

Defensa persistente avanzada

Un modelo multinivel de ciberdefensa para latinoamérica

DOI: 10.29236/sistemas.n180a5

Resumen

El ciberespacio ha evolucionado hacia un entorno de competencia geopolítica permanente, lo que exige transitar de una defensa estática hacia la Defensa Persistente Avanzada (DPA). No obstante, en América Latina, la implementación de este paradigma enfrenta obstáculos estructurales derivados de la fragmentación institucional y la posición de los Estados respecto a la “línea de pobreza cibernética”. Este concepto, adaptado del nivel organizacional al nivel Estatal, define un umbral de suficiencia basado en cuatro brechas: presupuesto, talento, tecnología e influencia. Este estudio propone el modelo DPA-LAC, cuya innovación radica en una secuencia de implementación invertida que prioriza el “componente cero” o base mínima de suficiencia nacional. A través de un análisis comparado de Brasil, Chile, México y Colombia, se evidencia una marcada dispersión de capacidades que imposibilita la integración regional uniforme. Se concluye que el éxito estratégico regional reside en la elevación de la base mínima común de capacidades cibernéticas y en la resiliencia como estrategia defensiva viable y costo-efectiva para la región ante sus limitaciones presupuestarias.

Palabras clave: defensa persistente avanzada, línea de pobreza cibernética, ciberdefensa, América Latina, resiliencia estratégica

Introducción

El ciberespacio dejó de comportarse como un dominio de crisis coyunturales para consolidarse como un escenario de competencia continua. Buchanan (2020) documenta que los ataques cibernéticos no se materializaron en el equivalente digital de una guerra nuclear, sino en una forma de baja intensidad y alta frecuencia de la competencia geopolítica, en la que los Estados moldean el entorno estratégico mediante espionaje, sabotaje y desestabilización antes que mediante señalización coercitiva. Este contexto desplaza el eje del debate: si la agresión es permanente, la defensa no puede ser intermitente.

De este escenario surge la Defensa Persistente Avanzada (DPA), concepto formulado por Abdul Rahman (2026) como visión complementaria de la amenaza persistente avanzada. En su formulación original, la DPA articula tres funciones en el plano organizacional: recolección de inteligencia e intercambio de información, monitoreo activo para la cacería de amenazas y respuesta orientada a mitigar el impacto, y las proyecta hacia los planos nacional y regional, exigiendo coherencia interna de los enfoques estatales y coordinación entre defensores civiles y militares. El caso que sustenta la propuesta es el del Sudeste Asiático, con Singapur como refe-

rente de madurez y las normas internacionales sobre comportamiento responsable de los Estados como marco común.

La propuesta, sin embargo, descansa sobre precondiciones que no son universales. La DPA supone un proceso de integración digital formalizado, la existencia de un Estado fuerte capaz de exportar capacidades hacia sus vecinos y arquitecturas regionales de ciberseguridad ya operativas. América Latina no reúne ninguna de las tres. El problema no es solo de rezago tecnológico: es de arquitectura institucional y de distribución desigual de capacidades entre Estados que comparten un mismo espacio de exposición.

Este artículo sugiere que la variable explicativa de esa asimetría es la posición estructural de los Estados respecto de la línea de pobreza cibernética. El concepto fue acuñado por Nather y Ellis (2013) para designar el umbral por debajo del cual una organización no puede defenderse eficazmente de los incidentes cibernéticos, y fue sistematizado posteriormente por el Atlantic Council (2022) en términos de cuatro brechas de recursos: presupuesto, experticia, capacidad tecnológica e influencia para obtener apoyo externo. Su formulación es organizacional; su traslado al nivel estatal constituye una extensión

analítica que este estudio asume de manera explícita para plantear una propuesta de defensa persistente.

El argumento se despliega en cuatro movimientos. Primero, la extensión de escala del umbral, que permite pensar la capacidad soberana en términos de suficiencia defensiva. Segundo, el diagnóstico regional por dispersión antes que por déficit uniforme. Tercero, la demostración de que la secuencia descendente del modelo original resulta inviable en contextos de alta variación de capacidades, lo que obliga a invertirla. Cuarto, la reformulación del criterio de éxito, que abandona la paridad de capacidades y adopta la elevación de la base mínima requerida, esto es mejoramiento de las capacidades cibernéticas básicas disponibles.

Metodológicamente, el trabajo es de carácter teórico-analítico con aplicación a un caso. Construye un modelo conceptual, denominado DPA-LAC, a partir de la genealogía doctrinal de la persistencia cibernética, y lo somete a contraste mediante el análisis del caso colombiano comparado con Brasil, Chile y México, seleccionados por representar posiciones distintas respecto del umbral de pobreza cibernética. El texto se organiza iniciando con la evolución del concepto de defensa persistente avanzada (DPA), luego con la propuesta de modelo de DPA, seguidamente el caso aplicado a Colombia, la discu-

sión de ventajas y limitaciones del modelo, terminado con algunas conclusiones.

Defensa persistente avanzada: origen y evolución del concepto

La genealogía de la DPA no comienza en 2026. Su antecedente doctrinal directo es la noción de persistencia cibernética formulada por Nakasone (2019), quien argumentó que el concepto estratégico de una fuerza de respuesta: mantener capacidades en reserva para responder después del hecho, resultaba análogo a la doctrina naval anterior a 1945 y cedía la iniciativa estratégica a adversarios dispuestos a operar de manera continua. La alternativa propuesta fue la persistencia: competir globalmente y a escala, operar por debajo del umbral del uso de la fuerza y defender hacia adelante, sustituyendo relaciones transaccionales con el sector privado por colaboración operativa continua.

