

Capítulo 5

Infraestructura crítica y riesgo sistémico: retos para Colombia en la era de la ciberguerra*

DOI: <https://doi.org/10.25062/9786287818705.05>

Carlos Enrique Álvarez Calderón
Óscar Vega Pulido

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo analiza los fundamentos doctrinales, regulatorios y estratégicos necesarios para que Colombia diseñe una arquitectura nacional de ciberseguridad eficaz frente al riesgo sistémico derivado de la interdependencia de sus infraestructuras críticas y las amenazas ciberfísicas emergentes. Se sostiene que la protección de la Infraestructura Crítica Cibernética (ICC) constituye un imperativo estratégico para la estabilidad del Estado, la continuidad de los servicios esenciales y la defensa nacional. Se discuten los desafíos asociados a la gestión de riesgos, las brechas institucionales y los vacíos normativos, así como la necesidad de articular una gobernanza cibernética robusta. Si bien el capítulo aborda de forma general las capas del ciberespacio (física, lógica, informativa y de usuario), el foco recae en las vulnerabilidades estructurales, los perfiles de agresores y los tipos de ataques más relevantes para el contexto colombiano. Finalmente, se plantea la urgencia de fortalecer las capacidades de disuasión, resiliencia, cooperación público-privada y respuesta ofensiva ante escenarios de conflictividad geopolítica digital.

Palabras clave: ciberespacio; ciberguerra; infraestructura crítica; soberanía digital

* Capítulo de libro resultado del proyecto de investigación "Desafíos y nuevos escenarios de la seguridad multidimensional a nivel nacional, regional y hemisférico en el decenio 2015-2025", del grupo de investigación Centro de Gravedad, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado como A por MinCiencias y registrado con el código COL0104976. Los puntos de vista pertenecen a los autores, y no necesariamente reflejan el pensamiento de las instituciones participantes.

Carlos Enrique Álvarez Calderón

Candidato a doctor en Estudios Estratégicos, Seguridad y Defensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Coaching Ontológico Empresarial, Universidad San Sebastián, Chile. Politólogo y Magíster en Relaciones Internacionales, Pontificia Universidad Javeriana, Colombia. Investigador Asociado MinCiencias y Docente Investigador, Escuela Superior de Guerra "General Rafael Reyes Prieto". Profesional Oficial de Reserva, Fuerza Aeroespacial Colombiana. Asesor y consultor en seguridad y defensa para instituciones de las Fuerzas Militares de Colombia y a nivel internacional.

<https://orcid.org/0000-0003-2401-2789> - Contacto: carlos.alvarez@esdeg.edu.co

Oscar Vega Pulido

Magíster en Seguridad y Defensa Nacional, y maestrando en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Administración de la Seguridad, Universidad Militar Nueva Granada, Colombia. Economista, Universidad de la Salle, Colombia. Docente de posgrado, Universidad Militar Nueva Granada. Director Nacional de Seguridad Integral, Grupo Olímpica S. A.

<https://orcid.org/0009-0003-5777-4816> - Contacto: ovega@olimpica.com.co

Citación APA: Álvarez Calderón, C. E. & Vega Pulido, O. (2026). Infraestructura crítica y riesgo sistémico: retos para Colombia en la era de la ciberguerra. En C. E. Álvarez Calderón (Ed.), *El campo de batalla digital: la defensa nacional en la era algorítmica, Volumen I. (Infraestructuras de la guerra digital: computación, ciberguerra y defensa del ciberespacio)* (pp. 317-378). Sello Editorial ESDEG.

<https://doi.org/10.25062/9786287818705.05>

EL CAMPO DE BATALLA DIGITAL: LA DEFENSA NACIONAL EN LA ERA ALGORÍTMICA

VOLUMEN I. INFRAESTRUCTURAS DE LA GUERRA DIGITAL: COMPUTACIÓN, CIBERGUERRA Y DEFENSA DEL CIBERESPACIO

ISBN IMPRESO (Obra completa): 978-628-7818-65-1

ISBN DIGITAL (Obra completa): 978-628-7818-69-9

ISBN IMPRESO Volumen I: 978-628-7818-66-8

ISBN DIGITAL Volumen I: 978-628-7818-70-5

DOI: <https://doi.org/10.25062/9786287818705>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2026



Introducción

A lo largo de la historia los Estados nacionales han luchado por controlar rutas comerciales, territorios estratégicos y recursos vitales. Hoy, en el siglo XXI, el dominio más disputado no es una frontera terrestre ni una isla remota, sino un entorno intangible y ubicuo: el ciberespacio. Esta vasta red de redes ha dejado de ser un mero medio de comunicación para convertirse en el sistema circulatorio del poder global. En él se transfieren capitales, se controlan infraestructuras vitales, se ejecutan decisiones gubernamentales y se moldea la opinión pública. Como advierte Buchanan (2020), los Estados que dominen el ciberespacio no solo podrán espiar, interrumpir o sabotear a sus rivales, sino que podrán redibujar las reglas del orden internacional desde las sombras.

El ciberespacio¹ es, por ende, un nuevo teatro de confrontación estratégica, y posee su propia arquitectura, como cables submarinos, satélites, centros de datos, *routers* y redes eléctricas que lo hacen tangible y vulnerable. Esta infraestructura crítica (IC) —es decir, los sistemas que sostienen el funcionamiento básico de la sociedad— se ha digitalizado a tal punto que su protección ya no puede considerarse un asunto técnico aislado, sino un imperativo de seguridad nacional. La capacidad para transmitir datos de texto y voz de manera instantánea a través del ciberespacio ha sido el motor tanto del funcionamiento del sistema económico

¹ El escritor William Gibson, considerado el padre del *ciberpunk*, acuñó el término "ciberespacio" en su novela *Neuromancer* (1984), una obra que revolucionó la ciencia ficción al anticipar la convergencia entre redes digitales, IA y control corporativo en un mundo hiperconectado. En *Neuromancer*, Gibson no solo introdujo una estética distópica marcada por la tecnificación del cuerpo y la disolución de las fronteras entre lo real y lo virtual, sino que también formuló una visión profética del "ciberespacio" como una "alucinación consensual experimentada diariamente por miles de millones", décadas antes de la consolidación de internet. Su obra fundacional influenció el pensamiento sobre la seguridad informacional, el poder algorítmico y las nuevas formas de conflicto en el entorno digital. Los términos "ciberseguridad", "cibercrimen", "ciberguerra" y "ciberterrorismo" devienen todos del concepto de "ciberespacio", que, a su vez, proviene del término "cibernética".

global como de las operaciones modernas de los Estados, las fuerzas militares y las organizaciones sociales. En este entorno interconectado, las capacidades de poder de los actores globales (incluidos gobiernos, empresas y grupos transnacionales) dependen cada vez más de su grado de acceso y participación en el ciberespacio (Álvarez & Zambrano, 2017).

Por lo tanto, esta centralidad del ciberespacio ha reconfigurado profundamente el paradigma de la defensa nacional, ya que en la actualidad no es necesario cruzar fronteras ni desplegar ejércitos para paralizar a un Estado adversario: basta con comprometer sus nodos digitales vitales (Stoddart, 2022). En efecto, la arquitectura de poder en el siglo XXI ya no se construye exclusivamente sobre la base del control territorial, sino también sobre el dominio de los flujos informacionales que sostienen la IC del Estado moderno. Como advierte Castells (2009), la exclusión de esas redes de información implica, en términos prácticos, la exclusión del poder mismo.

La evidencia empírica de los últimos años confirma esta evolución. Desde el apagón masivo en Ucrania, en 2015, atribuido a *hackers* rusos, hasta el ataque de *ransomware* a Colonial Pipeline, en Estados Unidos, en 2021, el patrón es claro: los sistemas críticos (energía, transporte, telecomunicaciones, finanzas y salud) son objetivos preferidos de actores estatales y criminales que utilizan herramientas cibernéticas como instrumentos de coacción, sabotaje o extorsión (Lonergan & Lonergan, 2023). Ante esta nueva lógica de la agresión, la doctrina clásica de defensa, centrada en la integridad territorial y la capacidad de respuesta militar convencional, resulta insuficiente.

Colombia no es ajena a esta realidad, ya que ha experimentado, en los últimos años, un proceso acelerado de digitalización en sectores clave, acompañado por un aumento progresivo en los incidentes cibernéticos de alto impacto. Según Crowther et al. (2022), América Latina se ha convertido en un terreno fértil para el ensayo de ciberataques asimétricos, debido a brechas normativas, débil capacidad institucional y baja cultura de ciberseguridad. Y en el caso del Estado colombiano, en particular, se presenta una IC expuesta a múltiples vectores de riesgo (desde ataques de denegación de servicio hasta intrusiones en redes industriales), sin un sistema robusto de respuesta coordinada.

Aunque Colombia sí ha avanzado en la formulación de políticas públicas y en la creación de capacidades institucionales en materia de ciberseguridad, persisten importantes limitaciones para consolidar una arquitectura nacional que articule de manera efectiva los ejes de defensa, resiliencia y soberanía digital. Si bien la Política Nacional de Ciberseguridad y Confianza Digital (CONPES, 2020) representa

un esfuerzo significativo en la definición de objetivos estratégicos, su implementación ha enfrentado desafíos de coordinación interinstitucional, desarrollo normativo y fortalecimiento operacional. Por ende, la ausencia de una estructura integrada de forma plena, que combine capacidades ofensivas y defensivas, una regulación robusta sobre IC y una estrategia clara de autonomía tecnológica, sigue constituyendo una vulnerabilidad estratégica frente al carácter dinámico, persistente y asimétrico de las amenazas en el ciberespacio.

Más aún, la dimensión geopolítica del problema amplifica su gravedad. En un entorno internacional marcado por la rivalidad entre potencias tecnológicas y la proliferación de actores no estatales con capacidades ofensivas, el control sobre la infraestructura digital se ha vuelto un indicador clave de poder. Como sostienen Haber y Topor (2023), los Estados autoritarios están construyendo “burbujas de internet”: es decir, ecosistemas cerrados que buscan proteger su soberanía digital, mientras que las democracias enfrentan mayores dificultades para controlar sus espacios cibernéticos sin comprometer derechos fundamentales. En ese contexto, Colombia debe navegar una compleja tensión entre apertura tecnológica, seguridad nacional y soberanía regulatoria.

El reto no es tan solo técnico: también requiere una comprensión profunda del ciberespacio como dominio estratégico y del tipo particular de conflicto que allí se libra. A diferencia de los ataques cinéticos en los dominios tradicionales de la guerra, los ciberataques pueden ser invisibles, ambiguos y difíciles de atribuir, lo que dificulta aplicar mecanismos tradicionales de disuasión y respuesta. Además, los actores pueden operar por medio de terceros, como *proxies* criminales o grupos hacktivistas, y así generar una dinámica de “guerra gris” permanente (Buchanan, 2020). Esto exige no solo capacidades defensivas, sino también marcos normativos modernos, doctrinas adaptativas y una gobernanza nacional capaz de articular a los sectores público, privado y militar.

Hans Morgenthau (1960) sostiene, desde el realismo clásico, que la seguridad nacional de un Estado depende fundamentalmente de la integridad de sus fronteras físicas y de la solidez de sus instituciones políticas. Sin embargo, el advenimiento del siglo XXI transformó de modo radical este paradigma, ya que la ubicuidad e interdependencia de las tecnologías de la información y las comunicaciones (TIC) han hecho que casi todos los aspectos de la vida humana y del funcionamiento institucional del Estado dependan de sistemas digitales interconectados. La interrupción o sabotaje de un solo componente de esta red puede desencadenar un efecto en cascada sobre otros sistemas críticos, y comprometer

así la estabilidad económica, política y social de un Estado. A medida que infraestructuras como el sistema financiero, telecomunicaciones, energía o el transporte se informatizan y se integran a redes globales, aumenta exponencialmente su exposición a amenazas multidimensionales que desafían la concepción tradicional de soberanía y defensa nacional².

Debido a lo anterior, la soberanía ya no depende únicamente del control territorial, sino también del control funcional sobre los sistemas digitales que permiten operar un Estado. Por lo tanto, ya no se trata solo de un problema técnico o sectorial, sino de una cuestión existencial para los Estados modernos, ya que el ciberespacio, como dominio estratégico, ha modificado la naturaleza del conflicto (Álvarez et al., 2017b). En el plano táctico puede emplearse como vector de ataque para degradar, inutilizar o destruir funciones específicas de la IC de un adversario. En el plano estratégico busca interrumpir o manipular el flujo de información alterando la percepción y capacidad de respuesta de los sistemas políticos, militares o sociales (Lonergan & Lonergan, 2023). Como advierte Smith (1999), el ciberespacio no solo ha alterado la geografía tradicional del poder, sino que ha redefinido las formas como los Estados proyectan influencia, controlan información y ejercen soberanía.

En el contexto descrito, surge un interrogante central que orienta este capítulo: ¿Qué elementos doctrinales, regulatorios y estratégicos debe contemplar Colombia para diseñar una arquitectura nacional de ciberseguridad que, considerando el riesgo sistémico asociado a infraestructuras interdependientes y las tendencias globales de ataques ciberfísicos y ciberoperacionales, garantice la protección efectiva de su propia IC en un entorno de amenazas cibernéticas crecientes y disputas geopolíticas digitales? La pregunta se fundamenta en la premisa de que la protección de la IC no es tan solo un asunto técnico, sino un desafío estratégico y existencial para el Estado. Responde, además, a la necesidad de trascender el análisis descriptivo de incidentes para explorar de manera integral los componentes doctrinales, institucionales y normativos que podrían fortalecer la posición de Colombia frente a un panorama cibernético cada vez más hostil y complejo.

Para dar respuesta al interrogante planteado, el capítulo se estructura en cuatro grandes apartados analíticos. En primer lugar, se examina la naturaleza de la IC en el siglo XXI destacando su interdependencia digital y los riesgos sistémicos que pueden generar efectos en cascada ante fallas o ataques coordinados. En

² La "seguridad multidimensional" es un concepto que involucra las amenazas externas de tipo militar, y la incorporación de otro tipo de amenazas internas y externas a la seguridad y defensa de los Estados, incluyendo las económicas, ambientales, sociales, políticas y tecnológicas, así como las nuevas amenazas características del siglo XXI (Álvarez et al., 2017a).

segundo lugar, se analizan los vectores de ataque y los actores amenazantes haciendo énfasis en la evolución global de los ataques ciberfísicos y ciberoperacionales que han marcado un cambio de paradigma en la conducción y el carácter de la guerra, en lo que Álvarez et al. (2017b) denominan “guerras de quinta generación” (G5G). Posteriormente, se estudian modelos internacionales de ciberseguridad y lecciones recientes, con el propósito de identificar tanto las buenas prácticas como los vacíos en las arquitecturas nacionales de defensa digital. Finalmente, se aborda el caso colombiano identificando brechas estructurales, riesgos específicos y posibles lineamientos estratégicos, doctrinales y regulatorios para el diseño de una arquitectura nacional de ciberseguridad que articule defensa, resiliencia y soberanía digital.

