

DE LA GUERRA HÍBRIDA A LA VULNERABILIDAD HÍBRIDA ESTRUCTURAL: CUANDO EL EFECTO SUPERA LA INTENCIÓN

Pablo S. Caubarrere Diab*

RESUMEN

Este artículo propone una distinción conceptual de relevancia doctrinal: la diferencia entre la guerra híbrida intencional (GHI) —cuya eficacia depende de un adversario que diseña y ejecuta una campaña multidominio con objetivo estratégico definido— y la vulnerabilidad híbrida estructural (VHE), condición en la que la convergencia no coordinada de múltiples vectores de daño —narcotráfico, desinformación, dependencia tecnológica, erosión institucional, guerra cognitiva— produce efectos funcionalmente equivalentes a los de una campaña híbrida deliberada, aunque ningún actor los haya orquestado. Esta distinción tiene implicancias operativas directas: los instrumentos clásicos de la contrainteligencia y la disuasión resultan insuficientes frente a una VHE, que exige resiliencia sistémica, inteligencia de patrones y cohesión social como política activa. El artículo actualiza el marco doctrinal incorporando los modelos VICA, BANI y CAVE, integra la guerra cognitiva como el vector más peligroso dentro de la VHE e incluye recomendaciones estratégicas diferenciadas para el contexto uruguayo e iberoamericano.

Palabras clave: guerra híbrida, guerra cognitiva, resiliencia institucional, inteligencia estratégica, Iberoamérica, Uruguay.

Lista de siglas y abreviaturas

Sigla	Significado
AFP	Agence France-Presse
AGESIC	Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento

* Centro de Altos Estudios Nacionales (CALEN). Coronel (R) del Arma de Infantería. Magister en Estrategia Nacional. Licenciado en Ciencias Militares. Diplomado en Estado Mayor. Posgrado en Seguridad y Defensa. Coordinador y Docente de la Cátedra de Estrategia, CALEN e IMES. pablo.caubarrere@calen.edu.uy

Sigla	Significado
BANI	Frágil (Brittle), Ansioso (Anxious), No lineal (Nonlinear), Incomprensible (Incomprehensible)
CAVE	Convergencia tecnológica, Autonomía de sistemas, Vulnerabilidad digital, Evolución exponencial
CERTUY	Centro Nacional de Respuesta a Incidentes de Seguridad Informática
CODENA	Consejo de Defensa Nacional
COT	Crimen Organizado Transnacional
DGI	Dirección General Impositiva
DIE	Dirección de Inteligencia del Estado
DOTMLPF-I	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities – Interoperability
DSA	Digital Services Act (Reglamento de Servicios Digitales, Unión Europea)
EEAS	European External Action Service (Servicio Europeo de Acción Exterior)
ESMADE	Estado Mayor de la Defensa
FIMI	Foreign Information Manipulation and Interference (Manipulación e Interferencia de Información Extranjera)
GC	Guerra Cognitiva
GHI	Guerra Híbrida Intencional
IoT	Internet of Things (Internet de las cosas)
NATO/OTAN	North Atlantic Treaty Organization / Organización del Tratado del Atlántico Norte
NIST	National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología, EE. UU.)
OSINT	Open Source Intelligence (Inteligencia de fuentes abiertas)
PNSP	Plan Nacional de Seguridad Pública
PQC	Post-Quantum Cryptography (Criptografía poscuántica)
PSYOPS	Psychological Operations (Operaciones psicológicas)
SENACLAFT	Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo
SIEE	Secretaría de Inteligencia Estratégica del Estado
SILCON	Sistema de Lucha contra el Crimen Organizado y Narcotráfico
SNIE	Sistema Nacional de Inteligencia del Estado
SVR	Sluzhba Vneshney Razvedki (Servicio de Inteligencia Exterior de Rusia)
VHE	Vulnerabilidad Híbrida Estructural

Sigla	Significado
VICA	Volátil, Incierto, Complejo, Ambiguo

Introducción

En un entorno internacional marcado por la volatilidad, la ambigüedad y la saturación informativa, la guerra híbrida se ha consolidado como la forma dominante de conflicto en el siglo XXI. En Iberoamérica, sus manifestaciones ya operan bajo presión criminal, cibernética, informativa y jurídica, afectando la soberanía estatal, la legitimidad institucional y la seguridad humana.

La literatura estratégica y los marcos doctrinales predominantes abordan la guerra híbrida fundamentalmente como un fenómeno de arquitectura intencional: un adversario identificable que despliega de forma coordinada múltiples instrumentos con un objetivo estratégico definido. Esta conceptualización es operativamente válida para escenarios como la intervención rusa en Ucrania o las operaciones de influencia chinas en el Indo-Pacífico, donde existe una cadena de mando, una doctrina explícita y una voluntad política centralizada.

Sin embargo, esta concepción resulta insuficiente para describir —y sobre todo para responder— a la situación que enfrenta la mayoría de los Estados iberoamericanos. Los efectos estratégicos de daño institucional, erosión de la cohesión social y degradación de la capacidad decisional del Estado no provienen necesariamente de un adversario que los ha diseñado. Proviene de la convergencia funcional de actores con objetivos parciales y dispares —el narcotráfico que busca rentas, los operadores de desinformación que buscan polarización, las dependencias tecnológicas que generan exposición cibernética, la fragmentación social que erosiona confianza— que no se coordinan entre sí pero cuyos efectos se acumulan y convergen en el mismo resultado: un Estado debilitado, una sociedad fragmentada, una soberanía degradada.

Este artículo propone nominar ese fenómeno como Vulnerabilidad Híbrida Estructural (VHE) y argumenta que constituye una categoría analítica propia, irreducible a la guerra híbrida intencional (GHI), con implicancias doctrinales y operativas específicas. La distinción no es semántica: determina el diseño de las herramientas de respuesta, la arquitectura institucional de defensa y la asignación de recursos estratégicos.