Esta doctrina fue objeto de una revisión crítica por parte de Hurel y Mott (2025). Los académicos identifican cinco escuelas en el debate sobre disuasión cibernética: la analogía nuclear, el escepticismo, el compromiso persistente, la resiliencia sobre la disuasión y la disuasión transdominio. Su análisis señala que los supuestos de la disuasión clásica, señalar umbrales precisos, atribuir con rapidez y demostrar represalia creíble, rara vez se satisfacen en el ciberespacio, donde los adversarios explotan la

ambigüedad de los umbrales y externalizan operaciones a intermediarios. La escuela de la resiliencia se distancia de la centralidad de la disuasión y propone construir sistemas capaces de absorber, adaptarse y recuperarse con disrupción mínima, negando al atacante el efecto buscado.

Ese giro hacia la resiliencia adquiere una orientación organizacional en Nobrega et al. (2024), quienes proponen la noción de ciberdefensa integral. Su argumento central es que la exposición se ha ampliado por la conectividad extendida y que la respuesta exige sincronizar práctica y teoría a través de múltiples actores: profesionales de seguridad, usuarios, reguladores y proveedores, en lugar de confinar la defensa al perímetro técnico de cada organización. La DPA hereda de esta corriente su carácter multiactor y se aparta de la separación entre defensa técnica y gobernanza institucional.

Un cuarto pilar es la atribución. Rid y Buchanan (2015) establecieron que la atribución no es un problema binario de identificación técnica, sino un proceso graduado que combina evidencia forense, análisis operacional y juicio político, y cuyo resultado admite grados de confianza antes que certezas. Hedling y Ördén (2025) extienden el argumento al terreno político: distinguen entre atribución pública, que impone costos sociales y señala capacidad y resolución, y no atribu-

ción, entendida como decisión deliberada de no asignar responsabilidad pese a disponer de evidencia. La atribución deja así de ser un acto técnico para constituirse en instrumento de política exterior cuyo uso depende de la resiliencia social percibida.

El cuarto vector proviene de la inteligencia artificial y altera los supuestos del modelo. Maschmeyer (2026) sostiene que existe una brecha de automatización entre ofensiva y defensiva: la ofensiva depende de la creatividad y del engaño, tareas en las que los modelos actuales rinden mal, mientras que la defensiva depende del reconocimiento de patrones, donde sobresalen. La consecuencia es que la defensiva obtiene ganancias superiores de eficiencia y eficacia, y que la brecha se ensancha a medida que aumentan las apuestas. Dotterer et al. (2026) matizan esta conclusión al identificar un déficit de control: la automatización ofensiva puede ser desplegada por actores individuales con infraestructura mínima, mientras que la automatización defensiva exige integración, validación y coordinación organizacional extensas. Esta asimetría de requisitos institucionales es clave para las reflexiones de este estudio.

Rosen y Kraprayoon (2026) advierten que los agentes autónomos representan una categoría nueva de amenaza para la seguridad nacional, y observan que las institu-

ciones que sostienen infraestructura crítica suelen operar con sistemas obsoletos, recursos insuficientes y experticia interna limitada. El Instituto Nacional de Ciberseguridad (2026) traduce ese diagnóstico a medidas concretas, subrayando que el acortamiento de los tiempos de detección de vulnerabilidades exige acelerar los procesos de actualización y parches, para los cuales muchas organizaciones no están preparadas.

La dimensión cognitiva completa la revisión. Whyte et al. (2020) muestran que las campañas de guerra de información habilitadas por medios cibernéticos operan bajo una lógica de involucramiento antes que de disrupción indiscriminada, y que su conceptualización sigue siendo insuficiente en la literatura sobre disuasión. Jaidka et al. (2025) documentan cómo la inteligencia artificial generativa reduce las barreras para producir y difundir desinformación, dificulta la atribución de fuentes y erosiona la confianza incluso hacia medios reconocidos, lo que sitúa la resiliencia informacional como componente de la defensa y no como asunto separado.

La convergencia de estas siete corrientes permite formular la DPA no como una innovación aislada, sino como la materialización representativa de un desplazamiento acumulado. El movimiento va de la respuesta a la persistencia (Nakasone, 2019), de la disuasión a la

resiliencia (Hurel y Mott, 2025), del perímetro técnico a la coordinación multiactor (de Nobrega et al., 2024), de la atribución técnica a la atribución política (Hedling y Ördén, 2025; Rid y Buchanan, 2015) y de la presunta ventaja ofensiva a la ventaja defensiva estructural condicionada (Dotterrer et al., 2026; Maschmeyer, 2026). La Tabla 1 sintetiza esta genealogía. Lo que la DPA aporta es la integración de estos desplazamientos en un mismo marco y su proyección a los planos nacional y regional. Lo que no aporta es una teoría de las condiciones materiales que hacen posible esa integración, y es precisamente ese vacío el que la línea de pobreza cibernética permite ocupar.

Finalmente, la dimensión material. Kajander et al. (2025) evidencian que los requisitos de ciberseguridad para sistemas de armas permanecen fragmentados y en gran medida clasificados, y que no existe una disposición explícita de derecho internacional que los imponga. Gopal Chari (2025) sitúa este vacío en el marco del desacoplamiento de cadenas de suministro y de la búsqueda de soberanía tecnológica, señalando que las economías emergentes de África y América Latina enfrentan obstáculos considerables para acceder a estas tecnologías mientras permanecen dependientes de proveedores extranjeros. Es en ese punto donde la línea de pobreza cibernética adquiere pertinencia analítica: la

dependencia tecnológica no es solo una condición económica, sino un determinante de la capacidad defensiva soberana.