Infraestructura crítica y ciberguerra: exposición cibernética y vulnerabilidades en el entorno digital

En el siglo XXI la infraestructura crítica (IC) se ha convertido en el pilar del funcionamiento de los Estados. Tradicionalmente, el concepto de IC se asociaba a instalaciones físicas como redes eléctricas, sistemas de transporte, instalaciones sanitarias, redes de agua y petróleo, y servicios de emergencia. Sin embargo, la progresiva digitalización de estos sectores ha difuminado la frontera entre lo físico y lo virtual generando una categoría híbrida donde los sistemas digitales se han integrado de manera estructural al funcionamiento de las infraestructuras tradicionales (Pesch-Cronin & Marion, 2024). Este fenómeno, que algunos autores denominan “convergencia” (Pesch-Cronin & Marion, 2024), implica que la falla o interrupción de un nodo digital puede desencadenar un efecto en cascada capaz de paralizar múltiples sectores interdependientes.

Naturaleza de la infraestructura crítica en el siglo XXI: interdependencia digital y riesgo sistémico

De acuerdo con Stoddart (2022), la IC puede clasificarse en dos grandes categorías: la infraestructura física tradicional y la infraestructura digital o virtual. La primera incluye sectores como la energía, el transporte, el agua, la salud y las telecomunicaciones, cuya interrupción genera consecuencias directas en la vida cotidiana de la población. La segunda comprende los sistemas de datos, centros

de procesamiento de información, redes de comunicaciones y servicios basados en la nube, que, si bien no siempre son visibles para la ciudadanía, resultan esenciales para la operación coordinada de los sistemas físicos. Según Pesch-Cronin y Marion (2024), la IC moderna no es tan solo un conjunto de activos físicos, sino una red compleja que integra datos, procesos automatizados y comunicaciones en tiempo real.

El sector energético ilustra bien esta distinción: las plantas de generación eléctrica y las redes de distribución son activos físicos, pero su operación depende de sistemas de control industrial y plataformas digitales interconectadas. Un ataque que comprometa el *software* de supervisión puede detener una planta entera sin necesidad de destruir físicamente sus componentes (Stoddart, 2022). Algo similar ocurre en la banca y las finanzas, donde las operaciones físicas (como el retiro de efectivo) dependen casi por completo de sistemas de pagos electrónicos y redes interbancarias basadas en la nube. En ese sentido, la IC digital no solo apoya, sino que en muchos casos sustenta funcionalmente a la IC física.

La creciente digitalización de la actual IC se manifiesta principalmente en la incorporación de los Sistemas de Control y Adquisición de Datos (en inglés, SCADA, por las iniciales de *Supervisory Control and Data Acquisition*), así como de otras tecnologías operacionales. Dichos sistemas permiten supervisar y controlar procesos industriales de forma remota, y así optimizan recursos y reducen costos operativos. No obstante, su interconexión con redes corporativas y, en muchos casos, con internet ha incrementado de modo exponencial la superficie de ataque (Nguyen & Sparks, 2020). De acuerdo con Henrie (2013), el término SCADA comenzó a utilizarse en la década de 1960, aunque sus antecedentes se remontan a 1912, cuando la industria eléctrica de Chicago implementó sistemas rudimentarios de comunicación telefónica para monitorear y controlar estaciones remotas. El siguiente gran salto en el tema se produjo en 1959, con la introducción de computadores industriales en la refinería Texaco Port Arthur, lo que marcó el inicio de los sistemas automatizados de control de procesos. A lo largo de las décadas, SCADA evolucionó desde circuitos telefónicos dedicados y sistemas propietarios hacia entornos basados en redes y estándares abiertos, integrados con tecnologías de la información (TI) y las telecomunicaciones globales (Henrie, 2013).

Si bien esta evolución ha permitido mayores niveles de eficiencia, seguridad y productividad (asegurando, por ejemplo, un suministro eléctrico estable, gas natural a hospitales o el monitoreo avanzado de oleoductos), también ha generado nuevas y variadas vulnerabilidades. Stoddart (2022) advierte que muchos de esos sistemas conservan componentes heredados (*Legacy Systems*) diseñados en

épocas en que la ciberseguridad no era prioritaria, lo que los hace susceptibles a intrusiones y sabotajes. Asimismo, Henrie (2013) señala que la convergencia entre SCADA y TI ha incrementado drásticamente el riesgo, pues la utilización de *hardware* y *software* estandarizado, y el uso compartido de las infraestructuras de telecomunicaciones expone dichos sistemas a amenazas que antes eran impensables. Así, los SCADA, concebidos originalmente para operar en entornos aislados, se han transformado en verdaderos “cerebros automatizados” de la IC moderna, pero también en uno de sus principales puntos débiles desde la perspectiva de la ciberguerra.

El Internet de las Cosas (IoT) amplifica aún más esta exposición, ya que dispositivos inteligentes (sensores, medidores, controladores de temperatura y presión) se incorporan de forma masiva a infraestructuras críticas para monitorear su desempeño en tiempo real. Empero, esta hiperconectividad, también llamada “Internet de las Amenazas”, ha introducido nuevos vectores de intrusión (Stoddart, 2022). En otras palabras, basta con comprometer un sensor mal configurado para obtener acceso a toda la red SCADA. Por su parte, los servicios en la nube se han vuelto la columna vertebral de la gestión de datos en sectores como la salud, las finanzas y las telecomunicaciones. Aunque ofrecen ventajas en escalabilidad y redundancia, también generan dependencias críticas en relación con proveedores externos, lo que plantea riesgos de soberanía tecnológica y aumenta la posibilidad de interrupciones generalizadas en caso de ataques coordinados (Sin & Washburn, 2022). La nube, además, actúa como un punto de convergencia donde múltiples sectores comparten infraestructuras, lo que incrementa el riesgo de propagación de amenazas de un sector a otro.

En términos analíticos, estas transformaciones obligan a abandonar una concepción sectorial o fragmentada de la seguridad de la IC y adoptar una mirada sistémica. Desde la teoría de los sistemas complejos, un sistema se caracteriza por la interacción de múltiples subsistemas interconectados, mecanismos de autoorganización, la ausencia de control centralizado, la retroalimentación positiva y negativa, y la emergencia de comportamientos globales que no pueden explicarse a partir del análisis de sus partes individuales. Por consiguiente, las IC contemporáneas pueden entenderse como sistemas complejos adaptativos, caracterizados por altos niveles de interdependencia funcional, acoplamientos no lineales y dinámicas de retroalimentación que conectan componentes técnicos, organizacionales y sociales. En este tipo de sistemas el riesgo no se limita a la probabilidad de falla de un activo individual, sino que emerge como una propiedad sistémica, derivada de la arquitectura del conjunto y de la densidad de sus interconexiones.

En este marco, el “riesgo sistémico” se define como la posibilidad de que una perturbación localizada (técnica, operativa o intencional) genere efectos en cascada capaces de comprometer la estabilidad y funcionalidad del sistema en su totalidad. No es una anomalía externa, sino una propiedad endógena del sistema, producto de su propia arquitectura, densidad de interconexión y grado de acoplamiento funcional. Como señalan Thurner et al. (2018), en los sistemas complejos la estabilidad no equivale a equilibrio, sino a la capacidad para absorber perturbaciones y reorganizarse sin colapsar. Cuando dicha capacidad se ve superada, pequeñas disrupciones pueden generar consecuencias desproporcionadas a través de mecanismos de amplificación sistémica.

A fin de traducir este concepto abstracto en una lógica analítica comprensible, resulta útil representar de manera esquemática las interdependencias funcionales entre los principales sectores de IC (tabla 1). Este ejercicio no busca identificar activos específicos ni vulnerabilidades operativas, sino visualizar, a nivel sistémico, cómo una perturbación en un nodo clave puede propagarse transversalmente al conjunto del sistema.

Tabla 1. *Interdependencias sistémicas entre infraestructuras críticas en entornos ciberfísicos*

Infraestructura base	Dependencias primarias	Efectos en cascada ante disrupción	Relevancia estratégica
Energía	Telecomunicaciones; sistemas de control industrial (SCADA); logística	Paralización de comunicaciones; colapso de servicios financieros; interrupción de agua y salud	Nodo sistémico central; habilita el funcionamiento del resto de la IC
Telecomunicaciones	Energía; nube; centros de datos	Pérdida de mando y control (C-2); interrupción de servicios financieros y gubernamentales	Clave para C-2, continuidad estatal y gestión de crisis
Finanzas	Energía; telecomunicaciones; nube	Interrupción de pagos; pánico financiero; crisis de confianza	Instrumento de coerción económica y desestabilización social
Salud	Energía; telecomunicaciones; sistemas digitales	Riesgo directo para la vida humana; colapso de atención médica	Alto impacto político y humanitario
Transporte y logística	Energía, telecomunicaciones, sistemas de posicionamiento	Desabastecimiento, interrupción de cadenas de suministro	Afecta movilidad militar, económica y social
Defensa y seguridad	Energía; telecomunicaciones; ciberinfraestructura	Degradación de C-2; pérdida de conciencia situacional	Impacto directo en capacidad disuasiva y respuesta

Fuente: elaboración propia.

Como se desprende de la tabla 1, a diferencia de los riesgos convencionales, que suelen ser lineales y contenibles, el riesgo sistémico se manifiesta de forma no proporcional: fallas menores pueden amplificarse rápidamente y producir consecuencias estratégicas. Desde la economía política del riesgo, esta vulnerabilidad se ve reforzada por modelos de gestión que privilegian la eficiencia, la estandarización y la concentración funcional reduciendo redundancias y aumentando la dependencia mutua entre sectores críticos.

En el ámbito digital estas dinámicas adquieren una dimensión adicional. La convergencia entre sistemas industriales, tecnologías de la información, servicios en la nube y el IoT ha intensificado el grado de acoplamiento entre infraestructuras, haciendo que una disrupción en un nodo clave pueda propagarse transversalmente a múltiples sectores. En consecuencia, la interdependencia creciente de la IC ha dado lugar a lo que diversos autores denominan “riesgo sistémico cibernético”. Según Stoddart (2022), un ataque a un único sector (por ejemplo, el eléctrico) puede desencadenar un efecto dominó que afecte simultáneamente al agua potable, el transporte, la banca y las telecomunicaciones. Este fenómeno se observó en el ataque a la red eléctrica de Ucrania, en 2015, cuando el apagón prolongado generó interrupciones en hospitales, problemas en el abastecimiento de agua y colapso temporal de las comunicaciones (Loneragan & Loneragan, 2023). La energía eléctrica es el nodo más crítico: sin ella los sistemas de bombeo se detienen, los servidores bancarios caen y las telecomunicaciones se paralizan. Stoddart (2022) describe este escenario como una posible “parálisis estratégica”, en la que un ataque bien orquestado puede devolver a una sociedad moderna a inicios del siglo XX en cuestión de días.

En términos de la ciberguerra, este tipo de efectos en cascada es atractivo para las acciones ofensivas. Como plantea Buchanan (2020), la ciberguerra no necesariamente busca la destrucción física de objetivos, sino la disrupción prolongada de funciones críticas, a fin de generar presión política y social sobre el adversario, ya que un ataque sistémico exitoso puede inducir crisis económicas y pánico social, así como debilitar la capacidad de respuesta estatal sin necesidad de lanzar un solo misil.

Por consiguiente, la relación entre IC y ciberguerra es cada vez más evidente. Loneragan y Loneragan (2023) explican que los actores estatales y no estatales han pasado de realizar ataques aislados o actos de espionaje a desarrollar estrategias ofensivas orientadas a degradar la IC del adversario como un medio para lograr objetivos estratégicos. “Stuxnet” (2010), dirigido contra centrifugadoras iraníes, y

el ataque de *ransomware* a Colonial Pipeline (2021), que paralizó temporalmente el suministro de combustible en la costa este de Estados Unidos, son ejemplos paradigmáticos de cómo los ciberataques contra la IC pueden generar efectos geopolíticos significativos.

Este uso deliberado de la IC como objetivo responde a dos razones principales: 1) la alta dependencia social y económica de esos sistemas, lo que convierte cualquier disrupción en un multiplicador de efectos políticos y mediáticos, y 2) la dificultad de atribución directa en el ciberespacio, lo que permite a los atacantes operar con un alto grado de impunidad utilizando como intermediarios *proxies* criminales o grupos hacktivistas. Desde una perspectiva realista, atacar la IC es atacar el “centro de gravedad” de un Estado. Como afirma Morgenthau (1960), el poder estatal depende del control sobre los recursos esenciales para su funcionamiento. En la era digital dicho control no se limita al territorio, sino que se extiende al dominio funcional de sistemas interconectados que sustentan la vida moderna.

En síntesis, la actual IC es un sistema complejo e interdependiente, donde lo físico y lo digital se encuentran estrechamente entrelazados. SCADA, IoT y servicios en la nube han mejorado la eficiencia operativa, pero también han ampliado de forma exponencial la superficie de ataque, y creado así vulnerabilidades que pueden ser explotadas con fines estratégicos. El riesgo sistémico y los efectos en cascada posicionan a la IC como un objetivo prioritario en las G5G, donde la capacidad para paralizar funciones esenciales de un Estado puede equivaler a una victoria estratégica sin necesidad de confrontación cinética. Para los Estados, y particularmente para Colombia, comprender esa dinámica no es opcional: es un imperativo, a fin de diseñar arquitecturas de ciberseguridad capaces de anticipar, resistir y responder a amenazas cada vez más sofisticadas y persistentes.

Vectores de ataque y actores en la ciberguerra contra la infraestructura crítica

En el contexto de la ciberguerra contemporánea, los ataques a la IC son ejecutados por una combinación de actores estatales, *proxies*, grupos de amenazas persistentes avanzadas (APA) y organizaciones criminales, que, de manera coordinada o independiente, explotan la creciente interdependencia digital de los sistemas esenciales para la vida moderna (Buchanan, 2020; Stoddart, 2022). Los Estados son los principales responsables de la ciberguerra dirigida contra la IC, debido a los recursos financieros, humanos y tecnológicos que poseen para llevar a cabo operaciones ofensivas sofisticadas. Estas acciones suelen ejecutarse a través de

grupos de APA, quienes operan durante meses o años en las redes de sus blancos recopilando inteligencia, preposicionando *malware* y preparando ataques de disrupción o destrucción a gran escala. Grupos como APT28 ("Fancy Bear"), asociado al GRU ruso, o APT29 ("Cozy Bear"), vinculado al FSB, han sido señalados por infiltrarse en sistemas gubernamentales y energéticos para recolectar información estratégica o preparar escenarios de sabotaje (Stoddart, 2022).

No obstante, los Estados nacionales rara vez actúan de manera abierta. Por el contrario, algunos recurren a *proxies* (grupos criminales, hacktivistas o colectivos "patrióticos"), que actúan como "cibermercenarios", y proporcionan así un grado adicional de negación plausible. Buchanan (2020) argumenta que esa delegación es característica de la ciberguerra en la llamada "zona gris", donde los ataques no suelen cruzar el umbral de un acto formal y abierto de guerra, pero logran debilitar las defensas, erosionar la confianza pública y aumentar los costos económicos del adversario. Este modelo híbrido de guerra cibernética ofrece ventajas estratégicas: permite a los Estados proyectar poder a bajo costo y con menor riesgo de represalias directas, al tiempo que preserva la ambigüedad sobre su participación y reduce los costos políticos de atribución.