El artículo se estructura en torno a tres ejes. El primero actualiza el marco doctrinal incorporando los modelos VICA, BANI y CAVE y establece la distinción GHI/VHE con precisión analítica. El segundo examina la guerra cognitiva como vector singular dentro de la VHE. El tercero traduce el análisis al contexto uruguayo e iberoamericano, formulando recomendaciones estratégicas diferenciadas por tipo de amenaza. El análisis se apoya en fuentes doctrinales, literatura académica especializada y casos empíricos documentados en fuentes abiertas; no incluye trabajo de campo primario, lo que abre la necesidad de investigación empírica sistemática sobre las variables identificadas.

Marco teórico y doctrinal

Definición y evolución doctrinal

La guerra híbrida se caracteriza por la convergencia funcional de medios convencionales, irregulares, cibernéticos, informacionales, jurídicos y económicos. A diferencia de los conflictos tradicionales, no se despliega en fases secuenciales ni en dominios aislados, sino como una arquitectura simultánea, persistente y adaptativa orientada a generar efectos estratégicos sin necesidad de guerra declarada (Hoffman, 2007; Murray & Mansoor, 2012).

Doctrinalmente, esta lógica se actualiza en la propuesta de Gerasimov (2013) de integración entre medios militares y no militares con énfasis en la desorganización del adversario desde adentro, lo que en Iberoamérica introduce el riesgo de sobre atribuir intencionalidad a dinámicas que son en parte estructurales.

Sus componentes doctrinales incluyen acciones cinéticas limitadas, ciberoperaciones, campañas de desinformación, *lawfare* —uso instrumental del derecho como herramienta de presión estratégica (Dunlap, 2008)— y coerción económica. Los desarrollos más recientes —los informes del EEAS (2026) sobre FIMI, las conclusiones del Consejo de la Unión Europea (2026)— confirman que la guerra híbrida incorpora inteligencia artificial generativa y expande su radio hacia Iberoamérica, como evidencia la operación "La Compañía" contra Argentina en abril de 2026.

Entornos VICA, BANI y CAVE como catalizadores

La eficacia de la guerra híbrida se potencia en entornos que amplifican la penetración de actores hostiles y dificultan la respuesta institucional. El modelo VICA (Volátil, Incierto, Complejo, Ambiguo) describe un mundo donde

la velocidad del cambio y la ambigüedad informativa generan escenarios donde las amenazas híbridas operan con ventaja. El modelo BANI (Frágil, Ansioso, No lineal, Incomprensible), propuesto por Cascio (2021), actualiza el VICA para describir cómo la fragilidad institucional y la ansiedad social favorecen la manipulación cognitiva y la polarización.

El modelo CAVE —Convergencia tecnológica, Autonomía de sistemas, Vulnerabilidad digital y Evolución exponencial— fue propuesto por el Coronel (R) Pedro Martín Gómez-De Luca (2025) para describir el entorno específico generado por la revolución tecnológica. En él, la convergencia del internet de las cosas (IoT), inteligencia artificial y análisis de big data crea interdependencias sistémicas; sistemas autónomos operan con mínima intervención humana; y el ritmo de innovación excede la capacidad de adaptación institucional. El autor añade una dimensión metafórica deliberada: cave en inglés significa caverna, evocando la Alegoría de la Caverna de Platón: el riesgo que describe es que decisores operen confundiendo sombras de desinformación con la realidad estratégica.

La dimensión de evolución exponencial del CAVE incluye un vector de vulnerabilidad de horizonte cercano: la computación cuántica. Cuando esta tecnología madure, será capaz de quebrar los sistemas criptográficos que hoy protegen las comunicaciones estatales, financieras y de defensa. La amenaza no es futura sino presente, bajo la lógica de "cosechar ahora, descifrar después": actores estatales ya interceptan y almacenan comunicaciones cifradas para descifrarlas cuando la capacidad cuántica esté disponible. En respuesta, el NIST publicó en 2024 los primeros estándares de criptografía poscuántica, iniciando una transición global cuya planificación los Estados no pueden diferir (NIST, 2024).

La interacción entre los tres modelos no es aditiva sino multiplicativa: sus efectos se potencian mutuamente. Un Estado cuyas instituciones son frágiles (BANI) y cuya infraestructura tecnológica presenta dependencias no gestionadas (CAVE) ofrece al mismo tiempo una superficie de ataque cognitivo amplificada y una capacidad de respuesta degradada ante la velocidad del cambio (VICA). Esa combinación genera las condiciones para que la VHE se consolide sin necesidad de arquitecto externo.

Multiplicadores exógenos y marcos jurídicos nacionales

La guerra híbrida puede verse amplificada por factores exógenos —desastres climáticos, pandemias, deterioro ambiental— que desorganizan la respuesta estatal y saturan capacidades logísticas. Estos multiplicadores no

constituyen amenazas híbridas por sí mismos, pero pueden ser funcionalizados dentro de la VHE. La pandemia de COVID-19 es el caso más documentado: permitió operaciones en dominios informacional, logístico y jurídico bajo condiciones de alta ansiedad y baja capacidad de verificación.

En el caso de Uruguay, el Decreto 371/020 establece diez amenazas estratégicas para el período 2020-2025, varias de las cuales son vectores de VHE: la violación de la soberanía en el ciberespacio, el crimen organizado transnacional, los ciberataques y la inestabilidad democrática regional son los de mayor funcionalización híbrida directa. Es metodológicamente relevante señalar que el decreto no menciona explícitamente la desinformación, el lawfare ni la guerra cognitiva como amenazas autónomas. Esta brecha entre amenaza formal y amenaza funcional es precisamente el espacio donde opera la VHE.

Guerra Híbrida Intencional vs. Vulnerabilidad Híbrida Estructural: la distinción conceptual

La distinción entre GHI y VHE constituye el aporte conceptual central de este trabajo. No es una distinción de grado sino de naturaleza, con consecuencias operativas directas.

La GHI se define por la presencia de un arquitecto estratégico: un actor que diseña, coordina y ejecuta una campaña multidominio con un objetivo estratégico definido, empleando deliberadamente la ambigüedad como ventaja operativa. La GHI es susceptible de ser respondida mediante disuasión, atribución y contraoperaciones. Los ejemplos paradigmáticos son la intervención rusa en Ucrania desde 2014 y la operación "La Compañía" del SVR en Argentina (Cariboni, 2026).