Modelo DPA-LAC y sus componentes

El modelo DPA-LAC se construye sobre una premisa que lo distingue de su matriz asiática: la línea de pobreza cibernética no es un dato contextual, sino la variable que ordena la secuencia de implementación. En consecuencia, el modelo incorpora un componente cero que opera como precondition de los demás.

El primer movimiento del argumento es la extensión de escala. La

línea de pobreza cibernética, formulada por Nather y Ellis (2013) para organizaciones y sistematizada por el Atlantic Council (2022) en cuatro brechas de recursos, se traslada aquí al nivel estatal. Existe un umbral de capacidad: presupuestal, de talento, tecnológica y de influencia, por debajo del cual un Estado no puede sostener defensa persistente, sino únicamente respuesta reactiva y coyuntural. La analogía es justificable porque las cuatro brechas originales tienen equivalentes soberanos directos: el presupuesto de defensa cibernética, la disponibilidad de talento especializado formado localmente, la capacidad tecnológica no dependiente de proveedores externos y la

Tabla 1
Genealogía doctrinal de la Defensa Persistente Avanzada

Corriente	Fuente	Aporte conceptual a la DPA
Persistencia cibernética	Nakasone (2019)	Sustitución de la respuesta por la iniciativa continua; defensa hacia adelante y colaboración operativa permanente.
Debate sobre disuasión	Hurel y Mott (2025)	Delimitación de cinco escuelas y reconocimiento de la resiliencia como denegación de efecto.
Ciberdefensa integral	de Nobrega et al. (2024)	Fundamento multiactor y sincronización entre práctica organizacional y teoría.
Atribución graduada	Rid y Buchanan (2015)	Atribución como proceso con grados de confianza, no como identificación binaria.
Política de la atribución	Hedling y Ördén (2025)	Distinción entre atribución pública y no atribución como decisiones estratégicas.
Brecha de automatización	Maschmeyer (2026)	Ventaja estructural de la defensa derivada de la asimetría entre engaño y detección.
Déficit de control	Dotterrer et al. (2026)	Condicionamiento de esa ventaja a la integración organizacional del defensor.
Dimensión cognitiva	Whyte et al. (2020); Jaidka et al. (2025)	Incorporación de la integridad informacional al perímetro de la ciberdefensa.

Nota. Elaboración propia a partir de las fuentes citadas.
El orden es cronológico-conceptual y no jerárquico.

influencia para obtener asistencia internacional en condiciones favorables.

El segundo movimiento es el diagnóstico regional por dispersión. América Latina no se sitúa uniformemente bajo el umbral: presenta niveles de variación de capacidades. Este hecho desplaza el problema. Si todos los Estados estuvieran igualmente por debajo, la solución sería la transferencia externa de capacidad. Si todos estuvieran por encima, la cooperación sería un asunto de coordinación. La dispersión genera un problema distinto: los Estados con mayor capacidad carecen de incentivos para vincular sus arquitecturas a las de sus vecinos, porque la integración importa riesgo sin aportar capacidad, mientras que los Estados con menor capacidad carecen de los prerrequisitos institucionales para absorber la asistencia que se les ofrece.

El tercer movimiento se deriva de lo anterior. La lógica del eslabón más débil que Abdul Rahman (2026) aplica al Sudeste Asiático resulta excesiva bajo alta dispersión: un diseño regional que presuponga capacidades nacionales homogéneas carece de base material. De ahí la inversión de secuencia. En el modelo original, el marco regional orienta y disciplina los enfoques nacionales. En el DPA-LAC, la persistencia se construye desde el nivel nacional hacia el subregional y solo después hacia el regional, y la cooperación regional deja de ser

el punto de partida para convertirse en el mecanismo de elevación del umbral.

El cuarto movimiento reformula el criterio de éxito. La métrica no puede ser la paridad de capacidades con potencias cibernéticas, que resulta inalcanzable y estratégicamente irrelevante para Estados de capacidad media. La métrica pertinente es doble: elevación de la base común y reducción de la variación de capacidades intrarregional. Esta reformulación tiene una consecuencia doctrinal precisa. La resiliencia deja de ser una alternativa entre otras dentro del debate sobre disuasión, tal como la presentan Hurel y Mott (2025), y pasa a ser un mecanismo relevante y costo-efectivo bajo restricción presupuestal.

Sobre esta base, el modelo se compone de seis elementos y dos ejes transversales. El componente cero, umbral de suficiencia defensiva, define la línea base nacional: marco normativo vigente, equipo de respuesta operativo, inventario de infraestructura crítica y canal de comunicación civil-militar establecido, sin el cual los demás componentes carecen de sustento. El componente uno, inteligencia anticipatoria compartida, se concibe como mecanismo de transferencia de capacidad y no solo de intercambio de indicadores, siguiendo la lógica multiactor de Nobrega et al. (2024). El componente dos, cacería persistente de amenazas, es escalable

según la posición del Estado respecto del umbral, y admite implementaciones mínimas basadas en monitoreo centralizado antes que en capacidades distribuidas.