Maurer (2018) explica que los Estados emplean *proxies* no solo por conveniencia táctica, sino también como parte de estrategias de largo plazo orientadas a externalizar las capacidades ofensivas, y reducir así los costos políticos de una operación fallida o accidentalmente escalatoria. En efecto, Galeotti (2017) documenta que durante la década de 2010 el Gobierno de Rusia fomentó la existencia de comunidades cibercriminales altamente especializados que actuaban como "consultores externos" en operaciones específicas, y dichos grupos mantenían estructuras informales más cercanas a redes de expertos que a organizaciones criminales jerarquizadas. Este modelo ruso se complementó con colectivos "patrióticos", como CyberBerkut, que participaron activamente en campañas de desinformación y ataques distribuidos de denegación de servicio (DDoS) contra infraestructuras ucranianas en 2014, durante la anexión de Crimea (Egloff & Smeets, 2023).

En la misma línea, China ha sido señalada por utilizar grupos APA vinculados al Ejército Popular de Liberación de China (EPL), y en ocasiones, colectivos de *hackers* "nacionalistas", como el grupo APT41, cuyo accionar combina espionaje industrial y ataques disruptivos contra sectores estratégicos extranjeros (Haber, 2022). Esta delegación también se halla presente en el caso norcoreano, donde grupos como Lazarus Group operan tanto para ejecutar ataques de espionaje militar como realizar operaciones de *ransomware* destinadas a financiar al régimen.

En este sentido, el ataque “WannaCry”, en 2017, es paradigmático, ya que afectó a más de 150 países, donde paralizó no solo hospitales, sino también servicios públicos y redes corporativas. Ello demuestra cómo un grupo criminal respaldado por un Estado puede acabar generando consecuencias globales equivalentes a las de un ataque militar tradicional (Buchanan, 2020).

Esta dinámica se ve reforzada por el problema de atribución, que constituye, según Rid y Buchanan (2015), un “campo de batalla político” en sí mismo, pues atribuir un ataque públicamente es no solo un ejercicio técnico, sino también un acto político deliberado que busca construir narrativas estratégicas y legitimar posibles represalias. Por lo tanto, un problema clave que refuerza el uso de *proxies* es la dificultad para atribuir el ciberataque. Egloff y Smeets (2023) señalan que la “ambigüedad atribuible” es un recurso estratégico en sí mismo, pues cuanto más complejo es vincular un ataque con un Estado, mayor es la capacidad de ese Estado para evadir represalias y moldear las narrativas en los foros internacionales. Este fenómeno crea lo que los autores denominan una “capa de invisibilidad estratégica”, que no solo retrasa la respuesta del adversario, sino que también socava los esfuerzos de gobernanza global en materia de ciberseguridad. Empero, Lonergan y Lonergan (2023) advierten que dicha relación asimétrica y codependiente entre Estados y *proxies* es inestable: si bien los *proxies* son herramientas útiles para operar en la zona gris, su relativa autonomía puede desencadenar incidentes no deseados, y así escalar conflictos de manera inadvertida.

Pero independientemente de los riesgos, los *proxies* se convierten en actores esenciales en la ciberguerra, pues amplifican el poder estatal sin comprometer directamente su responsabilidad. Su participación refuerza la idea de que los ataques a IC son el producto no solo de ejércitos cibernéticos estatales, sino de un ecosistema híbrido donde convergen intereses estatales, motivaciones económicas y narrativas ideológicas. Esa hibridación complejiza los mecanismos de disuasión y exige repensar los marcos jurídicos internacionales, ya que la línea entre criminalidad común y acción bélica se vuelve cada vez más difusa.

Cabe señalar, sin embargo, que el papel de los actores criminales no se limita al oportunismo económico. Si bien grupos de *ransomware* suelen actuar motivados por beneficios financieros, sus acciones pueden tener efectos estratégicos equivalentes a los de una operación estatal. El ataque al Colonial Pipeline, en 2021, atribuido al grupo criminal DarkSide, obligó al cierre temporal de uno de los principales oleoductos de Estados Unidos, y ello generó desabastecimiento de combustible en la costa este y puso en evidencia la fragilidad de infraestructuras energéticas críticas (Haber, 2022). Aunque no hubo pruebas concluyentes de

apoyo estatal, Buchanan (2020) advierte que esos incidentes son aprovechados políticamente por Estados rivales, que pueden tolerar o, incluso, proteger a dichos grupos dentro de sus fronteras como parte de una estrategia de presión indirecta.

La evolución de los ataques contra IC muestra un tránsito desde operaciones de espionaje y sabotaje selectivo hacia estrategias más agresivas que combinan efectos ciberfísicos y ciberoperacionales. El caso paradigmático es "Stuxnet" (2010), un sofisticado *malware* diseñado para sabotear centrifugadoras nucleares iraníes. Stoddart (2022) destaca que "Stuxnet" fue el primer ejemplo documentado de un ciberataque que generó daños físicos significativos en una IC, y sentó así un precedente para el uso del ciberespacio como herramienta de guerra preventiva.

Desde entonces se han multiplicado los ataques con potencial destructivo directo: por ejemplo, el apagón en Ucrania, en 2015, atribuido al grupo ruso Sandworm, demostró cómo los sistemas SCADA de distribución eléctrica pueden acabar siendo manipulados para cortar el suministro en regiones enteras, y así afectar hospitales, transporte y telecomunicaciones (Lonergan & Lonergan, 2023). En 2017 el ataque "NotPetya", inicialmente dirigido a sistemas contables ucranianos, se propagó a escala global, y entonces paralizó puertos, empresas de transporte y hospitales en más de 60 países, lo que evidenció la dificultad de contener los efectos colaterales en un mundo interconectado.

En el ámbito ciberoperacional, los ataques a hospitales y servicios sanitarios se han convertido en un vector recurrente, como ocurrió en especial durante la pandemia de Covid-19. Lonergan y Lonergan (2023) señalan que los ataques a hospitales europeos entre 2020 y 2021, en muchos casos mediante *ransomware*, no solo interrumpieron cirugías y tratamientos críticos, sino que también fueron utilizados como instrumentos de presión para obligar al pago de rescates, y ello afectó la percepción pública de la capacidad estatal para proteger a sus ciudadanos.

Las redes móviles avanzadas y la tecnología 5G representan un nuevo vector estratégico en la ciberguerra contra infraestructuras críticas, debido a su creciente integración en sectores esenciales, como salud, transporte, energía y finanzas. A diferencia de generaciones anteriores, el 5G proporciona una conectividad de alta velocidad con baja latencia, lo cual permite la interconexión en tiempo real de millones de dispositivos IoT, sensores industriales y sistemas SCADA. Sin embargo, esta hiperconectividad incrementa la superficie de ataque, pues comprometer una sola estación base o nodo de red puede afectar simultáneamente múltiples servicios interdependientes. Kulkarni et al. (2025) advierten que la arquitectura distribuida del 5G, con funciones virtualizadas y dependientes de *software*, abre la puerta a intrusiones remotas en la capa de control de red, y eso permite a los atacantes

manipular el flujo de datos, interrumpir comunicaciones críticas o, incluso, desviar tráfico hacia servidores comprometidos para espionaje y sabotaje.

El riesgo se amplifica por la creciente dependencia de servicios en la nube y de proveedores externos para gestionar funciones clave del 5G, lo que introduce vulnerabilidades en la cadena de suministro digital (Kulkarni et al., 2025). Según Lonergan y Lonergan (2023), un ataque exitoso en un nodo 5G interconectado con sistemas industriales podría desencadenar un efecto en cascada paralizando operaciones logísticas o sanitarias, y traer consecuencias comparables a las de un ataque directo a SCADA. Además, Katagiri (2023) subraya que la proliferación de dispositivos IoT no seguros amplifica esta amenaza, pues cada dispositivo actúa como un posible punto de entrada. En términos estratégicos, las intrusiones en redes 5G no solo permiten disrupciones funcionales, sino que también tienen un impacto psicológico y político, al demostrar la incapacidad del Estado para proteger servicios esenciales que dependen cada vez más de dichas infraestructuras. Por tanto, las redes móviles y el 5G se perfilan como un nuevo “campo de batalla” en la ciberguerra, donde el control de la conectividad equivale al control del flujo de la vida moderna.

En conclusión, los casos que se han mencionado hasta el momento revelan tres implicaciones estratégicas clave. Primero, los ataques a IC han reducido el umbral de la guerra, al permitirles a los actores ofensivos que ejerzan coerción con efectos comparables a los de un ataque cinético, pero con menor riesgo de represalias militares inmediatas (Buchanan, 2020). Segundo, la atribución limitada y la negación plausible dificultan la aplicación de normas internacionales claras, lo que debilita los mecanismos de disuasión y fomenta una carrera de armamentos cibernéticos entre potencias (Stoddart, 2022). Tercero, la gobernanza global se enfrenta a una crisis de legitimidad: organismos como la Organización de las Naciones Unidas (ONU) o la Organización del Tratado del Atlántico Norte (OTAN) han tenido serias dificultades para consensuar marcos legales efectivos para proteger la IC, mientras que Estados con capacidades ofensivas avanzadas moldean unilateralmente las reglas del juego digital.

En este contexto, la protección de la IC ya no puede entenderse como un asunto meramente técnico o de gestión de riesgos. Es, en esencia, un problema de seguridad nacional y de equilibrio de poder global, donde cada ataque exitoso reconfigura las percepciones de vulnerabilidad y poder relativo en el sistema internacional. Como advierten Lonergan y Lonergan (2023), la ciberguerra contra IC no busca solo la interrupción temporal de servicios, sino la erosión de la confianza en las instituciones estatales, lo que convierte a dichas infraestructuras en verdaderos centros de gravedad estratégicos en el campo de batalla digital.

Escenarios de escalamiento y uso estratégico de la IC en la ciber guerra

La IC se ha transformado en un elemento central de la ciber guerra, no solo como blanco preferido de ataques, sino como un instrumento estratégico para el ejercicio de la coerción política, presión económica y manipulación psicológica. En un mundo interconectado, donde la dependencia funcional entre sectores es creciente, el sabotaje de infraestructuras esenciales tiene el potencial de producir efectos sistémicos que alteran la estabilidad interna de un Estado, así como la reconfiguración de sus relaciones internacionales (Katagiri, 2023; Wilner, 2017).

A diferencia de la guerra cinética tradicional, donde el escalamiento suele estar asociado a incrementos progresivos de la fuerza militar, en el ciber espacio el escalamiento suele manifestarse mediante la ampliación del alcance funcional y geográfico de los ataques. Según Lonergan y Lonergan (2023), los actores estatales diseñan operaciones cibernéticas escalonadas que comienzan con acciones de espionaje o intrusión pasiva y evolucionan hacia ataques disruptivos o destructivos conforme aumenta la tensión política o militar. Este patrón se evidenció en la guerra en Ucrania, donde los ciberataques rusos pasaron de campañas de desinformación a operaciones dirigidas contra la red eléctrica y sistemas gubernamentales, como parte de un esfuerzo coordinado para minar la resiliencia nacional y debilitar la moral civil (Brantly & Brantly, 2024).

En esta lógica, los ataques se planifican deliberadamente para mantenerse en la “zona gris”: es decir, por debajo del umbral que activaría represalias militares convencionales. Buchanan (2020) sostiene que dicha estrategia permite a los Estados ejercer presión sostenida sin cruzar líneas rojas formales, manteniendo un alto grado de ambigüedad estratégica. Esa ambigüedad les otorga la capacidad para modular la intensidad de la coerción, ajustando la presión según sus objetivos políticos, al tiempo que minimizan el riesgo de provocar una respuesta militar directa del adversario. Katagiri (2023) añade que esta ambigüedad se ve favorecida por los vacíos del derecho internacional, como la falta de efectividad del principio de distinción, lo que habilita ataques a IC con el argumento de su uso dual (civil-militar).

Los ataques a la IC no se conciben como objetivos aislados, sino como instrumentos estratégicos orientados, a su vez, a lograr objetivos políticos o geopolíticos. Wilner (2017) argumenta que el sabotaje de infraestructuras esenciales puede actuar como una forma de “coerción inversa”, en la cual el atacante impone costos tan elevados que obliga al adversario a priorizar la restauración interna por sobre la proyección de poder externo. Esta lógica se evidencia en diversos casos recientes.

Por ejemplo, en 2019 un ataque coordinado contra la red eléctrica de Sudáfrica provocó cortes prolongados en Johannesburgo, lo que exacerbó la inestabilidad política en medio de tensiones sociales preexistentes (Kulkarni et al., 2025). De manera similar, el grupo iraní APT33 ejecutó operaciones de tipo *wiper malware* contra compañías petroleras saudíes (como el caso de “Shamoon”, en 2012, y sus variantes posteriores), y logró afectar miles de computadores y enviar un mensaje geopolítico directo en el contexto de la rivalidad energética regional³.

Estos incidentes confirman lo que Katagiri (2023) ha denominado “parálisis estratégica”: es decir, interrupciones prolongadas de servicios básicos que no solo generan descontento civil, sino que erosionan la confianza en las instituciones estatales y condicionan la toma de decisiones gubernamentales. En este sentido, la IC se ha convertido en un arma psicológica y económica, cuyo impacto trasciende lo técnico y se proyecta en el terreno de la percepción pública y la legitimidad política.

Asimismo, el escalamiento en la ciberguerra contra la IC puede analizarse en dos dimensiones complementarias. La primera es el escalamiento vertical, que supone un incremento progresivo en la intensidad y la sofisticación de los ataques, al pasar de simples intrusiones a operaciones con efectos físicos significativos. Un ejemplo ilustrativo es el ataque con *malware* “Industroyer2”, detectado en 2022, que apuntó a subestaciones eléctricas ucranianas con una versión más avanzada del código utilizado en 2016. Esta evolución demostró la capacidad de los atacantes para refinar técnicas y explotar vulnerabilidades previas aumentando la efectividad destructiva con cada iteración (Brantly & Brantly, 2024).

La segunda dimensión es escalamiento horizontal, caracterizado por la ampliación del alcance funcional y geográfico de un ciberataque a la IC afectando simultáneamente múltiples sectores. Un caso relevante fue la Operación Olympic Destroyer, durante los Juegos Olímpicos de Invierno en Pyeongchang, en 2018, que, si bien dirigida principalmente a los sistemas informáticos del evento, interrumpió de forma temporal servicios de transmisión, redes corporativas y sistemas logísticos en varios países involucrados en la organización. Este tipo de incidentes demuestra cómo un ataque focalizado puede propagarse de manera no lineal, hasta afectar sectores interconectados y generar consecuencias imprevistas a nivel

³ El caso Shamoon en 2012 es considerado uno de los primeros ataques a gran escala con *malware* tipo *wiper* contra una IC. Atribuido a actores vinculados a Irán, el ataque comprometió a Saudi Aramco, la principal compañía petrolera saudí, al destruir datos en aproximadamente 30.000 computadores y paralizar temporalmente sus operaciones administrativas. El objetivo no fue interrumpir directamente la producción de petróleo, sino enviar un mensaje geopolítico simbólico en el contexto de la rivalidad energética y política entre Arabia Saudita e Irán. Variantes posteriores, como “Shamoon 2” (2016-2017), confirmaron la reutilización de este vector con fines estratégicos, combinando sabotaje con operaciones de influencia.

global (Buchanan, 2020). Estas dinámicas evidencian que los ataques a IC poseen un alto potencial sistémico: incluso operaciones limitadas pueden desencadenar efectos en cascada que trascienden sectores y fronteras, y eso dificulta prever su verdadera magnitud (Lonergan & Lonergan, 2023).