La VHE, en cambio, se produce cuando múltiples actores —el narcotráfico, grupos de desinformación, empresas que capturan regulación, dependencias tecnológicas no gestionadas— operan con lógicas propias sin coordinación entre sí, pero cuyos efectos convergen en el mismo resultado estratégico: un Estado con capacidad de respuesta degradada, una sociedad con confianza institucional erosionada. En la VHE no hay un arquitecto. Pero los efectos acumulados producen exactamente el mismo resultado que produciría una campaña deliberada.

Esta distinción tiene una implicación metodológica de primer orden: el analista que busca al "adversario" detrás de una VHE incurre en un error de encuadre que lo llevará a respuestas insuficientes. La VHE no tiene adversario

central al que disuadir. Tiene condiciones estructurales que solo pueden ser atacadas mediante resiliencia sistémica.

Es importante precisar que ambas condiciones no son mutuamente excluyentes. Un Estado puede enfrentar simultáneamente una GHI de origen externo —como la presión informacional del SVR sobre el ecosistema mediático rioplatense— y una VHE de origen estructural interno. El caso uruguayo ilustra precisamente esa coexistencia: la amenaza externa tiene arquitecto; la vulnerabilidad interna, no.

Dimensión	GHI — Guerra Híbrida Intencional	VHE — Vulnerabilidad Híbrida Estructural
Arquitecto	Sí — actor identificable con objetivo estratégico	No — convergencia de actores con objetivos parciales dispares
Coordinación	Deliberada — cadena de mando funcional	Ausente — efectos convergentes sin diseño
Objetivo final	Definido — geopolítico, económico o ideológico	No existe — cada actor persigue objetivos propios
Atribución	Posible con inteligencia suficiente	Estructuralmente difícil — no hay responsable central
Herramienta de respuesta	Disuasión, atribución, contraoperaciones	Resiliencia sistémica, inteligencia de patrones, cohesión social
Efecto estratégico	Erosión deliberada del Estado objetivo	Erosión no planificada pero funcionalmente equivalente
Reversibilidad	Alta si se neutraliza al actor	Baja — requiere transformaciones estructurales

Tabla 1. Comparación entre Guerra Híbrida Intencional (GHI) y Vulnerabilidad Híbrida Estructural (VHE)

Fuente: Elaboración propia a partir de Hoffman (2007), Murray & Mansoor (2012), Osinga & Sweijs (2021) y Mazarr (2015).

Arquitectura operativa híbrida

Convergencia de actores y saturación multidominio

Los actores involucrados en la guerra híbrida pueden ser estatales, paraestatales o no estatales, pero lo relevante es su capacidad de operar de forma coordinada aunque no necesariamente jerárquica. Esta descentralización

táctica permite negación plausible y adaptabilidad en tiempo real, dificultando la atribución y la respuesta institucional (Murray & Mansoor, 2012). La convergencia entre crimen organizado y actores estatales o paraestatales ha sido documentada desde el control territorial en México hasta la penetración logística en el Cono Sur. En el contexto de la VHE, esta convergencia no requiere siquiera comunicación entre actores: la estructura de incentivos del entorno genera sinergia sin coordinación.

La guerra híbrida se despliega a través de saturación multidominio: activación simultánea del dominio cinético (sabotajes, incursiones sin declaración formal), cibernético (ataques a infraestructuras críticas, espionaje digital), informacional (desinformación, manipulación narrativa), jurídico (lawfare) y económico (coerción encubierta). En el contexto de la VHE, estos dominios son activados de forma independiente por distintos actores, pero sus efectos se acumulan produciendo la misma saturación que caracteriza a la GHI.

Adaptabilidad contextual y tipología de adversarios

La guerra híbrida se mimetiza con el contexto, ajustando su intensidad según las vulnerabilidades del sistema objetivo. En Europa se manifiesta con componentes cinéticos visibles combinados con operaciones informacionales. En Iberoamérica, en cambio, opera predominantemente como VHE: crimen organizado con capacidad estratégica, ciberamenazas, manipulación narrativa y litigios instrumentales configuran una arquitectura de conflicto sin confrontación directa (Bartolomé, 2019; Lessing, 2021).

En el contexto específico de la VHE, emerge una categoría de actor adicional: los operadores jurídicos infiltrados —abogados, fiscales, jueces funcionalizados por el crimen organizado— que capturan el aparato normativo desde adentro, generando lo que puede denominarse lawfare criminal. En Uruguay, el intento más documentado ocurrió en 2025: al menos tres abogados defensores de organizaciones narcocriminales se presentaron al concurso de fiscales adscriptos, y uno de ellos superó la prueba, lo que fue advertido por la fiscal de Corte ante la Comisión de Asuntos Administrativos del Senado en abril de 2025 (Búsqueda, 2025). Semanas después, la vivienda de la fiscal fue objeto de un atentado con granada y disparos atribuido a estructuras vinculadas al narcotráfico (Infobae, 2025). La secuencia ilustra con precisión la doble presión —captura institucional y coerción violenta— característica del lawfare criminal.

Convergencia no coordinada: vectores sin arquitecto

La arquitectura operativa de la VHE difiere estructuralmente de la GHI en un aspecto fundamental: no requiere diseño. Los vectores que la componen —narcotráfico, desinformación, dependencia tecnológica, erosión institucional— no actúan de forma coordinada ni comparten objetivos estratégicos. Lo que los convierte en un problema de seguridad nacional no es su coordinación, sino su convergencia funcional: los efectos se acumulan sobre el mismo sustrato institucional.

Esta convergencia tiene una propiedad analítica crítica: es autorreforzante. La erosión institucional producida por el narcotráfico facilita la penetración de la desinformación; la polarización generada por la desinformación dificulta la respuesta legislativa frente al narcotráfico; la dependencia tecnológica no gestionada amplifica la exposición a ambos vectores. El ciclo es autosostenido y no puede interrumpirse neutralizando a un actor central. Un Estado que responde a la VHE como si fuera GHI puede incurrir en securitización regresiva, instrumentalizando el discurso de amenaza para justificar medidas que erosionan los derechos fundamentales que debería proteger (Kloetzer, 2021).