El componente tres, atribución graduada y decisión política, incorpora la distinción de Rid y Buchanan (2015) entre grados de confianza y la de Hedling y Ördén (2025) entre atribución pública y no atribución. En contextos de capacidad media, la atribución forense completa tiene un costo exagerado para un Estado individual, lo que la convierte en candidata natural a bien público regional. El componente cuatro, resiliencia como sustituto funcional de la disuasión, traduce el argumento del tercer movimiento en capacidades concretas de continuidad operativa, respaldos inmutables y recuperación verificada, en línea con las medidas propuestas por el Instituto Nacional de Ciberseguridad (2026). El componente cinco, gobernanza normativa y confianza, adopta las normas internacionales y los marcos hemisféricos como sustituto funcional de una integración formal que en América Latina no existe.

Los dos ejes transversales atraviesan todos los componentes. El eje de inteligencia artificial y automatización es ambivalente: la brecha identificada por Maschmeyer (2026) favorece estructuralmente a la defensa, pero el déficit de control descrito por Dotterrer et al. (2026) implica que capitalizar esa ventaja

exige integración organizacional importante, precisamente el recurso más escaso bajo el umbral. La automatización puede, por tanto, reducir o ampliar la distancia al umbral según la capacidad institucional previa. El eje cognitivo reconoce que la desinformación constituye el vector de menor costo contra Estados situados bajo el umbral, dado que explota la confianza institucional antes que la infraestructura técnica (Jaidka et al., 2025; Whyte et al., 2020; Erendor, 2024).

La Tabla 2 sintetiza la arquitectura resultante. Conviene subrayar que el orden de los componentes no es jerárquico sino secuencial: expresa una precedencia de implementación y no una escala de importancia. Un Estado situado claramente por debajo del umbral que invirtiera en cacería persistente de amenazas sin haber consolidado el componente cero obtendría capacidad técnica sin una base institucional para sostenerla, patrón que la literatura sobre cooperación en seguridad documenta con frecuencia bajo la forma de capacidades donadas que se degradan una vez concluida la asistencia externa. Inversamente, un Estado que consolidara el componente cero sin avanzar hacia los siguientes permanecería en la respuesta reactiva y coyuntural que el modelo busca superar. La utilidad del DPA-LAC reside, por tanto, en ordenar decisiones de inversión bajo restricción presupuestal antes que en prescribir una dotación completa de capacidades.

Tabla 2

Componentes del modelo DPA-LAC y su función respecto del umbral de suficiencia defensiva

Código	Componente	Función respecto del umbral
C0	Umbral de suficiencia defensiva	Define la línea base nacional; precondition de operabilidad de los componentes restantes.
C1	Inteligencia anticipatoria compartida	Opera como mecanismo de transferencia de capacidad y no solo de intercambio de indicadores.
C2	Cacería persistente de amenazas	Escalable según la posición del Estado respecto del umbral; admite implementaciones mínimas.
C3	Atribución graduada y decisión política	Bien público regional ante el costo individual exagerado de la capacidad forense completa.
C4	Resiliencia como sustituto funcional de disuasión	Estrategia dominante bajo restricción presupuestal; denegación de efecto al atacante.
C5	Gobernanza normativa y confianza	Normas internacionales como sustituto funcional de una integración formal inexistente.
Eje A	Inteligencia artificial y automatización	Reduce o amplía la distancia al umbral según la capacidad institucional previa.
Eje B	Dimensión cognitiva	Vector de menor costo contra Estados situados por debajo del umbral.

Nota. Elaboración propia. La numeración expresa precedencia de implementación y no jerarquía de importancia.

Modelo DPA-LAC: Caso aplicado a Colombia

La aplicación del modelo a Colombia exige situarla primero en el contexto regional. El Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones (2024) ofrece una medida comparable de compromiso estatal en cinco pilares: jurídico, técnico, organizacional, desarrollo de capacidades y cooperación, y clasifica a los países en cinco niveles. En América Latina, Brasil es el único Estado clasificado como modelo de referencia; México y Ecuador se ubican en el nivel de avance; Chile, Colombia, Costa Rica, Panamá y Perú, entre otros, en el nivel de establecimiento; y una porción sustancial de la región permanece en niveles de

evolución o construcción. Esta distribución confirma empíricamente el segundo movimiento del argumento: el problema regional no es un déficit uniforme, sino una dispersión que abarca cuatro de los cinco niveles disponibles.

Brasil opera por encima del umbral en la mayoría de las dimensiones. Su escala demográfica y económica sostiene un presupuesto de defensa cibernética sin equivalente regional, cuenta con industria nacional de defensa y con un comando militar cibernético consolidado, y su clasificación como modelo de referencia refleja madurez homogénea en los cinco pilares. Su limitación no es de capacidad sino de vocación: la asimetría con sus veci-

nos reduce los incentivos para vincular su arquitectura a esquemas regionales que aportarían poco a su postura y añadirían exposición (OEA-BID, 2020).

Chile representa el caso de mayor densidad normativa. La Ley 21.663 estableció un marco general de ciberseguridad y creó la Agencia Nacional de Ciberseguridad, con obligaciones específicas para operadores de importancia vital, incluidos sistemas de gestión de seguridad de la información, designación de oficiales de ciberseguridad y plazos escalonados de reporte de incidentes (Congreso Nacional de Chile, 2024). Este diseño resuelve institucionalmente el componente cero del modelo y establece una línea base verificable. Su clasificación en el nivel de establecimiento sugiere, no obstante, que la maduración normativa aún no se ha traducido plenamente en capacidad técnica y operativa.