Para comprender de manera operativa cómo los ataques cibernéticos contra IC pueden traducirse en efectos estratégicos, resulta necesario ir más allá de los estudios de caso y avanzar hacia esquemas analíticos que permitan capturar la lógica de interdependencia y escalamiento del impacto. En contextos de alta interconexión digital, los efectos de un ataque no dependen exclusivamente de su sofisticación técnica o del daño inmediato producido, sino de su inserción dentro de una arquitectura sistémica caracterizada por acoplamientos no lineales, dependencias funcionales y retroalimentaciones cruzadas entre sectores.

Desde esta perspectiva, los ataques a la IC deben entenderse como instrumentos de coerción escalonada, capaces de generar efectos acumulativos que van desde disrupciones locales hasta crisis de gobernabilidad y parálisis estratégica. Tal como sugiere la literatura sobre coerción inversa, el objetivo no necesariamente es la destrucción física del adversario, sino la imposición de costos sistémicos que obliguen a priorizar la gestión de la crisis interna sobre la proyección de poder externo. En este marco el impacto de los ciberataques puede analizarse en función de su alcance funcional, su temporalidad y sus implicaciones políticas, lo que permite identificar distintos niveles de escalamiento dentro de una misma lógica estratégica.

Con el fin de operacionalizar el concepto de riesgo sistémico cibernético y facilitar su análisis desde una perspectiva estratégica y de política pública, la tabla 2 presenta un esquema sintético de escalamiento del impacto de los ataques contra IC atendiendo a la interdependencia sectorial, los tipos de efectos generados y la lógica estratégica subyacente.

Tabla 2. Escalamiento del impacto sistémico de ataques cibernéticos contra IC⁴

Nivel de impacto	Alcance funcional	Sectores potencialmente afectados	Tipo de efectos sistémicos	Temporalidad	Implicaciones políticas	Lógica estratégica predominante
Local	Infraestructura; ciudad o región específica	Energía local; transporte urbano; redes hospitalarias	Disrupción operativa específica; degradación de servicios	Corto plazo	Presión administrativa; gestión de crisis local	Señalización limitada; prueba de capacidades
Sectorial	Un sector crítico completo	Energía; telecomunicaciones; finanzas; agua	Efectos en cadena dentro del sector; pérdida de continuidad operativa	Corto-medio plazo	Costos económicos; descontento social	Coerción selectiva
Nacional	Múltiples sectores interdependientes	Energía-comunicaciones-banca-transporte	Cascadas sistémicas; fallas cruzadas	Medio plazo	Crisis de gobernabilidad; desgaste institucional	Presión estratégica sostenida (coerción inversa)
Estratégico	Sistema Estado-sociedad	Infraestructura intersectorial + esfera civil	Parálisis funcional; erosión de la confianza pública	Medio-largo plazo	Crisis de legitimidad; inestabilidad política	Parálisis estratégica
Internacional	Efectos transfronterizos	Cadenas de suministro; mercados; aliados	Externalidades no intencionadas; propagación regional	Variable	Escalada diplomática; sanciones; alineamientos	Señalización geopolítica
Transversal (zona gris)	Persistente y difuso	Infraestructura + cognición social	Erosión acumulativa y normalización del conflicto	Prolongada	Ambigüedad estratégica; desgaste prolongado	Dominio bajo umbral

Fuente: elaboración propia.

Más allá de sus efectos funcionales y sistémicos, los distintos niveles de escalamiento del impacto ya descritos adquieren sentido estratégico en tanto mecanismos de comunicación coercitiva entre Estados. El escalamiento en la ciber guerra contra la IC cumple, a su vez, una función de señalización estratégica dentro de la diplomacia cibernética. Como señalan Egloff y Smeets (2023), los ciberataques dirigidos a dichos sistemas actúan como auténticos “mensajes coercitivos”,

⁴ Este esquema tiene un propósito analítico y comparativo. No representa una clasificación oficial ni un inventario de infraestructuras críticas nacionales.

diseñados para comunicar determinación, advertir sobre posibles represalias o condicionar el comportamiento del adversario sin recurrir a la violencia abierta. Esta lógica ha sido evidente en diversas crisis recientes: Rusia, por ejemplo, usó ataques limitados a redes ucranianas como mecanismo de advertencia antes de iniciar operaciones militares convencionales, y así envió un mensaje de capacidad y voluntad de escalada (Brantly & Brantly, 2024).

De manera similar, China ha utilizado intrusiones selectivas en sectores energéticos y financieros regionales como parte de lo que Nye (2017) describe como “coerción latente”: una estrategia que mantiene presión política sobre los adversarios mientras evita asumir públicamente la autoría de los ataques. En tal sentido, la diplomacia cibernética termina convirtiendo la IC en una herramienta de negociación geopolítica, donde los ataques cuidadosamente calibrados no buscan únicamente disrupción funcional, sino influir en la toma de decisiones del adversario. Como explica Lancelot (2020), estas operaciones se diseñan para ejercer presión política gradual modulando la intensidad de la amenaza y manteniendo la ambigüedad estratégica, lo que permite a los Estados avanzar en sus objetivos sin desencadenar una escalada militar abierta.

El control del escalamiento cibernético enfrenta serias limitaciones, debido a las particularidades de la disuasión en el ciberespacio. Wilner (2017) identifica tres factores centrales que socavan su efectividad. En primer lugar, los problemas de atribución, ya que la dificultad para identificar con certeza al agresor reduce la credibilidad de las amenazas de represalia y, por ende, debilita la capacidad disuasoria. En segundo lugar, la asimetría digital, que incentiva a actores más débiles (como *proxies* y grupos criminales) a atacar Estados altamente digitalizados aprovechando su mayor vulnerabilidad estructural. En tercer lugar, la ambigüedad de las “líneas rojas”, pues no existe un consenso internacional sobre qué tipo de ciberataque constituye un acto de guerra, lo que genera respuestas inconsistentes y, en ocasiones, contradictorias.

A partir de estas dinámicas, es posible anticipar tres escenarios prospectivos de escalamiento en la ciberguerra contra las IC. El primero es un escalamiento progresivo como herramienta de negociación, donde ataques calibrados interrumpen temporalmente servicios críticos, con el objetivo de inducir concesiones políticas o forzar diálogos. El segundo es un escalamiento desbordado o no intencionado, en el que el *malware* se propaga fuera de los objetivos inicialmente previstos y afecta a terceros neutrales, como ocurrió con “NotPetya” en 2017. El tercero es un escalamiento cruzado (*cross-domain*), en el que ciberataques contra IC se utilizan para provocar respuestas en otros dominios (militar, económico o diplomático)

debilitando, por ejemplo, la logística militar antes de una ofensiva convencional (Brantly & Brantly, 2024).

En conclusión, el uso estratégico de la IC en la ciberguerra demuestra que estos ataques no se limitan a la interrupción de servicios, sino que constituyen auténticas herramientas de presión geopolítica y diplomática. Sin embargo, la interdependencia digital, la proliferación de nuevos vectores de ataque y las limitaciones inherentes a la disuasión crean un entorno en extremo inestable, donde operaciones inicialmente limitadas pueden escalar de forma impredecible. Comprender estas dinámicas resulta clave para el diseño de estrategias nacionales de ciberseguridad que integren defensa, resiliencia y diplomacia cibernética combinando la gestión técnica de riesgos con la construcción de narrativas disuasorias creíbles.

Arquitecturas nacionales de ciberseguridad: modelos, lecciones y vacíos

El desarrollo de arquitecturas nacionales en materia de ciberseguridad⁵ para la protección de las IC constituye hoy por hoy uno de los mayores retos de gobernanza en el ciberespacio. Como señalan Weiss y Biermann (2023), proteger la IC frente a los ciberataques implica enfrentar un dilema estructural. Aunque la ciberseguridad es una responsabilidad pública, su implementación recae en gran parte sobre actores privados, y ello obliga a los Estados nacionales a decidir entre modelos jerárquicos centralizados o esquemas basados en colaboración público-privada. Este dilema es sobre todo relevante en el caso de infraestructuras esenciales como energía, transporte, finanzas o telecomunicaciones, cuya interrupción afecta directamente la estabilidad política y económica de los Estados.

La arquitectura institucional de cada Estado responde a factores históricos, políticos y económicos. Por ejemplo, Francia, a través de la ANSSI⁶, ha optado por

⁵ La ciberseguridad puede definirse como el conjunto de principios, políticas, prácticas y tecnologías diseñadas para proteger los sistemas informáticos, redes y datos frente a accesos no autorizados, ataques, daños o interrupciones. De acuerdo con Gai et al. (2024), implica la defensa técnica de infraestructuras digitales, y la gestión integral del riesgo, la resiliencia operativa y la capacidad de anticipación mediante la ciberinteligencia, en entornos interconectados como el IoT. Chesney et al. (2023) añaden que, en el contexto estratégico resulta ser un componente clave de la seguridad y defensa nacional, pues permite garantizar la confidencialidad, integridad y disponibilidad de la información en un entorno caracterizado por amenazas persistentes, y actores estatales y no estatales con motivaciones políticas, económicas o militares.

⁶ La *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI) es la autoridad nacional francesa de ciberseguridad, creada en 2009 bajo la Secretaría General de Defensa y Seguridad Nacional (SGDSN). Su mandato incluye la protección de IC nacionales, la emisión de normativas y estándares obligatorios para ope-

un enfoque vertical y normativo que obliga a operadores públicos y privados a cumplir estándares mínimos de seguridad y reportar incidentes, estableciendo un control jerárquico de supervisión (Weiss & Jankauskas, 2019). En contraste, el Reino Unido ha favorecido un modelo liberal basado en incentivos económicos y asociaciones voluntarias con el sector privado, como el *Cyber Information Sharing Partnership*⁷, lo que refleja la confianza en la autorregulación de los operadores (Carr, 2016). Por su parte, en Estados Unidos, la estrategia *Defend Forward*⁸, de USCYBERCOM y la coordinación de la CISA⁹, han consolidado un enfoque híbrido que combina capacidades ofensivas con marcos de colaboración público-privada buscando anticipar y neutralizar amenazas antes de que afecten territorio nacional (Slayton, 2023).

El diseño de estas arquitecturas debe considerar no solo la defensa reactiva, sino también la gestión de los riesgos sistémicos y de la resiliencia de los sistemas interdependientes. Como indican Pesch-Cronin y Marion (2024), la protección de la IC no puede reducirse a la seguridad técnica: requiere estrategias integrales que

radores públicos y privados y la coordinación de respuestas ante incidentes a gran escala mediante el CERT-FR, así como la certificación de productos y servicios de ciberseguridad empleados en sistemas críticos. La ANSSI es considerada un modelo jerárquico centralizado de gobernanza, e impone obligaciones estrictas de reporte y cumplimiento a los operadores de servicios esenciales, lo que ha fortalecido la resiliencia francesa frente a ataques de alto impacto (Weiss & Jankauskas, 2019).

⁷ El *Cyber Information Sharing Partnership* (CiSP) es una plataforma de intercambio británica de información sobre ciberamenazas, creada en 2013 por el Centro Nacional de Seguridad Cibernética (en inglés, NCSC, por las iniciales de National Cyber Security Centre). Su fin es facilitar la colaboración público-privada mediante el intercambio en tiempo real de datos sobre incidentes, indicadores de compromiso (*Indicators of Compromise* [IoC]), y de las buenas prácticas de mitigación. A diferencia de modelos centralizados como el francés, el CiSP opera sobre la base de la participación voluntaria de empresas y organizaciones, lo cual refleja el enfoque liberal británico, que privilegia la confianza y la autorregulación del sector privado en la protección de infraestructuras críticas (Carr, 2016).

⁸ La estrategia *Defend Forward* es el marco doctrinal adoptado por el U. S. Cyber Command desde 2018, orientado a anticipar y neutralizar amenazas cibernéticas fuera del territorio estadounidense. Su principio central es operar de forma proactiva en las redes extranjeras (incluidas las de potenciales adversarios), para identificar, vigilar e interrumpir actividades maliciosas antes de que alcancen IC nacionales. Según Slayton (2023), dicha estrategia marca una transición de un enfoque puramente defensivo hacia una persistencia ofensiva, combinando ciberinteligencia y operaciones preventivas como elementos clave de la protección nacional. Aunque ha fortalecido la resiliencia de Estados Unidos, también ha generado debates sobre los riesgos de escalamiento involuntario y sobre los límites legales de actuar en redes ajenas.

⁹ La *Cybersecurity and Infrastructure Security Agency* (CISA) es la agencia federal estadounidense responsable de la protección de infraestructuras críticas y la coordinación de la ciberseguridad nacional. Creada en 2018 bajo el Departamento de Seguridad Nacional, su misión es identificar, mitigar y responder a amenazas cibernéticas que afecten sectores esenciales, como energía, finanzas, salud y telecomunicaciones. CISA opera como un nodo de coordinación público-privado ofreciendo asistencia técnica, emitiendo alertas de amenazas y desarrollando marcos de gestión de riesgos. Su enfoque se basa en fortalecer la resiliencia de los operadores de servicios esenciales mediante estándares voluntarios, asociaciones de intercambio de información y ejercicios de respuesta a incidentes a nivel nacional.

incluyan regulación diferenciada según el nivel de criticidad de los activos, inversiones en capacidad de respuesta y un marco de ciberinteligencia robusto para anticipar amenazas. Además, el auge del IoT y de los sistemas ciberfísicos añade complejidad a estas arquitecturas, y amplía la superficie de ataque a través de sensores, redes móviles y servicios en la nube (Gai et al., 2024).

Modelos internacionales de protección de infraestructura crítica

La protección de la IC se ha consolidado como un eje central de las estrategias nacionales de ciberseguridad, debido al impacto sistémico que los ciberataques pueden generar sobre sectores esenciales. Sin embargo, los modelos institucionales para proteger esos activos varían significativamente entre los Estados, reflejo de diferencias en la organización estatal, la relación con el sector privado, e incluso, la cultura estratégica. Dichos modelos pueden agruparse en tres grandes enfoques: centralizados y jerárquicos, descentralizados o basados en la colaboración público-privada, e híbridos o multinivel.

Los modelos centralizados se caracterizan por un fuerte liderazgo estatal y una estructura jerárquica de supervisión y control. El paradigma de ese enfoque es Francia, donde la ANSSI actúa como la autoridad nacional responsable de la protección de IC. Según Weiss y Jankauskas (2019), la ANSSI impone estándares obligatorios de ciberseguridad a los operadores de servicios esenciales, exige reportes de incidentes en plazos estrictos y hace auditorías de cumplimiento, lo que refuerza la resiliencia de los sectores estratégicos. Este modelo ha demostrado eficacia frente a amenazas de alto impacto, pero también enfrenta críticas por su rigidez burocrática y dificultad para adaptarse rápidamente a entornos tecnológicos dinámicos.