Manifestaciones en Iberoamérica y Uruguay

Presión híbrida regional en entornos de paz formal

Iberoamérica enfrenta una presión híbrida estructural que no se presenta como guerra formal pero opera como conflicto persistente. El crimen organizado con capacidad estratégica actúa como actor híbrido funcional en la región. Las ciberamenazas han escalado desde el espionaje técnico hacia el sabotaje digital. La guerra informacional se ha convertido en componente estructural del conflicto híbrido regional. En el plano de la GHI con origen externo, la intervención de actores extrarregionales como Irán —a través de Hezbollah y canales mediáticos como Hispan TV— y de Rusia confirman que las amenazas no se limitan al plano doméstico.

La operación "La Compañía", expuesta en abril de 2026, documentó un presupuesto de 283.000 dólares para publicar al menos 250 artículos en más de 20 medios digitales argentinos, con el objetivo de desacreditar al gobierno mientras Argentina profundizaba su respaldo a Ucrania (Cariboni, 2026). La relevancia para Uruguay es inmediata: el mismo ecosistema lingüístico, cultural y mediático. El modelo de distribución —portales digitales de apariencia

legítima, amplificación por redes sociales— es directamente reproducible en el contexto uruguayo.

El caso uruguayo: presión híbrida y VHE

Uruguay no enfrenta guerra declarada, pero sí presión híbrida persistente y condiciones de VHE. El crimen organizado transnacional utiliza nodos logísticos locales —puertos, zonas francas, rutas estratégicas— para operaciones ilícitas de alcance regional. El intento de infiltración en el Ministerio Público (caso Ferrero, 2025) evidencia que esta presión ha alcanzado el nivel de captura institucional. Las ciberamenazas afectan sistemas administrativos y financieros: en 2024 el CERTUY registró 14.264 incidentes contra el Estado —casi el triple que en 2023—, incluyendo el ataque de ransomware contra la Intendencia de Paysandú que bloqueó por meses la liquidación de sueldos y los sistemas de cobro (CERTUY, 2025). La desinformación documentada durante el proceso electoral de 2024 —27 incidentes identificados por AFP Factual— constituye evidencia de guerra cognitiva en operación activa (Montero et al., 2025).

La vulnerabilidad normativa merece atención específica. La propuesta inicial en el proyecto de presupuesto 2025 de eliminar la intervención judicial para el levantamiento del secreto bancario por parte de la DGI ilustra el dilema entre respuesta funcionalmente necesaria frente al lavado de activos y riesgo de securitización regresiva. Ante la presión de la oposición parlamentaria y el sector bancario, el Gobierno acordó un esquema de "silencio positivo": si el juez no se expide en diez días hábiles, la solicitud se considera aprobada (El País, 2025). El desenlace fue más equilibrado que la propuesta original, pero el propio debate ilustra la tensión estructural que la VHE introduce: la presión para responder puede generar respuestas que reproducen el daño que se pretendía evitar.

La convergencia de estos tres vectores —captura institucional, ciberamenazas y desinformación— sobre el mismo sustrato estatal uruguayo ilustra con precisión el mecanismo de la VHE: ninguno de los actores involucrados coordinó con los demás —al menos no hay indicios verificables de ello—, pero sus efectos se acumulan sobre la misma capacidad de respuesta del Estado. Uruguay no es un caso excepcional en la región sino un caso revelador: su perfil —Estado pequeño con alta institucionalidad relativa, nodo logístico marítimo de alcance regional y ecosistema mediático compartido con Argentina— lo convierte en un punto de entrada privilegiado para vectores que operan a escala del Cono Sur. La comparación sistemática entre el perfil de

vulnerabilidad uruguayo y el de otros Estados de la región con distintas combinaciones de fortaleza institucional y exposición híbrida constituye una agenda de investigación que excede los límites de este trabajo pero que los hallazgos aquí presentados fundamentan.

La guerra cognitiva como vector singular

Por qué la guerra cognitiva exige tratamiento diferenciado

Dentro del espectro de vectores que componen tanto la GHI como la VHE, la guerra cognitiva (GC) ocupa una posición singular. No es simplemente un instrumento más de la guerra híbrida: es el vector que opera con mayor eficacia en ausencia de arquitecto central, que produce los efectos de menor reversibilidad y que resulta prácticamente imposible de atribuir con medios convencionales. Estas características la convierten en el vector más peligroso de la VHE.

La GC ha emergido como el sexto dominio autónomo del conflicto contemporáneo, situando el cerebro humano como blanco principal. A diferencia de las operaciones psicológicas (PSYOPS, por sus siglas en inglés), la GC no apunta a lo que los individuos piensan, sino a cómo piensan, alterando los mecanismos de procesamiento y decisión (NATO ACT, 2023; Claverie & du Cluzel, 2021). Su característica más perturbadora es que convierte al objetivo en agente activo de su propia manipulación. El 4. ° Informe FIMI de la EEAS (2026) confirmó 540 incidentes globales solo en 2025, con el empleo de inteligencia artificial creciendo un 259% respecto al año anterior.

Taxonomía de la guerra cognitiva por capas

La Capa 1 —informativa— incluye desinformación, ultra falsificaciones (deepfakes), redes de agentes automatizados (bots), plataformas con algoritmos de Estado (TikTok) y ecosistemas de medios falsos (Doppelgänger). Produce efectos con reversibilidad alta si se actúa oportunamente.

La Capa 2 —conductual— incluye microfocalización cognitiva con inteligencia artificial, PSYOPS digitales personalizadas e ingeniería del sesgo de largo plazo. Opera en zonas grises normativas con marcos jurídicos aún incompletos.

