deficiencias en absorción tecnológica, baja actualización doctrinaria y limitaciones institucionales, lo que incrementa su exposición frente a ataques cibernéticos, fallas algorítmicas y operaciones cognitivas. Los vacíos de gobernanza constituyen el patrón común más crítico en toda la región. Ningún país dispone de un marco normativo integral para regular IA militar, armas autónomas, ciberoperaciones ofensivas ni control humano significativo. Los vacíos éticos y operativos son más profundos en Argentina, México y Perú, mientras que Brasil, Chile y Colombia muestran avances parciales pero insuficientes. Esta ausencia

	de gobernanza genera espacios para la captura tecnológica, la opacidad operativa y la dependencia estructural de proveedores externos. Respecto a la competencia geoestratégica en tecnologías críticas, todos los países latinoamericanos enfrentan presiones derivadas de la rivalidad China–Estados Unidos, pero su margen de maniobra varía. Brasil exhibe la mayor diversificación tecnológica, mientras que México y Perú dependen fuertemente de proveedores estadounidenses, lo que limita su autonomía estratégica. Chile y Colombia buscan equilibrios, pero mantienen dependencia en ámbitos clave como ciberseguridad y hardware militar. En conjunto, la región carece de una estrategia común para enfrentar la disputa entre potencias. En síntesis, comparativa, América Latina ingresa a la era de la guerra inteligente con una arquitectura defensiva fragmentada, capacidades dispares, marcos regulatorios insuficientes y baja autonomía tecnológica. La ausencia de cooperación regional, sumada a la dependencia de tecnologías críticas importadas, limita la posibilidad de construir una defensa interoperable y soberana. El carácter multidimensional de la guerra inteligente: cognitivo, algorítmico, cibernético y autónomo, desborda la capacidad actual de los Estados latinoamericanos, lo que aumenta la urgencia de políticas coordinadas en gobernanza tecnológica, actualización doctrinaria y desarrollo de capacidades soberanas.
Sentido estratégico regional	América Latina enfrenta la guerra inteligente desde una posición de vulnerabilidad estructural, caracterizada por capacidades desiguales, dependencia tecnológica, vacíos regulatorios y arquitectura de seguridad insuficiente para la era algorítmica. Brasil emerge como el único actor con potencial de liderazgo regional, mientras que el resto de los países se encuentra atrapado entre la necesidad de modernizarse y el riesgo de consolidar nuevas subordinaciones tecnológicas frente a China y Estados Unidos. La región carece de una estrategia colectiva que articule autonomía estratégica, gobernanza tecno-militar y cooperación regional sostenida.