Un caso similar es el de la República de China (Taiwán), cuya estrategia de ciberseguridad se basa en un modelo centralizado impulsado por el Gobierno de Taiwán. Este enfoque responde a la necesidad de enfrentar amenazas persistentes y coordinadas, atribuidas a actores vinculados con la República Popular de China. Como señalan Huang y Li (2018), la estrategia taiwanesa incluye la creación de un centro nacional de ciberseguridad que actúa como nodo único para coordinar operaciones defensivas y emitir directrices técnicas a las instituciones públicas y privadas de ese país. Aunque el modelo refuerza la capacidad de respuesta en crisis, su éxito depende de la disponibilidad de recursos estatales y de una fuerte coordinación interinstitucional. Italia también ha adoptado recientemente un

enfoque centralizado con la creación de la *Agenzia per la Cybersicurezza Nazionale* (ACN). De acuerdo con Monteleone y Rossi (2024), la ACN busca superar la fragmentación histórica del sistema italiano asumiendo competencias normativas y operativas sobre IC. Este “retorno del Estado” en la ciberseguridad italiana refleja la creciente preocupación por los riesgos sistémicos, así como la presión de la Unión Europea (UE) para implementar estándares uniformes.

En contraste, los modelos colaborativos priorizan la participación voluntaria del sector privado, y se apoyan en esquemas de intercambio de información y buenas prácticas. El Reino Unido es un ejemplo representativo: su plataforma CiSP, gestionada por el NCSC, promueve la colaboración público-privada mediante el intercambio en tiempo real de IoC y alertas de amenazas (Carr, 2016). Este modelo refleja un enfoque liberal que confía en la autorregulación empresarial, priorizando la construcción de confianza sobre la imposición de obligaciones legales estrictas.

Finlandia también se inscribe en esta categoría, aunque con particularidades. Según Griffith (2018), el modelo finlandés se basa en una cultura de cooperación multisectorial, donde los operadores de IC participan activamente en los ejercicios conjuntos de ciberseguridad y comparten información con el Centro Nacional de Ciberseguridad (NCSC-FI). Esta aproximación, aunque menos coercitiva que la francesa, ha demostrado ser eficaz, gracias a un alto nivel de confianza entre el Estado y el sector privado, y a una tradición de seguridad integral en la sociedad finlandesa. Canadá representa un modelo colaborativo con rasgos federales. En efecto, el gobierno federal del país establece lineamientos generales y proporciona apoyo técnico, pero las provincias y territorios conservan su autonomía para implementar sus propios planes de protección en materia de IC (Quigley et al., 2017). Este enfoque genera flexibilidad, aunque también produce desigualdades en las capacidades de respuesta entre regiones.

Los modelos híbridos combinan un control estatal fuerte con esquemas de cooperación público-privada. El caso más emblemático es Estados Unidos, cuyo sistema articula a la CISA con el U. S. Cyber Command, encargado de operaciones ofensivas. La estrategia *Defend Forward*, desarrollada por USCYBERCOM, busca anticipar y neutralizar amenazas en redes extranjeras antes de que impacten infraestructuras estadounidenses (Slayton, 2023). Este modelo refleja la doctrina de “persistencia ofensiva”, complementada con iniciativas como el National Risk Management Center, de CISA, que trabaja estrechamente con operadores privados mediante estándares voluntarios y ejercicios de resiliencia.

A nivel supranacional, la UE ha evolucionado hacia un enfoque multinivel. Según Pursiainen y Kytöma (2023), la transición de la Directiva NIS a la Directiva

sobre la Resiliencia de Entidades Críticas (CER) refleja un cambio de una protección reactiva a una visión proactiva basada en resiliencia. Este modelo combina marcos regulatorios vinculantes con incentivos para que los operadores privados adopten medidas preventivas. Asimismo, la Política Industrial de Ciberseguridad de la UE busca reforzar la autonomía estratégica europea fomentando la producción local de tecnologías críticas (Timmers, 2018). Finalmente, la OTAN ha empezado a desempeñar un papel en la defensa de infraestructuras civiles en contextos de conflicto. Según Neilsen y Pontbriand (2025), la OTAN ha adoptado un enfoque de “manos fuera del teclado”, en el que, si bien no opera directamente sistemas civiles, si coordina el apoyo a los Estados miembros mediante intercambio de inteligencia, ejercicios conjuntos y despliegue de capacidades de respuesta rápida.

El análisis comparado de estos modelos evidencia fortalezas y debilidades complementarias. En efecto, los modelos centralizados destacan por su capacidad de respuesta rápida e integral en momentos de crisis, pero enfrentan desafíos para adaptarse a ecosistemas digitales en constante evolución. Por su parte, los modelos colaborativos, basados en la confianza público-privada, son mucho más flexibles y fomentan la innovación, aunque su efectividad depende de un alto nivel de madurez institucional y cohesión social. Por último, los modelos híbridos ofrecen un equilibrio entre ambos extremos, pero implican riesgos geopolíticos, especialmente cuando combinan defensa nacional con operaciones ofensivas en redes extranjeras.

Para Estados como Colombia estas experiencias internacionales evidencian la necesidad de diseñar un modelo híbrido ajustado a su propio contexto. Dicho modelo debería articular un marco regulatorio robusto, que establezca estándares mínimos de protección, acompañado de incentivos para la colaboración público-privada. Asimismo, resulta indispensable fortalecer las capacidades de ciberinteligencia, orientadas tanto a la detección temprana como a la anticipación de amenazas, y desarrollar doctrinas de disuasión y resiliencia proactiva, capaces de garantizar la continuidad de los servicios esenciales frente a incidentes de alto impacto.

Lecciones de casos recientes y mejores prácticas

La experiencia acumulada en la última década demuestra que la protección de las IC no puede entenderse como una tarea exclusivamente técnica, sino como un componente estratégico que integra gestión institucional, cooperación público-privada, resiliencia y disuasión cibernética. Algunos incidentes recientes evidencian tanto los logros como las limitaciones de los modelos existentes y permiten extraer lecciones aplicables para la construcción de arquitecturas de ciberseguridad.

Una primera lección es la necesidad de contar con mecanismos claros de coordinación y mando, especialmente en contextos donde las competencias están distribuidas entre múltiples actores públicos y privados. En Estados Unidos el ataque de *ransomware* a Colonial Pipeline (2021) reveló fallas estructurales, pues aunque la CISA es la principal entidad designada para coordinar la protección de IC, la multiplicidad de agencias estadounidenses implicadas (FBI, Departamento de Energía, autoridades estatales) generó retrasos en la toma de decisiones y en la emisión de directrices unificadas (Bronk & Conklin, 2022). Este episodio reforzó la idea de que en situaciones de crisis resulta imprescindible designar autoridades con competencias jerárquicas claras y autonomía presupuestaria, tal como ocurre en otros modelos centralizados, como la ANSSI, en Francia, o la ACN, en Italia.

En sistemas federales, como Canadá, las lecciones apuntan a la necesidad de armonizar capacidades entre niveles de gobierno. Quigley et al. (2017) advierten que la disparidad de recursos entre las provincias crea zonas de vulnerabilidad desiguales, lo que debilita la capacidad global del Estado para enfrentar amenazas sistémicas. En esos casos los ejercicios conjuntos interjurisdiccionales, así como la homologación de estándares de respuesta, se convierten en prácticas esenciales.

No obstante, incluso con una gobernanza más coordinada, la protección de la IC no depende tan solo de la capacidad técnica o de respuesta interna, sino también de la capacidad para influir en el comportamiento de los actores externos mediante estrategias de disuasión. Empero, la “ciberdisuasión”, concebida como una extensión de los principios clásicos de la “disuasión estratégica”¹⁰, ha mostrado limitaciones significativas en su aplicación práctica, pues, como advierte Wilner (2017), existen al menos tres factores que debilitan su efectividad. En primer lugar, los problemas de atribución, que dificultan demostrar de forma rápida y concluyente la autoría estatal de un ataque, reducen la credibilidad de cualquier amenaza de represalia. En segundo lugar, los bajos umbrales de represalia, ya que los Estados suelen mostrarse reticentes a responder de forma proporcional, ante el temor de desencadenar una escalada no deseada. Finalmente, la ambigüedad normativa persiste como un obstáculo central, por cuanto no existe un consenso internacional sobre

¹⁰ La disuasión estratégica es un principio clásico de las relaciones internacionales y la teoría militar que busca influir en el comportamiento de un adversario mediante la amenaza creíble de represalias tan costosas que hagan irracional cualquier ataque inicial. Según Schelling (1966), la disuasión se basa en la credibilidad, capacidad y comunicación efectiva de la amenaza, y ha sido históricamente asociada a contextos de guerra nuclear y convencional. La ciberdisuasión es la adaptación de este concepto al ciberespacio, orientada a prevenir ataques cibernéticos contra sistemas críticos mediante la amenaza de represalias equivalentes (ya sean cibernéticas o convencionales), o a través de estrategias de negación: es decir, aumentando costos de un ataque mediante defensas robustas.

qué tipo de incidente puede considerarse un acto de guerra cibernética, lo que limita la previsibilidad de las respuestas y, por ende, el efecto disuasorio.

El ataque “WannaCry” (2017), atribuido al grupo norcoreano Lazarus, ilustra estas limitaciones. Aunque el origen fue identificado meses después, las respuestas internacionales se limitaron a la imposición de sanciones económicas, sin efectos disuasorios inmediatos. De forma similar, el *ransomware* contra Colonial Pipeline demostró que actores criminales, incluso sin respaldo explícito de un Estado nación, pueden generar impactos estratégicos significativos, y así erosionar la credibilidad de la disuasión.

Frente a estas limitaciones, Bronk y Conklin (2022), así como Wilner (2017), coinciden en que la disuasión debe ser complementada, pero no reemplazada, por estrategias de resiliencia y “persistencia ofensiva”¹¹. En este orden de ideas, modelos como el estadounidense han transitado hacia la doctrina Defend Forward, en la que se busca anticipar amenazas en redes extranjeras combinando las actividades de ciberinteligencia y operaciones ofensivas preventivas (Slayton, 2023). Sin embargo, este enfoque implica riesgos de escalamiento no intencionado, en especial cuando se emplean *proxies* o actores no estatales fuera del control directo del Estado (Katagiri, 2023).

Si bien la persistencia ofensiva busca contener al adversario en su propio terreno, no elimina la posibilidad de que los ataques lleguen a materializarse. De ahí que la resiliencia adquiera un papel insustituible como última línea de defensa, pues incluso cuando la disuasión y las operaciones preventivas fallan, la capacidad para anticipar, resistir y recuperarse con prontitud de un incidente se convierte en la herramienta estratégica más eficaz frente a amenazas persistentes. Sullivant (2015) propone un modelo de defensa en profundidad que combina segmentación de redes críticas, redundancia operativa y planes de continuidad, mientras que Lewis (2014) subraya la necesidad de considerar la resiliencia no solo un objetivo técnico, sino un componente estructural de la seguridad nacional.

El caso de la red eléctrica de Ucrania es ilustrativo. Tras el apagón de 2015, atribuido al grupo ruso Sandworm, Ucrania implementó medidas de aislamiento de SCADA, capacitación descentralizada de equipos de respuesta y mecanismos manuales de respaldo, lo que redujo significativamente el impacto de ataques posteriores, como “Industroyer2”, en 2022. Este aprendizaje confirma que, si bien

¹¹ La persistencia ofensiva es un enfoque doctrinal en ciberseguridad de los Estados Unidos que busca mantener una presión constante sobre los adversarios en sus propias redes, para anticipar, detectar y neutralizar amenazas antes de que impacten los sistemas nacionales.

no elimina las amenazas, la resiliencia reduce el tiempo de recuperación y mantiene la confianza pública en los servicios esenciales.

Los incidentes recientes también evidencian que los errores humanos y la baja conciencia en ciberseguridad siguen siendo las principales vulnerabilidades en la IC. Zwillling et al. (2022) demostraron que en sectores financieros y sanitarios las brechas de seguridad más explotadas no provienen de fallos tecnológicos, sino de la falta de capacitación en el manejo seguro de las contraseñas, dispositivos personales e identificación de *phishing*. El ataque a Travelex, en 2020, posibilitado por una vulnerabilidad no parcheada en su VPN, evidenció una falla en las políticas de actualización y en la cultura de seguridad organizacional. Las mejores prácticas identificadas en modelos como el NCSC-FI, de Finlandia, o la CISA estadounidense incluyen programas de capacitación continua, auditorías regulares de cumplimiento y ejercicios de simulación, que han demostrado reducir significativamente los incidentes derivados de negligencias humanas.

La mayoría de los ataques recientes confirman que la protección de la IC no es viable sin una colaboración público-privada, tanto estructurada como obligatoria. En muchos países existe una brecha entre la responsabilidad pública de garantizar la seguridad nacional y la dependencia de operadores privados para proteger sectores esenciales. En efecto, casos como "SolarWinds" (2020) evidencian cómo, aunque existan plataformas de intercambio de información, la falta de transparencia y de incentivos claros para el sector privado limita la efectividad de la respuesta. Modelos como el CiSP británico o los Acuerdos de Colaboración de CISA, en Estados Unidos, demuestran que protocolos de notificación obligatoria, incentivos fiscales y ejercicios conjuntos pueden mejorar la detección temprana y reducir el impacto operativo de los ataques.

En síntesis, los casos recientes permiten identificar varias lecciones clave para la protección de la IC. En primer lugar, la centralización del mando y la designación de autoridades con competencias claras resultan fundamentales para garantizar respuestas rápidas y coordinadas ante incidentes a gran escala. En segundo lugar, la ciberdisuasión, aunque necesaria, debe ser complementada con estrategias de resiliencia y persistencia ofensiva, asumiendo que la prevención absoluta es inviable en un entorno caracterizado por amenazas persistentes y actores asimétricos. A ello se suma la necesidad de invertir en una cultura de la ciberseguridad y en la reducción del riesgo humano consolidando programas de capacitación continua y protocolos estrictos de buenas prácticas como prioridad estratégica. Finalmente, la cooperación público-privada, sustentada en marcos regulatorios de carácter obligatorio e incentivos claros, se perfila como un elemento indispensable para fortalecer la capacidad colectiva de defensa.

En conjunto, estos factores constituyen los pilares de un modelo integral de protección de IC, adaptable a contextos como el colombiano. Aunque la madurez institucional y los recursos técnicos sean limitados, la integración progresiva de la resiliencia, la ciberinteligencia y los mecanismos de cooperación estructurada puede reducir de manera significativa la vulnerabilidad frente a amenazas de carácter sistémico.

Ciberinteligencia y persistencia ofensiva

La protección de IC en el contexto actual exige superar enfoques puramente reactivos y avanzar hacia modelos basados en la anticipación estratégica de los ataques cibernéticos. En este marco, la ciberinteligencia y la persistencia ofensiva se han vuelto dos componentes clave y complementarios, pues la primera proporciona el conocimiento necesario para identificar amenazas antes de que se materialicen, mientras la segunda interrumpe proactivamente las capacidades adversarias directamente en su origen, y evita así que los ataques alcancen su fase de ejecución.