La Capa 3 —biofísica o NeuroStrike— designa el empleo de tecnologías no cinéticas diseñadas para dañar funciones neurológicas sin rastro visible ni atribuible. El "Síndrome de La Habana", reportado entre personal diplomático y

de inteligencia estadounidense en decenas de países, constituye la evidencia más documentada: un comité de expertos convocado por las Academias Nacionales de Ciencias de EE. UU. concluyó que la energía dirigida de microondas era la explicación más plausible de los síntomas. En paralelo, informes de analistas de fuentes abiertas atribuyen al Ejército Popular de Liberación chino un programa deliberado de armas NeuroStrike —energía dirigida, infrasonido e interfaces cerebro-computadora— concebido como componente de su estrategia de guerra asimétrica (Eads et al., 2023). Corresponde señalar que esta evidencia es preliminar y objeto de controversia académica; su valor analítico reside en documentar una dirección de desarrollo, no capacidades confirmadas. La Capa 3 produce efectos con reversibilidad baja o nula y vacíos graves en el Derecho Internacional Humanitario.

La guerra cognitiva en el contexto de la VHE

La GC es el vector de la VHE por excelencia, precisamente porque no requiere coordinación central. Una red de desinformación que opera por incentivos económicos puede producir los mismos efectos cognitivos que una operación de GC estatal deliberada. Los algoritmos de las plataformas digitales, diseñados para maximizar la interacción mediante amplificación de contenido emocionalmente activante, operan como multiplicadores gratuitos de cualquier narrativa divisiva.

En el caso uruguayo, la GC ya opera en Capa 1 con evidencia documentada: desinformación electoral 2024, operación rusa "La Compañía" en el ecosistema mediático rioplatense, presencia de Hispan TV como canal iraní con línea editorial antioccidental. La ausencia de doctrina formal sobre GC en las Fuerzas Armadas uruguayas implica que cuando un oficial o institución son objeto de una operación de influencia cognitiva, carecen del marco conceptual para reconocerla.

Implicancias estratégicas e institucionales

Reconfiguración doctrinal y vulnerabilidades estructurales

La guerra híbrida exige complementar y superar el paradigma convencional de defensa centrado en amenazas externas, territoriales y militares. La guerra convencional no ha desaparecido como fenómeno estratégico: la experiencia de Ucrania y los conflictos en el Indo-Pacífico lo confirman. Pero ese paradigma resulta insuficiente por sí solo cuando las amenazas más inmediatas al Estado uruguayo no provienen de un adversario

convencional sino de la convergencia no coordinada de vectores híbridos. El Decreto 371/020 reconoce parcialmente esta reconfiguración, pero su implementación requiere una traducción operativa que articule capacidades multidominio, protocolos interagenciales y marcos normativos flexibles.

Las vulnerabilidades estructurales de Uruguay frente a la presión híbrida se evidencian en: la escasa capacidad de atribución frente a ciberincidentes, en un contexto donde los 14.264 incidentes registrados en 2024 superan ampliamente las capacidades de respuesta del Estado (CERTUY, 2025); la brecha entre el marco normativo de ciberseguridad —progresivamente fortalecido con la Ley N.º 20.212 (2023), la Ley N.º 20.327 (2024) y el Decreto N.º 66/025 (2025)— y la capacidad operativa real para contener las amenazas; la limitada coordinación interagencial entre defensa, inteligencia, justicia, relaciones exteriores y sociedad civil, evidenciada por la proliferación de estructuras con mandatos superpuestos en el dominio del crimen organizado transnacional —CODENA, SILCON, SENACLAFT, ESMAD y la Comisión de la Ley 19.513— sin protocolos formales de división de trabajo (Caubarrere Diab, 2026; Kettl, 2003; Bardach, 1998); la debilidad de los protocolos de respuesta frente a campañas de desinformación; y la ausencia de doctrina formal sobre guerra cognitiva.

Resiliencia institucional y el riesgo de securitización regresiva

La resiliencia institucional no debe entenderse como mera capacidad de recuperación, sino como arquitectura estratégica de anticipación, adaptación y continuidad operativa frente a presiones híbridas. Para la VHE, la resiliencia no es complementaria sino principal: en ausencia de adversario central, la única respuesta estructuralmente eficaz es construir un sistema capaz de funcionar bajo presión simultánea de múltiples vectores sin colapso institucional.

La guerra híbrida obliga al Estado a desarrollar mecanismos de control más sofisticados, pero esta necesidad plantea un dilema estratégico central: cómo proteger a la ciudadanía frente a amenazas difusas sin vulnerar los derechos individuales que constituyen la base de la seguridad humana. El fenómeno de la securitización regresiva —derivado de la teoría de la securitización (Buzan, Wæver & de Wilde, 1998), designa la construcción discursiva de amenazas que habilita medidas excepcionales sin control democrático ni proporcionalidad jurídica— es un riesgo real en el contexto iberoamericano (Kloetzer, 2021).

Herramientas diferenciadas de respuesta

Esta sección constituye el núcleo operativo del aporte doctrinal. La distinción GHI/VHE no tiene valor si no se traduce en herramientas de respuesta diferenciadas.

Frente a la GHI: las herramientas son de naturaleza defensivo-ofensiva y requieren capacidades de atribución, disuasión y respuesta proporcional. La atribución debe operar con estándares de certeza política —no exclusivamente penal—: el umbral es demostrar al adversario que fue detectado, sin necesariamente divulgar fuentes ni métodos. La cooperación regional e internacional es condición estructural: ningún Estado iberoamericano puede atribuir, responder ni coordinar eficazmente por sí solo frente a una GHI de origen estatal externo.