México ilustra la brecha entre exposición y arquitectura. Su clasificación en el nivel de avance convive con una fragmentación institucional persistente y con la ausencia de una ley marco equivalente a la chilena, en un contexto de integración productiva profunda con Norteamérica que amplifica las consecuencias de cualquier compromiso en su infraestructura crítica. Es el caso que mejor ilustra por qué la posición respecto del umbral no se deduce del tamaño económico (OEA-BID, 2020).

Colombia se ubica en el nivel de establecimiento y presenta un perfil característico de Estado en torno al umbral. Dispone de los elementos formales del componente cero: una política nacional de seguridad digital que define roles y responsabilidades de gobernanza, un equipo de respuesta a emergencias cibernéticas con función de punto de contacto nacional, un centro cibernético policial y capacidades de ciberdefensa militar bajo un comando conjunto cibernético (CONPES, 2020), además de regulación sectorial específica en el ámbito financiero que exige pruebas periódicas de ciberresiliencia. La política nacional de inteligencia artificial adoptada en 2025 incorporó lineamientos de ciberseguridad y privacidad como condición habilitante, lo que conecta el eje transversal de automatización con la agenda de política pública (CONPES, 2025).

El diagnóstico por componentes revela, sin embargo, brechas consistentes. En el componente uno, el intercambio de inteligencia opera predominantemente entre entidades estatales y con un flujo limitado hacia el sector privado y las entidades territoriales, lo que reproduce internamente la lógica de dispersión que caracteriza a la región: la capacidad se concentra en el nivel central mientras los municipios y las pequeñas y medianas empresas permanecen claramente bajo el umbral. En el componente dos, la cacería persistente de amenazas depende de capacidades concen-

tralizadas y no de una función distribuida, lo que limita su alcance a los activos de mayor visibilidad.

En el componente tres, la atribución constituye la brecha más marcada. El costo de una capacidad forense y analítica completa excede lo que un Estado de capacidad media puede sostener de manera autónoma, y la dimensión política de la atribución que describen Hedling y Ördén (2025) añade una restricción adicional en un entorno regional donde la asignación pública de responsabilidad tiene consecuencias diplomáticas inmediatas.

En el componente cuatro, la resiliencia muestra avances sectoriales, notablemente en el ámbito financiero, donde la exigencia regulatoria de pruebas periódicas ha generado capacidad verificable, pero desigualdad marcada entre sectores.

El componente cinco encuentra su principal limitación en la ausencia de un equivalente latinoamericano al andamiaje regional asiático. No existe un equipo regional de respuesta ni un centro de excelencia de ciberdefensa comparable, y los mecanismos hemisféricos operan con mandatos amplios y recursos limitados. La condición de Colombia como socio global de la Organización del Tratado del Atlántico Norte introduce un elemento distintivo: le proporciona acceso a marcos de interoperabilidad y a estándares de ciberseguridad para siste-

mas de armas cuya ausencia documentan Kajander et al. (2025), pero también la sitúa en una posición particular dentro de un entorno regional donde tal vinculación no es la norma.

Los dos ejes transversales operan con signo opuesto. En el eje de automatización, la ventaja estructural de la defensa que identifica Maschmeyer (2026) es teóricamente accesible, pero su realización depende de la integración organizacional que Dotterrer et al. (2026) señalan como requisito, y esa integración es precisamente lo que la fragmentación institucional colombiana dificulta. En el eje cognitivo, la exposición es alta: el entorno regional presenta condiciones propicias para operaciones de información, y la reducción de barreras para producir desinformación mediante inteligencia artificial generativa (Jaidka et al., 2025) amplifica un vector que no requiere superioridad técnica del atacante.

La Tabla 3 sintetiza el análisis comparado. El patrón que emerge es consistente con el segundo movimiento del argumento: los cuatro Estados examinados ocupan tres niveles distintos de clasificación y presentan configuraciones institucionales no equivalentes, de modo que ninguna arquitectura regional podría aplicarles obligaciones uniformes sin excluir de facto a los que se sitúan más abajo. Colombia, en particular, ilustra la condición de Estado en torno al umbral: dispone

de instituciones formales suficientes para operar los componentes básicos del modelo, pero no de la integración organizacional necesaria para capitalizar la ventaja defensiva que la automatización ofrece.

Ventajas y limitaciones para la aplicación del modelo

La primera ventaja del modelo es su realidad secuencial. Al establecer un componente cero como precondición explícita, el DPA-LAC evita el error recurrente de las agencias de cooperación regional que presuponen capacidades nacionales inexistentes. La secuencia invertida: nacional, subregional, regional, permite que cada Estado identifique su posición respecto del umbral antes de comprometerse con obligaciones que no puede sos-

tener, lo que reduce el riesgo de acuerdos formales sin implementación efectiva, un patrón frecuente en la cooperación latinoamericana en materia de seguridad.

La segunda ventaja es la reformulación del criterio de éxito. Al sustituir la paridad de capacidades por la elevación de la línea base común y la reducción de la variación de capacidades, el modelo ofrece métricas alcanzables y verificables.