Gentry (2023) define la “ciberinteligencia” como el proceso sistemático de recolección, análisis e interpretación de información en el ciberespacio, capaz de generar conocimiento procesable que oriente las decisiones estratégicas, operacionales y tácticas. A diferencia de los sistemas tradicionales de seguridad cibernética, orientados a la detección de incidentes en tiempo real, la ciberinteligencia se basa en el principio de que el análisis anticipado puede ofrecer alertas estratégicas y operacionales, y así reducir la ventana de vulnerabilidad. Según Gentry (2023), este proceso opera en tres niveles interdependientes: 1) estratégico, enfocado en la comprensión del contexto geopolítico y en la identificación de actores estatales y no estatales con motivaciones malignas, sean estas políticas, económicas o militares; 2) operacional, orientado al seguimiento de campañas y APA correlacionando patrones de comportamiento con objetivos específicos, y 3) táctico, centrado en la detección de IoC y sistemas críticos. Este enfoque multinivel permite correlacionar datos aparentemente aislados (como tráfico inusual en redes, dominios registrados con anterioridad o patrones de *malware*) con intenciones estratégicas adversarias, lo que resulta esencial para proteger SCADA, telecomunicaciones y redes eléctricas (Mattern et al., 2014).

Igualmente, la construcción de redes de ciberinteligencia es indispensable para enfrentar amenazas cada vez más complejas y transnacionales. Debido a que los ataques a las IC suelen originarse en múltiples jurisdicciones y emplean vectores distribuidos, ningún actor posee, por sí solo, la visibilidad suficiente para

rastrear las campañas de APA. Estas redes permiten compartir información entre los gobiernos, las empresas y los socios internacionales, y ello amplía el conocimiento situacional y reduce el tiempo de reacción (Pascal & Wieskamp, 2019). Además, la velocidad y el volumen creciente de los ataques hacen esencial la diseminación rápida de IoC, lo que solo es posible mediante mecanismos colaborativos (Gentry, 2023).

Al integrar datos dispersos provenientes de actores diversos, estas redes facilitan la correlación de eventos en apariencia aislados, y ello genera un panorama de amenazas más preciso y útil para la toma de decisiones estratégicas (Mattern et al., 2014). Asimismo, la participación del sector privado (operador de gran parte de la IC) se vuelve crucial, debido a que estas organizaciones suelen ser las primeras en detectar anomalías. Iniciativas como el CiSP, en el Reino Unido, o los acuerdos de intercambio de CISA, en Estados Unidos, evidencian cómo la cooperación público-privada mejora la capacidad colectiva de defensa (Work, 2020). Finalmente, fortalecer esas redes contribuye también a la disuasión indirecta, al mejorar la capacidad de atribución precisa y permitir respuestas diplomáticas o legales más creíbles, y así aumentar los costos estratégicos para el adversario (Rid & Buchanan, 2015).

De acuerdo con Pascal y Wieskamp (2019), las redes de ciberinteligencia pueden clasificarse en jerárquicas, distribuidas o híbridas, dependiendo de su grado de centralización, así como del flujo de intercambio de información. Las jerárquicas, características de modelos centralizados como los de Francia o Taiwán, se sustentan en un mando unificado y en el control directo por parte de una autoridad nacional, para garantizar coherencia en la toma de decisiones y uniformidad en los estándares de seguridad. Sin embargo, este modelo tiende a ser menos flexible en entornos donde múltiples actores gestionan infraestructuras interdependientes. Por su parte, redes distribuidas, como el modelo británico del CiSP, promueven la colaboración público-privada y la participación voluntaria, lo cual favorece la confianza mutua y la rapidez en la compartición de indicadores de compromiso, aunque adolecen de un menor control normativo y presentan disparidades en la calidad de la información compartida.

En el contexto descrito las redes híbridas se han consolidado como la opción más eficaz en ecosistemas complejos, donde confluyen actores públicos, privados e internacionales. Combinando un núcleo de coordinación centralizada con nodos de intercambio voluntario, estos sistemas han mantenido un equilibrio entre control normativo y flexibilidad operativa. Los acuerdos de intercambio de inteligencia de CISA los Estados Unidos son un ejemplo paradigmático: por un lado,

determinan obligaciones legales de notificación para los operadores de infraestructura crítica. Por otro, facilitan canales bidireccionales de cooperación con el sector privado, y mejoran así la detección temprana y la respuesta ante amenazas avanzadas (Work, 2020).

No obstante, uno de los principales desafíos sigue siendo la integración de la inteligencia comercial en estas redes de ciberinteligencia. Como advierte Work (2020), aunque los proveedores privados generan información de alto valor táctico e inmediato (como IoC o firmas de *malware*), suelen carecer de las capacidades analíticas necesarias para contextualizar amenazas a nivel estratégico o relacionarlas con dinámicas geopolíticas. Pese a esta deficiencia, su participación resulta indispensable, pues gran parte de la IC es operada por entidades privadas, y son estas las que, en la mayoría de los casos, detectan las primeras señales de anomalías en sus sistemas informáticos. En consecuencia, su incorporación dentro de modelos híbridos no solo complementa el trabajo de las agencias nacionales al servicio del Estado, sino que también amplía la cobertura de vigilancia, particularmente en sectores con una alta exposición, como suelen ser las telecomunicaciones, el transporte y la banca digital.

En este orden de ideas, la evolución hacia redes de ciberinteligencia híbridas e inclusivas se perfila como un requisito indispensable para fortalecer la resiliencia nacional y garantizar una respuesta coordinada frente a amenazas sistémicas integrando la experiencia táctica de actores privados con el análisis estratégico de las agencias gubernamentales. Con respecto a lo anterior, Colombia se encuentra en una fase incipiente de evolución hacia redes híbridas de ciberinteligencia, ya que la estructura actual es más cercana a un modelo jerárquico fragmentado, con roles definidos para ColCERT¹² y el CCOC¹³, pero sin un sistema integral que

¹² El *Colombian Computer Emergency Response Team* (ColCERT) representa el nodo técnico-operativo del Estado colombiano para la gestión de incidentes cibernéticos a nivel nacional. Creado en 2011 y adscrito a la Presidencia de la República a través de la Dirección Nacional de Inteligencia, su ubicación institucional refleja el reconocimiento del ciberespacio como asunto de seguridad nacional, y no solo como problema técnico-administrativo. ColCERT coordina la respuesta ante incidentes que afecten infraestructuras críticas, sistemas gubernamentales y operadores estratégicos, y funciona como interfaz entre Colombia y la red global de CERT. En términos estratégicos, cumple una función de alerta, contención y resiliencia sistémica frente a amenazas híbridas, ataques patrocinados por Estados y campañas de intrusión persistente avanzada. Sin embargo, el diseño actual presenta desafíos estructurales. Aunque el CONPES 3995 (2020) fortalece su mandato mediante alertas tempranas, análisis forense y ejercicios de simulación, la ausencia de mecanismos obligatorios de reporte para el sector privado limita la construcción de conciencia situacional nacional integrada. En un entorno donde la infraestructura digital es mayoritariamente privada, esta brecha reduce la capacidad del Estado para anticipar y mitigar riesgos sistémicos.

¹³ El Comando Conjunto Cibernético (CCOC) es la estructura especializada de las Fuerzas Militares de Colombia encargada de conducir operaciones en el dominio cibernético. Creado en 2013 y adscrito al Comando General

combine de manera orgánica la capacidad analítica estratégica del Estado con la recolección táctica de información por parte del sector privado. Por ende, el desarrollo de un modelo híbrido implicaría marcos regulatorios claros, incentivos para la notificación obligatoria de incidentes y la creación de nodos de intercambio similares al CiSP o a los acuerdos de CISA.

Ahora bien, como ya se mencionó, la persistencia ofensiva surge como una respuesta a las limitaciones de la ciberdisuasión. A diferencia de los modelos de defensa estática, este enfoque busca mantener una presión constante sobre los adversarios en sus propias redes anticipando y neutralizando amenazas antes de que impacten infraestructuras nacionales. Slayton (2023) señala que esta doctrina, consolidada en el *Defend Forward*, se basa en el despliegue de operaciones de ciberinteligencia activa y acciones ofensivas preventivas para desbaratar campañas en su fase de planificación. Un ejemplo fue la operación del USCYBERCOM contra la Agencia de Investigación de Internet rusa, en 2018, cuando se interrumpieron sus capacidades de propaganda durante las elecciones estadounidenses, mediante intrusiones directas y campañas disruptivas (McConnell & Grzegorzewski, 2022). Otro caso es el de Israel, en 2019, cuando, tras identificar mediante ciberinteligencia actividades hostiles de Hamas, llevó a cabo un ataque cinético contra la unidad cibernética responsable, lo cual demuestra cómo la persistencia ofensiva puede integrarse en una estrategia multidominio (Nguyen & Sparks, 2020)¹⁴.

de las Fuerzas Militares, establecerlo respondió al reconocimiento institucional de que el ciberespacio es no solo un entorno técnico, sino un nuevo dominio operacional que requiere capacidades orgánicas, doctrina propia y planificación estratégica integrada. Su misión consiste en planear, coordinar y ejecutar operaciones de ciberdefensa y ciberseguridad en el ámbito militar, con especial énfasis en la protección de infraestructuras estratégicas del Estado y en la defensa de la soberanía digital frente a amenazas provenientes tanto de actores estatales como de organizaciones criminales transnacionales. En este sentido, el CCOC cumple una función equivalente a la defensa territorial en el dominio físico, trasladada al plano digital. El Comando integra capacidades predominantemente defensivas, complementadas con capacidades ofensivas limitadas y reguladas, orientadas principalmente a la contención de ataques en tiempo real, la neutralización de intrusiones y la protección de redes críticas militares y gubernamentales. Según el CONPES 3995 (2020), mantiene mecanismos de cooperación con ColCERT y otras entidades civiles en escenarios de crisis, aunque su estructura organizacional responde a una lógica jerárquica propia del ámbito castrense. Sin embargo, desde una perspectiva estratégica, persisten desafíos relevantes. La ausencia de mecanismos institucionalizados de intercambio sistemático de inteligencia cibernética con el sector privado limita la construcción de una arquitectura nacional de defensa digital verdaderamente integrada. En un entorno donde buena parte de la infraestructura crítica (telecomunicaciones, energía, finanzas y servicios digitales) es operada por actores privados, esta brecha reduce la capacidad de anticipación y resiliencia sistémica frente a amenazas híbridas y campañas de intrusión persistente avanzada.

¹⁴ Sin embargo, la persistencia ofensiva no está exenta de riesgos. En efecto, Katagiri (2023) advierte que operar en redes extranjeras puede provocar escalamiento no intencionado, especialmente si se utilizan *proxies* o actores no estatales con autonomía táctica. Además, como subraya Buchanan (2020), el uso de *malware* persistente en IC extranjeras puede tener efectos colaterales en sistemas civiles de terceros países, y generar así indeseadas tensiones diplomáticas y cuestionamientos en los foros internacionales.

La sinergia entre ciberinteligencia y persistencia ofensiva es evidente, pues la primera proporciona el conocimiento situacional que reduce la incertidumbre operativa, mientras la segunda actúa como instrumento disuasorio y preventivo. No obstante, la persistencia ofensiva solo es efectiva cuando está sustentada en una inteligencia confiable, oportuna y contextualizada, capaz de diferenciar entre actividades preparatorias reales y ruidos de fondo en el tráfico digital (Mattern et al., 2014). Los casos recientes también muestran que la ciberinteligencia estratégica debe priorizar la atribución precisa. Rid y Buchanan (2015) afirman que la atribución técnica, complementada con análisis contextual, no solo mejora la eficacia de las operaciones ofensivas, sino que aumenta el valor disuasorio al permitir respuestas diplomáticas o jurídicas más creíbles.

Para Colombia, cuya capacidad ofensiva en el ciberespacio aún tiene margen de mejora, la prioridad inmediata debe centrarse en la construcción de un sistema nacional de ciberinteligencia sólido y articulado. Esto requiere, en primer lugar, el desarrollo de redes nacionales de intercambio de inteligencia que integren agencias estatales y organizaciones privadas en un modelo híbrido similar al CiSP británico, combinando coordinación centralizada con flujos bidireccionales de información. En segundo lugar, es imprescindible invertir en capacidades analíticas estratégicas y operacionales superando la actual dependencia de proveedores comerciales, cuya inteligencia, aunque valiosa en el plano táctico, resulta insuficiente para anticipar amenazas de carácter sistémico.

Asimismo, el fortalecimiento de las capacidades de atribución y del análisis contextual permitiría, en el mediano plazo, legitimar una doctrina de persistencia ofensiva limitada, orientada a la disuasión y neutralización de las amenazas críticas sin comprometer la estabilidad regional. Esta persistencia ofensiva, no obstante, debe integrarse en un marco más amplio de resiliencia, de modo que funcione como un recurso excepcional, y no como el núcleo de la defensa nacional. En síntesis, una ciberinteligencia robusta, articulada con las capacidades selectivas de persistencia ofensiva, constituye hoy un pilar de la protección de las IC. Sin embargo, su implementación exige mantener un equilibrio entre proactividad y prudencia, privilegiando la anticipación y la resiliencia como bases de una estrategia sostenible, jurídicamente legitimada y compatible con el derecho internacional.

El caso colombiano: riesgos, capacidades y estrategias

La evolución del internet en Colombia ha sido un proceso progresivo que ha transformado profundamente la dinámica económica, social y política, y sentado las

bases para su actual dependencia digital y, en consecuencia, también las de la creciente preocupación por proteger la IC cibernética (ICC). El salto tecnológico en materia de las tecnologías de la información y las comunicaciones (TIC) comenzó en 1986, cuando la Universidad de los Andes instauró el Programa Hermes, una iniciativa pionera que ofrecía a sus dependencias acceso gratuito a servicios de computación, así como el fomento de la alfabetización digital dentro de la comunidad universitaria. Gracias a este impulso uniandino, el centro de cómputo fue modernizado, y para 1988 se consolidó la Red de la Universidad de los Andes (RDU), una red interna que dos años más tarde logró expandir su conectividad a la Biblioteca Luis Ángel Arango (1990), lo cual marcó uno de los primeros hitos en la interconexión de instituciones en el país.

En la misma línea, la Universidad de los Andes se afilió a Bitnet, una red internacional de computadores creada en Estados Unidos y considerada una de las precursoras de Internet. Bitnet era utilizada por instituciones académicas de todo el mundo para compartir información a través de correo electrónico y otros servicios interactivos, lo que permitió a Colombia integrarse tempranamente a un circuito global de intercambio científico y tecnológico. Este interés académico en acceder al ciberespacio condujo poco después a la creación de la Red Universitaria Nacional de Colombia (Runcol), concebida como la primera red interuniversitaria del país. A este proyecto se unieron la Universidad Nacional, la Universidad del Valle, la Universidad del Norte, la Universidad Industrial de Santander y la Universidad EAFIT, con el apoyo técnico y financiero de Telecom¹⁵ (la entonces empresa estatal de telecomunicaciones), así como del Instituto Colombiano para el Fomento de la Educación Superior (ICFES). La Runcol se convertiría así en el germen de las primeras redes académicas nacionales, y sentó las bases para el posterior desarrollo del internet comercial en Colombia.