Frente a la VHE: las herramientas de atribución de actores y disuasión son insuficientes como respuesta exclusiva porque no existe adversario central. La inteligencia de patrones de convergencia es la herramienta analítica central: detectar la acumulación y sinergia de daños producidos por actores dispares sobre el mismo sustrato institucional. La cohesión social como política activa es probablemente la herramienta más contraintuitiva para el ámbito de defensa, pero la más eficaz frente a la VHE: esta prospera en sociedades fragmentadas y con baja confianza institucional. Implementar esta política implica concretamente, entre otros: programas de alfabetización mediática integrados al currículo educativo, mecanismos de participación ciudadana en la defensa nacional, y transparencia institucional como herramienta activa de cohesión —tal como demuestran los modelos finlandés y taiwanés.¹

Frente a la GC: la doctrina formal de defensa cognitiva, articulada por capas de intensidad y niveles de conducción, es el instrumento habilitador. Uruguay carece actualmente de esa doctrina. El sistema estatal debe determinar qué actor está en mejores condiciones de liderar su producción, integrada en el marco DOTMLPF-I (*Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities – Interoperability*), estándar de planificación de capacidades cuyas dimensiones equivalen a doctrina, organización, adiestramiento, material, liderazgo, personal, infraestructura e

¹ El modelo finlandés de seguridad integral (Comprehensive Security) articula la participación ciudadana en la defensa nacional con la alfabetización mediática como componente estructural.

interoperabilidad, de modo que la defensa cognitiva no quede como declaración doctrinal aislada sino como capacidad institucional completa.²

La formación en resiliencia cognitiva a todos los niveles de la cadena de comando es la contramedida de mayor impacto y menor costo disponible. Dos técnicas concentran la evidencia de eficacia: los juegos de guerra cognitivos — ejercicios de simulación en los que los participantes enfrentan campañas de manipulación controladas para entrenar su detección y respuesta— y la inoculación psicológica, que expone preventivamente a las personas a versiones debilitadas de las técnicas de manipulación para generar resistencia cognitiva ante su versión real, de modo análogo a una vacuna (Lewandowsky & van der Linden, 2021).

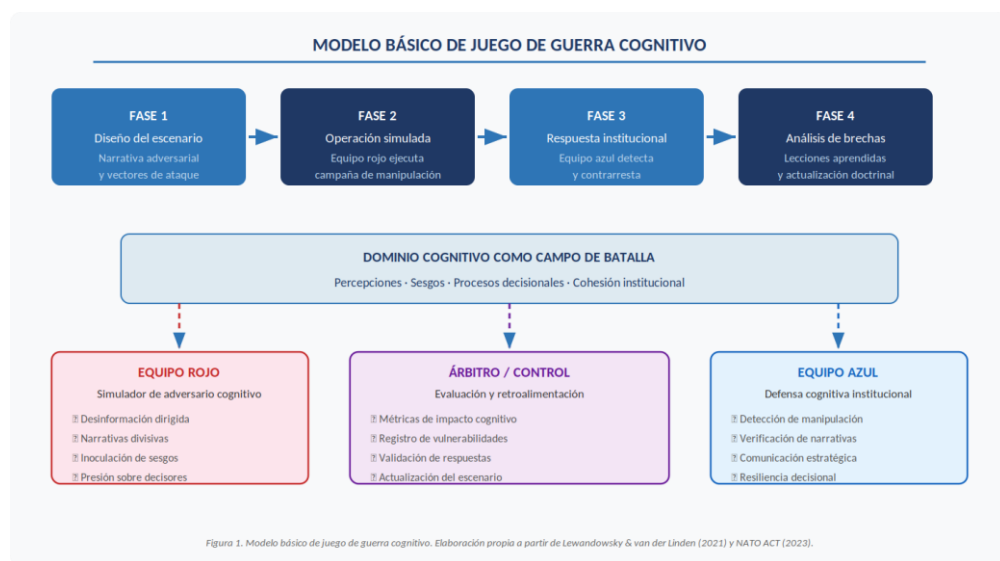


Figura 1. Modelo básico de juego de guerra cognitivo.

Fuente: Elaboración propia a partir de Lewandowsky & van der Linden (2021) y NATO ACT (2023).

² DOTMLPF-I proviene del marco de planificación de capacidades de la OTAN y los Joint Chiefs of Staff de EE. UU.: Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities – Interoperability. En el contexto uruguayo, su adopción no sustituye los marcos doctrinales nacionales vigentes sino que los complementa con una estructura de análisis que permite identificar brechas de capacidad de forma sistemática en cada dimensión.

El concepto de cadena de destrucción aplicado a FIMI constituye la orientación estratégica más relevante del 4. ° Informe EEAS (2026): en lugar de responder únicamente a los productos de una operación de manipulación informacional —los artículos, los videos, los mensajes viralizados—, este enfoque propone atacar las infraestructuras que la sostienen: las redes de financiamiento, los servidores de distribución, los intermediarios que conectan al operador con los medios amplificadores. Es la diferencia entre apagar incendios y cortar el suministro de combustible.

Conclusiones

La guerra híbrida se ha consolidado como la forma dominante de conflicto en el siglo XXI, pero su conceptualización clásica es insuficiente para describir la situación que enfrenta la mayoría de los Estados iberoamericanos. La principal contribución de este trabajo es la distinción formal entre la GHI y la VHE, y la demostración de que ambas exigen herramientas de respuesta cualitativamente distintas.

La VHE se produce cuando la convergencia no coordinada de vectores de daño genera efectos funcionalmente equivalentes a los de una campaña híbrida deliberada, sin que ningún actor los haya orquestado. Un Estado que responde a la VHE como si fuera GHI —buscando al adversario central, aplicando lógica de atribución clásica— no solo fracasa en su respuesta, sino que puede incurrir en securitización regresiva, reproduciendo el daño que pretendía evitar.

Los modelos VICA, BANI y CAVE no son marcos paralelos sino capas complementarias de descripción del mismo fenómeno. El modelo CAVE añade la especificidad tecnológica que los modelos anteriores no capturan: la convergencia de IoT, inteligencia artificial y conectividad genera una vulnerabilidad estructural que amplifica todos los demás vectores de la VHE y que solo puede responderse con soberanía regulatoria y resiliencia tecnológica activa.

La guerra cognitiva es el vector singular más peligroso dentro de la VHE por tres razones concurrentes: opera sin coordinación central; produce efectos de muy baja reversibilidad; y actúa como amplificador de todos los demás vectores. Los 540 incidentes FIMI globales documentados por el EEAS en 2025 y la operación "La Compañía" sobre el ecosistema mediático rioplatense confirman que la amenaza no solo no cede sino que se acelera.