Un Estado puede demostrar progreso mediante el ascenso de nivel en índices comparables o mediante la incorporación de entidades territoriales al perímetro de protección nacional, sin necesidad de compararse con actores cuya escala presupuestal es inalcanzable. Esta

Tabla 3
Análisis comparado de capacidades de ciberdefensa: Colombia, Brasil, Chile y México

Estado	Nivel UIT (2024)	Rasgo institucional distintivo	Brecha principal respecto del DPA-LAC
Brasil	Modelo de referencia	Escala presupuestal, industria nacional de defensa y comando militar cibernético consolidado.	Ausencia de incentivo para vincular su arquitectura a esquemas regionales (C5).
México	Avance	Integración productiva profunda con Norteamérica; alta exposición de infraestructura crítica.	Fragmentación institucional sin ley marco equivalente (C0).
Chile	Establecimiento	Ley 21.663 y Agencia Nacional de Ciberseguridad con rectoría concentrada.	Traducción incompleta de la madurez normativa en capacidad operativa (C2).
Colombia	Establecimiento	Política nacional de seguridad digital, colCERT, centro cibernético policial, comando conjunto cibernético y regulación sectorial financiera.	Atribución autónoma y cacería distribuida de amenazas (C2, C3).

Nota. Clasificación tomada de la Unión Internacional de Telecomunicaciones (2024); análisis institucional de elaboración propia.

reformulación tiene además un efecto político: convierte la ciberdefensa en una agenda de desarrollo institucional antes que en una carrera armamentista digital.

La tercera ventaja es la coherencia con la evidencia sobre automatización. Si la brecha identificada por Maschmeyer (2026) es correcta, los Estados que inviertan en automatización defensiva obtendrán ventajas crecientes sobre los que prioricen la automatización ofensiva. Para Estados de capacidad media, esta conclusión es estratégicamente favorable: sugiere que la inversión defensiva ofrece mayor retorno marginal que el desarrollo de capacidades ofensivas, cuyo costo y cuyos riesgos de escalamiento son considerablemente mayores.

La cuarta ventaja es la utilización de las normas internacionales como sustituto funcional de la integración formal. Dado que América Latina carece de un acuerdo de integración digital comparable al asiático, las normas internacionales sobre comportamiento responsable de los Estados ofrecen un lenguaje común que no requiere cesión de soberanía ni creación de instituciones nuevas, y que puede adoptarse de manera incremental y asimétrica según la capacidad de cada Estado.

Así mismo se presentan algunas limitaciones del modelo que se precisan a continuación. La primera y

más importante es de orden epistemológico: la extensión de la línea de pobreza cibernética del nivel organizacional al estatal es una analogía, no una equivalencia demostrada. Las organizaciones enfrentan un umbral definido por la disponibilidad de recursos en un mercado; los Estados enfrentan restricciones adicionales de soberanía, legitimidad democrática y economía política que no tienen equivalente organizacional, que ilustran los retos de las naciones en este contexto.

La segunda limitación es la operacionalización del umbral. El modelo postula un componente cero, pero no se detalla valores concretos que permitan determinar con precisión si un Estado se sitúa por encima o por debajo. Los índices comparados disponibles miden compromiso declarado y marcos institucionales antes que capacidad operativa efectiva, y su metodología descansa en autoreporte verificado. Una operacionalización concreta exigiría indicadores de desempeño: tiempos de detección y contención, cobertura efectiva de infraestructura crítica, densidad de talento especializado, que actualmente no se recopilan de manera comparable en la región.

La tercera limitación es el problema del incentivo asimétrico. El modelo propone que los Estados de mayor capacidad actúen como mecanismos de transferencia, pero no resuelve por qué habrían de hacer-

lo. En el caso asiático, la vinculación de la ciberseguridad a un acuerdo de integración económica genera un interés material directo. En América Latina, la ausencia de ese vínculo deja la cooperación dependiente de la voluntad política, históricamente volátil y sujeta a los ciclos electorales de cada Estado.

La cuarta limitación concierne a la atribución como bien público regional. La propuesta es analíticamente atractiva pero políticamente difícil: compartir capacidad de atribución implica compartir inteligencia, y ello exige un nivel de confianza intergubernamental que la región no ha construido. La distinción de Hedling y Ördén (2025) entre atribución y no atribución profundiza el reto, pues un mecanismo compartido obligaría a coordinar decisiones políticas sobre asignación pública de responsabilidad que cada Estado prefiere reservarse.

La quinta limitación es temporal. El modelo propone una secuencia ascendente que requiere años, mientras que la evolución de las capacidades ofensivas automatizadas transcurre en meses. Rosen y Kraprayoon (2026) advierten que el margen disponible se mide en años y no en décadas. Existe, por tanto, un riesgo real de que la construcción secuencial del umbral sea superada por la velocidad de la amenaza, escenario en el cual el modelo describiría correctamente el problema comprometiendo la oportunidad de la solución.

La sexta limitación es de alcance empírico. El caso aplicado se sustenta en fuentes documentales, normativas e índices comparados, sin trabajo de campo ni acceso a información operativa clasificada, que es precisamente donde reside buena parte de la capacidad real. Kajander et al. (2025) advierten que la naturaleza clasificada de los requisitos de ciberseguridad para sistemas de armas hace difícil establecer qué han implementado efectivamente los Estados. Esta opacidad afecta a cualquier evaluación externa y aconseja tratar los resultados como aproximaciones antes que como mediciones.

En conjunto, las ventajas del modelo se concentran en su capacidad de ordenar decisiones bajo restricción, y sus limitaciones en la ausencia de una teoría del incentivo que explique por qué los Estados de mayor capacidad deben participar. Esta asimetría entre lo que el modelo resuelve y lo que deja abierto no invalida la propuesta, pero delimita su alcance: el DPA-LAC es un instrumento de diseño de política pública nacional con proyección regional, y no un mecanismo de cooperación autoejecutable. Su valor práctico depende de que los Estados que lo adopten reconozcan su propia posición respecto del umbral antes de comprometerse con obligaciones externas, y de que las agencias de cooperación ajusten sus instrumentos de asistencia a esa secuencia en lugar de replicar modelos diseñados para

contextos con precondiciones distintas.