Con la llegada de Bitnet II, en 1991, la Universidad de los Andes liberó las direcciones IP que hasta ese momento utilizaba, las cuales pertenecían a la Universidad de Columbia, en Estados Unidos. A partir de entonces se inició el trámite ante el Internet Network Information Center (InterNIC), el organismo responsable de la asignación de dominios y direcciones IP en esa época, para obtener nuevas direcciones propias. Como resultado de dicho proceso, el dominio de nivel superior “.CO” comenzó a ser administrado por la Universidad de los Andes, en lo que fue

¹⁵ En ese entonces los procesos de conexión eran muy costosos: tanto, que un canal de 9,6 kb por segundo costaba alrededor de 10.000 dólares mensuales, lo cual era una suma enorme para las universidades colombianas. Por ende, Telecom ayudó a subsidiar una parte de los costos mediante cursos y consultorías, y la otra, en dinero.

un hito para la inserción de Colombia en la naciente red global. Posteriormente, la administración de este dominio pasó a manos del Estado, a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y se consolidó como un activo digital estratégico del país.

Actualmente, el dominio “.CO” ha experimentado un crecimiento exponencial. Lo que inició con apenas 27.000 páginas registradas ha multiplicado su operación en más de 80 veces, al alcanzar más de 3,2 millones de dominios activos en 190 países. De acuerdo con datos de MinTIC (2024), el “.CO” era el segundo mayor dominio de América Latina y el número 19 en todo el mundo, y contaba con más de 7.000 páginas posicionadas dentro del top del millón de sitios más visitados en el *ranking* de Alexa. En Colombia hay alrededor de 300.000 páginas registradas bajo dicha extensión, una cifra significativa en proporción con la población y el nivel de digitalización nacional. Un hecho relevante en la evolución reciente del dominio es que, tras años de estar operado por la empresa estadounidense Neustar Inc., MinTIC adjudicó en 2025 su operación a una empresa colombiana, y dio así un paso hacia la recuperación de la soberanía digital sobre este activo. Según cifras oficiales, en los últimos cinco años la gestión del dominio “.CO” ha generado ingresos superiores a los 500.000 millones de pesos, por lo cual se consolida no solo como un recurso de identidad digital, sino también como una fuente estratégica de recursos económicos para el país (MinTIC, 2024).

Este control reciente del dominio “.CO” y su creciente relevancia económica contrastan con los primeros años de desarrollo de internet en el país, cuando aún no se percibía su potencial estratégico. En la década de 1990 Colombia apenas comenzaba a dar sus primeros pasos en el ciberespacio, y a pesar del entusiasmo de las universidades, tanto el Gobierno como el sector empresarial subestimaban el impacto transformador que tendría esta tecnología. Un ejemplo ilustrativo fue la decisión del entonces Consejo Nacional de Ciencia y Tecnología (Colciencias) de rechazar en 1992 un proyecto destinado a financiar la conexión oficial del país a la red global. Sin embargo, la comunidad académica insistió, y mediante un trabajo colaborativo diseñó el “*Backbone* nacional”, un eje dorsal de interconexiones administrado por la National Science Foundation (NSF) de Estados Unidos.

Este avance motivó un cambio de postura, pues en 1993 Colciencias asumió el costo inicial de la inversión, lo que permitió crear InterRed, una corporación privada, integrada por representantes del entonces Instituto Colombiano para el Fomento de la Educación Superior (ICFES), Colciencias, la Universidad EAFIT, la Universidad del Valle y la Universidad Nacional, entre otras instituciones. La

infraestructura necesaria se instaló en el centro de cómputo de la Universidad de los Andes, mientras que la NSF donó un enrutador exclusivo para Latinoamérica, ubicado en Homestead (Florida), que sirvió como punto de enlace internacional. Este hito consolidó la primera conexión estable del país a la red global y marcó el inicio de su integración al ecosistema digital mundial. Con el arribo formal de Internet a Colombia, el 4 de junio de 1994, cuando la señal llegó desde Florida al centro de operaciones de Impsat (ubicado en el cerro de Suba, en Bogotá), y desde allí, al edificio Colpatria y a la Universidad de los Andes, el país inició una transformación digital gradual que en la última década se ha acelerado exponencialmente.

De acuerdo con el Boletín Trimestral de las TIC (MinTIC, 2025a), el número de accesos fijos a internet pasó de 7 millones en 2019 a 9,09 millones al cierre de 2024, lo que equivale a 17 accesos por cada 100 habitantes. Tecnologías como la fibra óptica han impulsado este crecimiento, representado por 4,5 millones de accesos, seguidas por el cable coaxial, con 4,1 millones. La velocidad de descarga promedio nacional se situó en 227,2 Mbps, con Bogotá a la cabeza, y alcanzar 289,4 Mbps en el segmento residencial. En cuanto al internet móvil, el país alcanzó 49,4 millones de accesos al cierre de 2024, lo que representa 93,8 accesos por cada 100 habitantes.

La tecnología 4G sigue siendo la dominante, con 41,5 millones de accesos, aunque la 5G ha experimentado un crecimiento acelerado, al alcanzar 3,8 millones de accesos, con una variación trimestral del 37,3 %. Pese a que la cobertura 5G aún es limitada (el 2,28 % de los municipios), la infraestructura LTE y 4G cubre el 100 % del territorio. El avance en la conectividad también se refleja en la expansión de la infraestructura en zonas apartadas. Según datos de MinTIC (2025), el 98 % de los municipios colombianos ya cuentan con conexión al ciberespacio, y más de 6.900 Kioscos Vive Digital¹⁶ han sido instalados en áreas rurales, lo que permite acceso comunitario a internet, telefonía IP y servicios básicos digitales.

En línea con esta transformación digital, la llegada de la tecnología 5G marca un nuevo hito en la conectividad nacional. La subasta de espectro realizada en diciembre de 2023 por MinTIC, especialmente en la banda de 3500 MHz, permitió adjudicar bloques a operadores como Claro, WOM, la alianza Tigo-Movistar y un nuevo actor: Telecall. Esta adjudicación, formalizada en febrero de 2024, habilitó el

¹⁶ Es un espacio que garantiza el acceso a las TIC mediante un modelo de servicios que permite integrar a la comunidad en escenarios de acceso, capacitación, entretenimiento y otras alternativas de servicios TIC en lugares de difícil acceso o precaria infraestructura. Cabe resaltar también la importancia de la Estrategia de "Gobierno en Línea", implementada desde 2008 por parte de MinTIC, y que ha sido una herramienta clave para avanzar en todos los planes de modernización administrativo del Estado colombiano.

inicio del despliegue oficial de redes 5G en el país. Para marzo de 2024 más de 1,6 millones de colombianos ya habían accedido a servicios 5G, lo que abrió paso a un ecosistema que promete transformaciones profundas en sectores industriales, logísticos, manufactureros, portuarios y de servicios públicos, así como en el ámbito del consumo masivo (TicTac, 2024).

El 5G en Colombia permitirá mayor velocidad de conexión, baja latencia y una capacidad ampliada para conectar simultáneamente miles de dispositivos, características clave para impulsar soluciones de Internet de las Cosas (IoT), realidad aumentada, computación en el borde y vehículos autónomos. Además, facilitará el acceso inalámbrico fijo (FWA), especialmente en zonas donde la infraestructura de última milla ha sido históricamente limitada o costosa, lo que representa una oportunidad real para cerrar la brecha digital rural. Según estimaciones del mismo informe, se espera que para 2030 esta tecnología represente el 44 % de las conexiones móviles del país y cubra al 68 % de la población, y fortalezca así no solo la inclusión digital, sino también la competitividad de Colombia en el entorno latinoamericano y global (TicTac, 2024).

Radiografía cibernética y de la infraestructura crítica en Colombia

La protección de la ICC colombiana se configura hoy como un imperativo estratégico frente a la creciente dependencia tecnológica del país y la convergencia entre seguridad nacional, defensa y desarrollo económico¹⁷. El concepto IC ha evolucionado en Colombia desde una visión sectorial hacia una comprensión más sistémica, centrada en la interdependencia de sistemas ciberfísicos, donde los componentes digitales (sensores, redes, algoritmos), controlan y optimizan funciones físicas esenciales. Bajo esta lógica, se entiende por ICC el conjunto de activos físicos y virtuales soportados por TIC y cuya afectación tendría un impacto grave en el bienestar económico y social de los ciudadanos o en el funcionamiento del Estado (MinTIC, 2022).

Los sectores típicamente priorizados incluyen los de la energía, transporte, agua, salud, telecomunicaciones, defensa, finanzas y alimentación, así como los servicios gubernamentales. Si estas infraestructuras no logran mantener un nivel

¹⁷ Según el CONPES 3854 de 2016, la infraestructura crítica cibernética nacional es “aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública” (DNP, 2016, p. 29).

mínimo de operación tolerable, o en caso de colapso, pueden comprometer la seguridad multidimensional del Estado (Álvarez & Zambrano, 2017). En efecto, la mayoría de esas infraestructuras funcionan como sistemas ciberfísicos; por ejemplo, en una central eléctrica los sensores y los actuadores interactúan constantemente para monitorear el estado del sistema, enviar información al centro de control y ejecutar comandos que modifiquen el comportamiento de los componentes físicos según como se requiera. La naturaleza crítica de dichos sistemas exige modelos de gestión basados en criterios de nodos de riesgo, niveles de criticidad, continuidad operativa y capacidades de respuesta claramente definidas¹⁸.

La identificación y evaluación de la ICC puede variar de un Estado a otro, en función de su nivel de desarrollo tecnológico, normativas, y de la dependencia de sus sectores estratégicos con respecto a las TIC. En el caso colombiano, la formulación de una política pública en esta materia se remonta al CONPES 3701 de 2011, el cual estableció los “Lineamientos de Política para Ciberseguridad y Ciberdefensa”. Su objetivo fue “fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético, creando un ambiente y unas condiciones para brindar protección en el ciberespacio” (DNP, 2011, p.13). Esta política propuso tres líneas fundamentales de acción: 1) establecer instancias institucionales para la prevención y regulación de amenazas cibernéticas; 2) desarrollar capacidades mediante formación e investigación en ciberseguridad y ciberdefensa¹⁹, y 3) reforzar el marco legal e impulsar la cooperación internacional en la materia.

Uno de los logros más destacados de dicha política fue el fortalecimiento institucional del aparato estatal en materia ciberespacial²⁰. En efecto, se crearon entidades especializadas como el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) en el Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares, el Centro

¹⁸ Por consiguiente, el Estado colombiano ha desarrollado una estrategia de ciberdefensa en relación con la integridad de las redes eléctricas, ya que la electricidad no tiene sustituto, y todas las demás infraestructuras dependen eventualmente de ella.

¹⁹ Labor en la cual se han destacado por sus aportes la Maestría en Ciberseguridad y Ciberdefensa, así como la Maestría en Seguridad y Defensa Nacionales, ambas de la Escuela Superior de Guerra “General Rafael Reyes Prieto” (ESDEG).

²⁰ El Documento CONPES 3701 definió la ciberseguridad como “la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética”; y “ciberdefensa” como “la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional” (DNP, 2011, p.13).

Cibernético Policial (CCP) y el CSIRT²¹ de la Policía Nacional, y la Delegatura de Protección de Datos Personales en la Superintendencia de Industria y Comercio, así como las estructuras técnico-operativas dentro de MinTIC y los comités de ciberdefensa en las tres Fuerzas (Ejército, Armada y Fuerza Aeroespacial)²².

Por consiguiente, el interés en la protección de la ICC en Colombia se intensificó a partir de 2011, y ese año el Comando General de las Fuerzas Militares definió los primeros lineamientos doctrinales sobre la materia. El proceso alcanzó un hito entre 2015 y 2016, cuando el CCOC elaboró tres documentos: 1) la *Guía para la Identificación de Infraestructura Crítica Cibernética*, de 2015; 2) los *Sectores Estratégicos desde la Óptica Cibernética*, de 2016, y 3) el *Catálogo de Infraestructura Crítica Cibernética de Colombia*, de 2016. Los tres instrumentos sentaron las bases para una estrategia nacional de defensa cibernética basada en la identificación de activos críticos, vectores de amenaza específicos y principios de continuidad operativa.

En particular, la elaboración del documento *Catálogo de Infraestructuras Críticas Cibernéticas Nacionales* (de carácter reservado) permitió establecer una metodología común para coordinar y gestionar los planes y programas de protección y defensa de los activos digitales esenciales de Colombia (DNP, 2016). Para su desarrollo, cada sector de la ICC (establecidos en *Sectores Estratégicos desde la Óptica Cibernética*) levantó información sobre su infraestructura digital prioritaria e identificó interdependencias con otras infraestructuras físicas del ecosistema de IC evaluando la continuidad de las operaciones frente a las amenazas latentes.

²¹ Un CSIRT (por las iniciales en inglés de *Computer Security Incident Response Team*) es una unidad técnica especializada a cargo de la gestión integral de incidentes de seguridad cibernética dentro de una organización, sector o IC determinados. Su función central no se limita a reaccionar ante eventos adversos, sino que consiste en estructurar un ciclo continuo de detección, análisis, contención, erradicación y recuperación frente a amenazas digitales. En términos operativos, el CSIRT actúa como primera línea de defensa ante intrusiones, vulnerabilidades explotadas, campañas de *malware*, ataques de DoS o filtraciones de información sensible. Su misión es reducir el tiempo de exposición al riesgo, limitar el daño sistémico y restaurar la normalidad operativa con el menor impacto posible sobre los activos críticos. Más allá de la respuesta inmediata, el CSIRT cumple una función estratégica de aprendizaje organizacional. Mediante el análisis de causa raíz, la correlación de eventos y la generación de inteligencia técnica, produce alertas tempranas, recomendaciones de mitigación y ajustes en políticas de seguridad. De este modo, contribuye a fortalecer la postura de ciberseguridad institucional y a incrementar la resiliencia frente a amenazas recurrentes o persistentes. Desde una perspectiva sistémica, el CSIRT constituye un nodo operativo dentro de la arquitectura más amplia de gobernanza digital conectando la dimensión técnica con la dimensión estratégica de la gestión del riesgo en el ciberespacio.

²² Adicionalmente, en el marco del Documento CONPES 3701 de 2011, se creó la Comisión Nacional Digital y de Información Estatal, mediante el Decreto 32 de 2013 de MinTIC, con el objetivo de ejercer la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para interacción con los ciudadanos y el uso efectivo de la información en el Estado colombiano. Sobre el particular se hablará ampliamente en el capítulo VII de esta obra.

Posteriormente, las partes interesadas²³ remitieron esta información al Ministerio de Defensa, que se encargó de clasificar, priorizar y definir el grado de criticidad de cada uno de los activos y entidades. El resultado fue una matriz de criticidad que debía constituirse en el insumo técnico principal para la formulación de una Estrategia Nacional de Protección y Defensa de la ICC.

Con la publicación, en 2025, de la “Estrategia Nacional de Seguridad Digital de Colombia 2025-2027”, Colombia dio un paso significativo hacia la estructuración de una política pública integral para fortalecer el ecosistema digital colombiano. Este instrumento, liderado por el Gobierno nacional (2025), a través del coordinador nacional de Seguridad Digital, define líneas de acción concretas para la protección de IC, el aseguramiento de servicios esenciales, la promoción de una cultura de ciberseguridad y el fortalecimiento de capacidades técnicas e institucionales. En particular, la Línea de Acción 2.2 de la “Estrategia Nacional de Seguridad Digital de Colombia 2025-2027” propone el diseño de una estrategia integral de protección de IC y servicios esenciales, con énfasis en su identificación, clasificación y monitoreo continuo, así como el uso de arquitecturas basadas en el principio de *Zero Trust*²⁴ y la formulación de planes de resiliencia cibernética en cadenas de suministro.