Uruguay enfrenta una VHE en curso. El intento de captura institucional del Ministerio Público (2025), los 14.264 incidentes cibernéticos registrados en

2024, la desinformación electoral documentada y la ausencia de doctrina formal sobre guerra cognitiva constituyen vectores activos de vulnerabilidad estructural. El país posee al mismo tiempo activos de resiliencia que el propio análisis precedente permite identificar: el marco normativo de ciberseguridad se ha fortalecido progresivamente (Ley N.º 20.212, 2023; Ley N.º 20.327, 2024); la vocación multilateral se expresa en décadas de participación en misiones de paz y en la membresía activa en el CICTE y el MERCOSUR; y el hecho de que el intento de infiltración en el Ministerio Público fuera detectado, denunciado ante el Parlamento y rechazado institucionalmente es en sí mismo evidencia de resiliencia democrática operativa. La distancia entre vulnerabilidades y activos es el espacio que la política estratégica debe ocupar; cuantificar esa distancia y compararla con otros casos del Cono Sur constituye una línea de investigación que este trabajo abre sin pretender cerrar.

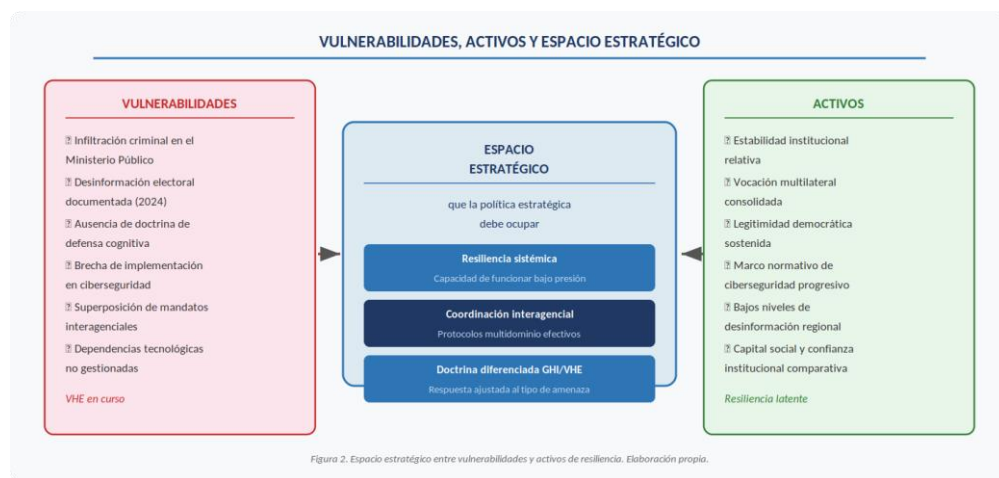


Figura 2. Espacio estratégico entre vulnerabilidades y activos de resiliencia.

Fuente: Elaboración propia.

La respuesta requiere visión estratégica, coordinación interagencial, resiliencia sistémica y una doctrina que distinga con precisión entre los tipos de amenaza y las herramientas que cada uno exige, sin sacrificar los principios democráticos que sustentan la legitimidad del Estado. La distinción GHI/VHE no es un aporte exclusivamente local: cualquier Estado iberoamericano con perfil institucional similar —pequeño o mediano, alta exposición a crimen organizado transnacional, dependencia tecnológica no gestionada y ecosistema mediático

permeable— puede aplicar este marco para diagnosticar su propia vulnerabilidad estructural y diseñar respuestas diferenciadas. Lo que este artículo aporta a la comunidad académica estratégica de la región es precisamente eso: no una solución, sino un instrumento analítico para formular las preguntas correctas.

Recomendaciones estratégicas

Las siguientes recomendaciones se derivan directamente de las vulnerabilidades identificadas en el análisis precedente y se organizan según el tipo de amenaza que atienden.

Bloque A — Frente a la Guerra Híbrida Intencional (GHI)

- Reconocer formalmente la GHI como amenaza estructural en los documentos estratégicos nacionales, incorporando su tipología de actores, dominios operativos y efectos acumulativos.
- Desarrollar capacidades de atribución híbrida con estándares de certeza política —no exclusivamente penal—, combinando evidencia técnica, trazabilidad narrativa y análisis jurídico.
- Establecer protocolos de coordinación interagencial para escenarios de GHI que integren defensa, inteligencia, justicia, relaciones exteriores y seguridad pública en cadenas de decisión preacordadas.
- Promover acuerdos multilaterales sobre ciberseguridad y lucha contra el crimen organizado, canalizados a través de la Conferencia de Ministros de Defensa de las Américas, el CICTE y el MERCOSUR.
- Iniciar la planificación de migración progresiva hacia criptografía poscuántica (PQC) siguiendo los estándares NIST 2024³, en respuesta a la amenaza de "cosechar ahora, descifrar después" identificada en el análisis del entorno CAVE.

Bloque B — Frente a la Vulnerabilidad Híbrida Estructural (VHE)

- Formalizar el concepto de VHE en la doctrina de defensa nacional, diferenciándolo de la GHI y estableciendo su propia lógica de respuesta basada en resiliencia sistémica.

³ NIST (National Institute of Standards and Technology) es el organismo federal de EE. UU. encargado de desarrollar estándares tecnológicos. En 2024 publicó los primeros estándares de criptografía poscuántica, diseñados para resistir el poder de cómputo de las computadoras cuánticas

- Desarrollar inteligencia de patrones de convergencia: capacidad analítica específica para detectar la acumulación y sinergia de daños producidos por actores dispares sobre el mismo sustrato institucional.
- Implementar una política activa de cohesión social como instrumento de seguridad nacional, incluyendo alfabetización mediática, transparencia institucional y participación ciudadana en la defensa nacional.
- Revisar los procesos de selección institucional y el marco legal aplicable en el Ministerio Público, el Poder Judicial y otros organismos críticos para detectar y prevenir intentos de captura normativa por parte del crimen organizado, identificando explícitamente los impedimentos normativos que deben superarse para garantizar esa revisión.
- Garantizar que toda medida de respuesta frente a la VHE esté sujeta a control judicial, trazabilidad institucional y supervisión democrática, para prevenir la securitización regresiva.