En la tabla 4 se resumen las ventajas, limitaciones y tensiones resultantes propias del modelo DPA-LAC.

Conclusiones

La Defensa Persistente Avanzada constituye una respuesta conceptualmente válida a la realidad de que la agresión en el ciberespacio es continua. Su traslado a América Latina, sin embargo, no puede ser

Tabla 4.
Ventajas y limitaciones del modelo DPA-LAC

Dimensión	Ventaja	Limitación	Tensión resultante
Diseño secuencial (C0)	Realismo: el umbral de suficiencia como precondición explícita evita agendas que presuponen capacidades inexistentes.	Sin valores de corte cuantitativos; los índices miden compromiso declarado, no capacidad operativa.	El modelo ordena la secuencia pero no permite determinar con precisión en qué punto se encuentra un Estado.
Criterio de éxito	Métricas alcanzables: elevación de la línea base común y reducción de la variación de capacidades en lugar de paridad.	Alcance empírico restringido: sin trabajo de campo ni acceso a información clasificada.	Las métricas son verificables en principio, pero la evidencia disponible es indirecta.
Cooperación regional (C5)	Las normas internacionales operan como sustituto de una integración formal inexistente, sin cesión de soberanía	Incentivo asimétrico: no explica por qué los Estados de mayor capacidad pueden ayudar a otros.	Ofrece el lenguaje de la cooperación sin resolver el reto de fondo.
Atribución (C3)	Concebirlo como bien público regional resuelve el costo individual de un Estado.	Exige compartir inteligencia y coordinar decisiones políticas que cada Estado reserva.	Solución económicamente racional, políticamente inviable en baja confianza.
Automatización (Eje A)	Ventaja estructural de la defensa; mayor retorno marginal que la inversión ofensiva.	Capitalizarla exige integración organizacional, el recurso más escaso bajo el umbral.	La ventaja teórica se invierte en la práctica para quienes más la necesitan.
Horizonte temporal	Secuencia ascendente adaptada a	Requiere años; las capacidades ofensivas automatizadas evolucionan en meses.	Riesgo de que el diagnóstico sea correcto y la solución llegue tarde.
Dimensión	Ventaja	Limitación	Tensión resultante
	restricción presupuestal real.		

Nota. Elaboración propia.

una operación de importación doctrinal. Las precondiciones que sostienen su formulación original: integración digital formalizada, un Estado fuerte con capacidades cibernéticas y arquitecturas de ciberseguridad operativas, son limitadas en la región, y esa ausencia no es contingente sino estructural.

Esta reflexión ha argumentado que la variable que explica la asimetría es la posición de los Estados respecto de la línea de pobreza cibernética. La extensión de este concepto del nivel organizacional al estatal, asumida explícitamente como aporte analítico, permite reconceptualizar el problema: la capacidad de sostener defensa persistente depende de un umbral de suficiencia por debajo del cual solo es posible la respuesta reactiva y coyuntural.

El diagnóstico regional resultante desplaza el foco tradicional de los análisis. El obstáculo principal para una arquitectura latinoamericana de ciberdefensa no es la carencia absoluta de capacidades, sino su dispersión. La clasificación comparada muestra a la región distribuida en cuatro de los cinco niveles disponibles, con Brasil como modelo de referencia y una porción sustancial de Estados en niveles iniciales.

Esta variación en las capacidades genera un problema de incentivos que ninguna transferencia de recursos resuelve por sí sola.

De ello se sigue la inversión de secuencia que constituye la contribución central del modelo DPA-LAC. Mientras el diseño original procede del marco regional hacia los enfoques nacionales, el modelo propuesto invierte el orden y convierte la cooperación regional en mecanismo de elevación del umbral antes que en punto de partida. El componente cero: umbral de suficiencia defensiva, opera como precondición explícita de los cinco componentes restantes y de los dos ejes transversales.

El caso colombiano confirma el diagnóstico. Colombia dispone de los elementos formales del componente cero pero presenta brechas consistentes en inteligencia compartida, cacería distribuida de amenazas y atribución, junto con avances sectoriales significativos en resiliencia. Su posición en torno al umbral la sitúa en una condición ambivalente: suficientemente desarrollada para operar los componentes básicos, insuficientemente integrada para capitalizar la ventaja defensiva que ofrece la automatización.

Tres implicaciones se desprenden del análisis. Primera, para Estados de capacidad media la resiliencia no es una opción doctrinal, sino un mecanismo costo-efecto y sostenible en el tiempo. Segunda, la ventaja estructural que la inteligencia artificial otorga a la defensa no es automática: depende de una inte-

gración organizacional que constituye precisamente el recurso más escaso bajo el umbral. Tercera, la métrica de éxito debe reformularse en términos de elevación de la línea base común y reducción de la variación de capacidades.

Las limitaciones identificadas delimitan el alcance de estas conclusiones. La analogía entre umbral organizacional y umbral estatal permanece requieren demostración empírica; el componente cero demanda valores de corte mínimos esperados; el problema del incentivo asimétrico no encuentra solución dentro del modelo; y la velocidad de evolución de las capacidades ofensivas automatizadas puede superar la secuencia ascendente propuesta.

La agenda de investigación que se abre es tiene dos elementos. En el plano conceptual, corresponde someter a prueba la validez de la extensión del modelo mediante estudios comparados que incorporen indicadores de desempeño operativo y no solo de compromiso declarado. En el plano aplicado, corresponde examinar si mecanismos de atribución compartida son viables en contextos de baja confianza intergubernamental, cuestión de la que depende buena parte de la factibilidad del modelo propuesto.