Bloque C — Frente a la Guerra Cognitiva

- Determinar qué actor del sistema estatal está en mejores condiciones de liderar la producción de la primera doctrina formal de defensa cognitiva, articulada por capas de intensidad y niveles de conducción, integrada en el marco DOTMLPF-I.
- Incorporar un módulo curricular obligatorio de resiliencia cognitiva en todos los niveles educativos de las Fuerzas Armadas, las fuerzas policiales y otras instituciones estatales con responsabilidades en seguridad, incluyendo juegos de guerra cognitivos e inoculación psicológica frente a desinformación.
- Regular las plataformas con algoritmos de Estado extranjero como asunto de seguridad nacional, siguiendo el modelo DSA europeo y el modelo taiwanés, procurando el mínimo de restricción a la libertad de expresión y las demás libertades individuales.
- Implementar plataformas de monitoreo narrativo OSINT adaptadas al ecosistema lingüístico del Río de la Plata, con capacidad de detectar patrones de manipulación en tiempo real.
- Establecer cooperación bilateral en defensa cognitiva con Estonia, Finlandia y Taiwán, países con mayor madurez doctrinal en este dominio.

Referencias

Fuentes doctrinales y académicas — Conflicto híbrido y seguridad

- Bartolomé, M. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (25), 8–23. <https://doi.org/10.17141/urvio.25.2019.4249>
- Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.
- Kloetzer, B. (2021). *Hybrid Threats and the Law*. DCAF.
- Lessing, B. (2021). Conceptualizing Criminal Governance. *Perspectives on Politics*, 19(3), 854–873. <https://doi.org/10.1017/S1537592720001243>
- Mazarr, M. J. (2015). *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. US Army War College Press.
- Murray, W., & Mansoor, P. R. (Eds.). (2012). *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge University Press.
- Osinga, F., & Sweijs, T. (Eds.). (2021). *Deterrence in the 21st Century: Insights from Theory and Practice*. T.M.C. Asser Press. <https://doi.org/10.1007/978-94-6265-419-8>

Fuentes doctrinales y académicas — Guerra cognitiva y desinformación

- Bardach, E. (1998). *Getting Agencies to Work Together: The Practice and Theory of Managerial Craftsmanship*. Brookings Institution Press.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner.
- Cascio, J. (2021). *Facing the Age of Chaos*. Medium. <https://medium.com/@cascio/facing-the-age-of-chaos-b00687b1f51d>
- Claverie, B., & du Cluzel, F. (2021). *The Cognitive Warfare Concept*. NATO Allied Command Transformation Innovation Hub.
- Dunlap, C. J. (2008). Lawfare Today: A Perspective. *Yale Journal of International Affairs*, 3(1), 146–154.

- Eads, L. J., Clarke, R., & Lin, X. S. (2024). The Evolution of Cognitive Warfare: NeuroStrike Capabilities and the Strategic Role of Infrasound Weapons. CCP BioThreats Initiative. <https://www.ccpbiothreats.com>
- Gómez-De Luca, P. M. (2025). Preparación militar y ciberseguridad en la era de los drones y la IA: ¿Oportunidad o amenaza? En Tomo XIV del Libro de la ACDIA, XXVI Conferencia de Directores de Colegios de Defensa Iberoamericanos (CDCDIA), IAEE, Asunción, Paraguay (pp. 355–ss.).
- Kettl, D. F. (2003). Contingent Coordination: Practical and Theoretical Puzzles for Homeland Security. *American Review of Public Administration*, 33(3), 253–277.
- Lewandowsky, S., & van der Linden, S. (2021). Countering Misinformation and Fake News Through Inoculation and Prebunking. *European Review of Social Psychology*, 32(2), 348–384. <https://doi.org/10.1080/10463283.2021.1876983>
- Montero, S., Rodríguez-Virgili, J., & Fernández, C. B. (2025). La desinformación en las campañas electorales: el caso uruguayo 2024 en el contexto hispanoamericano. *Revista de Comunicación Política*, 7, e250708. <https://doi.org/10.29105/rcp.v7i1.84>
- NATO Allied Command Transformation (ACT). (2023). Cognitive Warfare: The Battle for the Brain. NATO.

Fuentes institucionales y normativas

- CERTUY — Centro Nacional de Respuesta a Incidentes de Seguridad Informática. (2025). Estadísticas de incidentes 2024. AGESIC. <https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas>
- Consejo de la Unión Europea. (2026, marzo 16). Conclusiones sobre el avance de la capacidad de la UE para contrarrestar amenazas híbridas. <https://consilium.europa.eu>
- EEAS — European External Action Service. (2026). 4th FIMI Threat Report. <https://eeas.europa.eu>
- Gerasimov, V. (2013). The Value of Science is in the Foresight. *Military-Industrial Courier*.

NIST. (2024). Post-Quantum Cryptography Standards. National Institute of Standards and Technology.

Uruguay. (2020). Decreto 371/020 — Política de Defensa Nacional 2020–2025. Presidencia de la República.

Fuentes periodísticas y de prensa especializada

Búsqueda. (2025, octubre 9). Al menos tres abogados de narcos concursaron para ser fiscales; hay preocupación en Fiscalía y el sistema político. <https://www.búsqueda.com.uy/informacion/al-menos-tres-abogados-narcos-concursaron-ser-fiscales-hay-preocupacion-fiscalia-y-el-sistema-politico-n5405278>

Cariboni, D. (2026, 2 de abril). Leña al fuego: La campaña rusa para influir en los medios de comunicación de Argentina. openDemocracy. <https://www.opendemocracy.net/es/argentina-rusia-propaganda-medios-periodismo-milei-ucrania-putin-trump-prigozhin/>

El País. (2025, septiembre 25). Proyecto de Presupuesto flexibiliza el secreto bancario: la DGI podrá acceder a información sin pasar por juez. <https://www.elpais.com.uy>

Infobae. (2025, septiembre 29). Atentado contra la fiscal general de Uruguay: lanzan granada y disparos contra su vivienda. <https://www.infobae.com>

Fuente del autor

Caubarrere Diab, P. S. (2026). Guerra híbrida y narcoterrorismo en Uruguay. El Soldado. Revista del Centro Militar, LII (210).