Referencias

- Abdul Rahman, M. F. B. (2026). Securing ASEAN cyberspace: A case for Advanced Persistent Defence (IDSS Paper No. IP26074). S. Rajaratnam School of International Studies, *Nanyang Technological University*.
<https://rsis.edu.sg/rsis-publication/idss/ip26074/>
- Atlantic Council. (2022). Buying down risk: Cyber poverty line. Cyber Statecraft Initiative.
<https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-poverty-line/>
- Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.
- Congreso Nacional de Chile. (2024). Ley 21.663, Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información. Biblioteca del Congreso Nacional de Chile.
- Consejo Nacional de Política Económica y Social - CONPES. (2020). Documento CONPES 3995: Política Nacional de Confianza y Seguridad Digital. *Departamento Nacional de Planeación*.
<https://colaboracion.dnp.gov.co/CDT/Conpes/Economicos/3995.pdf>
- Consejo Nacional de Política Económica y Social - CONPES. (2025). Documento CONPES 4144: Política Nacional de Inteligencia Artificial. *Departamento Nacional de Planeación*.
<https://colaboracion.dnp.gov.co/CDT/Conpes/Economicos/4144.pdf>
- de Nobrega, K. M., Rutkowski, A.-F., & Saunders, C. (2024). The whole of cyber defense: Syncing practice and theory. *The Journal of Strategic Information Systems*, 33(4), Article 101861.
<https://doi.org/10.1016/j.jsis.2024.101861>
- Dotterrer, K., Hauptman, A. I., Richoux, B. P., & Corbett, M. L. (2026). Grand cha-

- llenges in agentic AI for cyber operations: A research agenda. *The Cyber Defense Review*, 11(3), 1–28.
<https://doi.org/10.55682/cdr/gcai-agda>
- Erendor, M. E. (Ed.). (2024). *Cyber security in the age of artificial intelligence and autonomous weapons*. CRC Press.
<https://doi.org/10.1201/9781003441700>
- Gopal Chari, S. (2025). Power, pixels and politics: The geopolitics of emerging technologies in the digital age. *London Journal of Research in Humanities and Social Science*, 25(2), 1–95.
https://journalspress.com/LJRHSS_Volume25/Power-Pixels-and-Politics-The-Geopolitics-of-Emerging-Technologies-in-the-Digital-Age.pdf
- Hedling, E., & Ördén, H. (2025). Disinformation, deterrence and the politics of attribution. *International Affairs*, 101(3), 967–985.
<https://doi.org/10.1093/ia/iaaf055>
- Hurel, L. M., & Mott, G. (2025). Rethinking cyber deterrence in a multipolar world: Emerging insights. *Royal United Services Institute for Defence and Security Studies*.
<https://www.rusi.org/explore-our-research/publications/emerging-insights/rethinking-cyber-deterrence-multipolar-world>
- Instituto Nacional de Ciberseguridad - INCIBE. (2026). Medidas de ciberseguridad y ciberresiliencia ante modelos de IA de frontera: Información para entidades. *INCIBE-CERT*.
<https://www.incibe.es/incibe-cert/blog/medidas-de-ciberseguridad-y-ciberresiliencia-ante-modelos-de-ia-de-frontera>
- Jaidka, K., Chen, T., Chesterman, S., Hsu, W., Kan, M.-Y., Kankanhalli, M., Lee, M. L., Seres, G., Sim, T., Taihagh, A., Tung, A., Xiao, X., & Yue, A. (2025). Misinformation, disinformation, and generative AI: Implications for perception and policy. *Digital Government: Research and Practice*, 6(1), Article 11.
<https://doi.org/10.1145/3689372>
- Kajander, A., Liivoja, R., & Naagel, M. (2025). Cybersecurity of weapon systems. *Journal of Cybersecurity*, 11(1).
<https://doi.org/10.1093/cybsec/tyaf017>
- Maschmeyer, L. (2026). Deception and detection: Why artificial intelligence empowers cyber defense over offense. *International Security*, 50(3), 86–126.
<https://doi.org/10.1162/ISEC.a.398>
- Nakasone, P. M. (2019). A cyber force for persistent operations. *Joint Force Quarterly*, 92, 10–14.
<https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950/a-cyber-force-for-persistent-operations/>
- Nather, W. & Ellis, A. (2013). Living below the security poverty line: coping mechanism. Akamai - 451 Research. *RSA Conference 2013*.
<https://www.infosecuritamagazine.nl/files/2fb0642808f57f0f9831532ae8f7e8fd.pdf>
- Organización de los Estados Americanos & Banco Interamericano de Desarrollo – OEA-BID. (2020). Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte de Ciberseguridad 2020. *OEA-BID*.
<http://dx.doi.org/10.18235/0002513>
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), 4–37.
<https://doi.org/10.1080/01402390.2014.977382>
- Rosen, B., & Kraprayoon, J. (2026). Cyberwar's new frontier. *Foreign Affairs*.
<https://www.foreignaffairs.com/united-states/cyberwars-new-frontier>

Unión Internacional de Telecomunicaciones – UIT. (2024). Global cybersecurity index 2024. UIT.
<https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>

Whyte, C., Thrall, A. T., & Mazanec, B. M. (Eds.). (2020). *Information warfare in the age of cyber conflict*. Routledge. 🌐

Jeimy J. Cano M., Ph.D, CFE, CICA. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.