Asimismo, la Línea de Acción 2.3 de la estrategia contempla el fortalecimiento de las capacidades de ciberdefensa del Estado colombiano, mediante el uso de tecnologías emergentes como la IA y el aprendizaje automático, la coordinación de CSIRT del sector defensa con otros equipos de respuesta a incidentes cibernéticos y la realización de ejercicios regulares de simulación frente a amenazas avanzadas como *deepfakes* o ataques con base en el uso de IA. Cabe resaltar que, si bien dichas acciones aluden indirectamente al rol de las Fuerzas Militares colombianas y organismos de inteligencia, la estrategia no destaca explícitamente su participación, lo cual plantea interrogantes sobre la profundidad de la articulación civil-militar en el diseño del marco estratégico vigente.

²³ Lo constituyen todos los que dependan del entorno digital para todas o algunas de sus actividades económicas y sociales, y quienes puedan ejercer distintos roles y tener distintas responsabilidades, como el Gobierno nacional, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las ICC nacionales, la academia y la sociedad civil.

²⁴ El modelo de seguridad *Zero Trust* (confianza cero) es un enfoque arquitectónico que parte del principio de que ningún usuario, dispositivo o sistema debe ser confiado por defecto, incluso si se halla dentro del perímetro de la red. En vez de asumir confianza interna, *Zero Trust* establece controles de acceso estrictos, autenticación continua y monitoreo constante, con base en el principio de “Nunca confíes, siempre verifica”. Su implementación busca reducir la superficie de ataque, limitar movimientos laterales dentro de redes comprometidas y fortalecer la resiliencia frente a amenazas persistentes avanzadas.

En ese contexto resulta estratégico que las Fuerzas Militares, a través del CCOC, se integren activamente en la implementación de la “Estrategia Nacional de Seguridad Digital 2025-2027” articulando sus funciones de defensa cibernética con las líneas de acción definidas en el documento. Si bien la estrategia tiene un enfoque marcadamente civil, la protección efectiva de IC y la respuesta ante amenazas complejas (como ciberataques dirigidos a servicios esenciales, sabotajes digitales o campañas de desinformación con efectos estratégicos) exige una visión de seguridad digital como asunto de interés nacional y multidimensional, que convoque capacidades tanto civiles como militares. En este sentido, el conocimiento doctrinal acumulado por el CCOC, la experiencia de las Fuerzas Militares en análisis de amenazas, ciberinteligencia y respuesta a incidentes, así como su cultura operativa y disciplina estratégica, pueden aportar valor agregado en escenarios donde se requiera actuar bajo condiciones de alta complejidad y riesgo.

Además, las Fuerzas Militares pueden liderar o acompañar el desarrollo de capacidades específicas contempladas en la estrategia, como la creación de CSIRT sectoriales críticos²⁵, la adopción de arquitecturas de seguridad avanzadas (*Zero Trust*), la ejecución de ejercicios conjuntos de simulación de ciberataques y la formulación de planes de resiliencia cibernética para las ICC. Esta participación no implica una “militarización” de la seguridad digital, sino una sinergia necesaria bajo criterios de subsidiariedad, complementariedad técnica y corresponsabilidad del Estado, en el marco de una gobernanza que respete la división civil-militar y se rija por principios democráticos, transparencia y eficacia.

En cuanto a la evolución normativa, se han mostrado avances fragmentados. Desde la Ley 527 de 1999, sobre comercio electrónico, hasta el CONPES 3995 de 2020, sobre confianza y seguridad digital, el país ha estructurado una arquitectura jurídica parcial, que no siempre se traduce en capacidades institucionales robustas (González & Acevedo, 2021). Uno de los mayores avances normativos ha sido

²⁵ Los CSIRT sectoriales son equipos de respuesta a incidentes de seguridad digital establecidos dentro de cada sector económico o social. Su función principal es garantizar la protección de los activos digitales y la continuidad operativa frente a amenazas cibernéticas, mediante la gestión oportuna de incidentes asociados al uso de TIC. En Colombia existen ejemplos como el CSIRT Financiero, coordinado por la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria), que brinda apoyo a las entidades del sistema financiero para prevenir y responder a fraudes electrónicos, o el CSIRT Académico, que atiende incidentes en el ámbito universitario y científico. Un CSIRT sectorial crítico se refiere a los equipos de respuesta a incidentes cibernéticos pertenecientes a sectores identificados como IC nacionales, debido a su relevancia para la seguridad, la economía y el funcionamiento del Estado. Dichos CSIRT desempeñan un rol estratégico, ya que se encuentran enfocados en servicios esenciales cuya interrupción tendría consecuencias graves. En el contexto colombiano destacan iniciativas como el CSIRT de Energía, vinculado al sector minero-energético y coordinado por el Ministerio de Minas y Energía, o el CSIRT de Salud, orientado a salvaguardar la ciberseguridad de hospitales, entidades promotoras de salud (EPS) y plataformas del sistema de salud pública.

el Decreto 338 de 2022, que establece lineamientos generales para la gobernanza de la seguridad digital, la identificación de ICC, la gestión de riesgos y la respuesta a incidentes. Sin embargo, su enfoque, centrado en el aparato estatal, y su escasa articulación con el sector privado han sido duramente cuestionados (Cabrera, 2024). Esta exclusión es problemática, dado que la mayoría de los servicios críticos (como la energía, la salud, el transporte y las telecomunicaciones) son concesionados o controlados por actores privados, lo que requiere una gobernanza de tipo colaborativo y multisectorial.

La creación, en 2024, del Centro de Operaciones de Seguridad Nacional (SOC), liderado por MinTIC, representa un esfuerzo importante para blindar digitalmente a las entidades públicas (MinTIC, 2025b), pero su alcance aún es limitado frente a los desafíos de ciberresiliencia de todo el ecosistema nacional. Esta brecha entre capacidades institucionales y amenazas reales se ha evidenciado con crudeza en los últimos años, donde los incidentes cibernéticos han superado con creces las previsiones y los niveles de preparación. Tan solo en 2023, Colombia enfrentó incidentes severos que afectaron simultáneamente a 25 entidades públicas, incluyendo la Fiscalía, la Superintendencia de Industria y Comercio y la Rama Judicial. Estos eventos evidencian la fragilidad del sistema y la necesidad apremiante de actualizar los protocolos, incluir al sector privado en el diseño de políticas y fortalecer a los CSIRT sectoriales. Además, las cifras de incidentes muestran una tendencia alarmante.

Según el *X-Force Threat Intelligence Index 2025*, Colombia fue el cuarto país latinoamericano con el mayor número de ciberataques en 2024, al registrar más de 36.000 millones de intentos de intrusión, y 20.000 millones de ellos tan solo en el primer semestre (La República, 2025). Esta cifra refleja una creciente vulnerabilidad estructural, especialmente en sectores como manufactura (26 %) y servicios financieros (23 %), que se han convertido en blancos prioritarios de actores maliciosos. A nivel global, IBM (2024) estimó que el costo promedio por violación de datos alcanzó los 4,9 millones de dólares en 2024, lo que amplifica la gravedad del panorama para economías en desarrollo, como la colombiana, donde los recursos para defensa digital son limitados.

Aunque América Latina representó apenas el 8 % de las amenazas globales (una disminución frente al 12 % de años anteriores), la magnitud de los intentos en Colombia evidencia una superficie de ataque amplia y en expansión. A esto se suma la detección de más de 22.000 vulnerabilidades por parte del Equipo de Respuesta a Emergencias Cibernéticas (ColCERT), lo que confirma la fragilidad de sistemas

críticos frente a vectores de ataque recurrentes como *ransomware*, *phishing*, *malware* y denegación de servicio (DDoS). La situación impacta de forma directa la confianza institucional, la estabilidad operativa y la seguridad de los servicios esenciales, y pone en evidencia la urgencia de fortalecer las capacidades nacionales en detección, prevención y respuesta frente a amenazas sofisticadas y dirigidas.

En el contexto colombiano, la seguridad cibernética tiene un matiz singular. Como lo señala Chenou (2021), la noción misma de “seguridad” en el ciberespacio es objeto de disputa en una sociedad marcada por conflictos armados, desigualdad y falta de confianza en las instituciones. En ese sentido, el enfoque tecnocrático y estatalista de las políticas actuales contrasta con la necesidad de una gobernanza más participativa, territorializada y centrada en la resiliencia de las comunidades y los ecosistemas digitales descentralizados. A nivel internacional, Colombia ha recibido cooperación y recomendaciones para cerrar brechas de capacidades. Sin embargo, los esfuerzos globales en ciberseguridad muestran una asimetría estructural, donde las democracias, como la de Colombia, enfrentan desafíos para acceder a tecnología, marcos de gobernanza y conocimiento experto en igualdad de condiciones (Calderaro & Craig, 2020).

La radiografía cibernética e infraestructural de Colombia muestra un país que avanza, pero a un ritmo desigual frente a la sofisticación del entorno cibernético²⁶. Los documentos doctrinales del CCOC, las reformas normativas recientes, como el Decreto 338 de 2022 y la creación de instancias como el SOC nacional, son pasos importantes, pero aún insuficientes. Por lo tanto, se requiere una verdadera política de resiliencia nacional que combine interoperabilidad institucional, cooperación multisectorial, formación de talento especializado, inversión en ciberinteligencia y una cultura de seguridad digital transversal. Solo de esa manera podrá protegerse adecuadamente lo que hoy es el corazón digital del Estado.

Propuestas para una arquitectura nacional de ciberseguridad

El contexto actual en Colombia, marcado por una acelerada digitalización y una creciente sofisticación de las amenazas, demanda una arquitectura nacional de ciberseguridad robusta, interoperable y resiliente. Pero esa arquitectura no debe entenderse únicamente como un conjunto de normas y tecnologías, sino también

²⁶ La masificación del 5G en Colombia (aún incipiente, pero en curso) añade nuevas dimensiones al problema. Como advierte el documento de TICTAC (2024), la llegada de redes 5G transforma la IC al integrar IoT, automatización industrial, ciudades inteligentes y datos en tiempo real. Esto amplía el perímetro de riesgo y obliga a repensar la noción de IC no solo como infraestructura “física conectada”, sino como un sistema sociotécnico de alta complejidad, interdependiente y vulnerable.

como un sistema sociotécnico compuesto por instituciones, capacidades humanas, esquemas de gobernanza y mecanismos de cooperación entre múltiples actores. La experiencia reciente de Colombia (desde el aumento exponencial de los ciberataques a entidades públicas hasta la exposición de sectores críticos como salud, energía, justicia y finanzas) confirma que la protección del ciberespacio ha dejado de ser una cuestión técnica para convertirse en un asunto de seguridad nacional y estabilidad institucional (Solar, 2020; Cabrera, 2024).

Una primera propuesta sería el diseño de una efectiva gobernanza integrada de ciberseguridad y ciberdefensa que logre superar el actual esquema fragmentado. Colombia ha desarrollado múltiples iniciativas desde diferentes entidades (MinTIC, CCOC, ColCERT, Fiscalía, Policía Nacional), pero sin un ente rector con autoridad, coordinación transversal y presupuesto suficiente. Por lo tanto, se hace necesaria la creación de una Agencia Nacional de Ciberseguridad, con autonomía técnica, financiera y administrativa, que le garantice independencia frente al ciclo político y continuidad en su accionar estratégico. Dicha entidad deberá encargarse de liderar la formulación, implementación, articulación interinstitucional y evaluación de la política nacional de ciberseguridad, así como de coordinar esfuerzos del Estado y del sector privado en materia de prevención, respuesta y resiliencia frente a las amenazas digitales²⁷.

En países como Colombia, donde las Fuerzas Militares han desempeñado un rol protagónico en la defensa del ciberespacio, resulta estratégico avanzar hacia un modelo de gobernanza que complemente ese liderazgo con el fortalecimiento de capacidades civiles especializadas. Más que un riesgo de militarización, el desafío consiste en articular sinergias entre el conocimiento operativo del sector defensa en Colombia y las competencias normativas, regulatorias y técnicas de las entidades civiles, bajo principios de coordinación, de transparencia y de corresponsabilidad. Tal enfoque no solo amplía el alcance de la ciberseguridad nacional, sino que legitima su implementación ante la ciudadanía y los actores no estatales comprometidos con la defensa del entorno digital (Solar, 2020).

²⁷ En 2023 el Gobierno nacional radicó ante el Congreso el Proyecto de Ley 023, para la creación de la Agencia Nacional de Seguridad Digital y Asuntos Espaciales, con el fin de fortalecer la ciberseguridad del país y establecer una política nacional en materia espacial. Sin embargo, agrupar dos dominios estratégicos distintos (el ciberespacio y el espacio ultraterrestre) en una sola entidad presenta serias limitaciones operativas e institucionales, pues sus misiones, marcos regulatorios, capacidades técnicas y horizontes estratégicos difieren sustancialmente. Mientras el ciberespacio exige respuestas inmediatas, articulación multisectorial y vigilancia constante, el sector espacial requiere planificación de largo plazo, cooperación científica e inversión tecnológica sostenida. Por ello, se recomienda establecer dos agencias separadas: una Agencia Nacional del Ciberespacio y una Agencia Colombiana del Espacio, para garantizar eficacia, especialización y una gobernanza adecuada en ambos campos.

Un segundo eje estratégico es el fortalecimiento del marco normativo para la identificación y protección de la ICC. Aunque el Decreto 338 de 2022 representa un avance importante, al establecer lineamientos para la identificación de estos activos, persisten vacíos en su implementación efectiva, sobre todo en lo referente a la articulación con el sector privado, que opera gran parte de los servicios esenciales. Es imprescindible construir un catálogo nacional dinámico y clasificado de ICC, con base en criterios técnicos de dependencia digital, impacto social y económico, y vulnerabilidad sistémica, como los desarrollados inicialmente por el CCOC en sus documentos reservados entre 2015 y 2016. Adicionalmente, ese catálogo debe estar vinculado a esquemas obligatorios de auditoría de ciberseguridad y planes de continuidad operativa, así como a ejercicios de simulación de incidentes cibernéticos y mecanismos de reporte obligatorio de brechas. Solo una comprensión sistémica de los activos críticos permitirá desarrollar capacidades de resiliencia organizacional ante ciberataques dirigidos, sabotajes digitales y campañas de desinformación vinculadas a amenazas híbridas.

El desarrollo del talento humano constituye una piedra angular para el éxito de cualquier arquitectura nacional de ciberseguridad. Colombia ha hecho avances significativos en este frente, en particular desde el ámbito de la defensa. Un ejemplo destacado es la Maestría en Ciberseguridad y Ciberdefensa, de la Escuela Superior de Guerra “General Rafael Reyes Prieto” (ESDEG), que ha contribuido a la formación de profesionales con alta preparación técnica, operativa y estratégica, capaces de afrontar los desafíos del entorno digital desde una perspectiva integral de seguridad nacional. No obstante, la velocidad a la que evolucionan las amenazas cibernéticas plantea un desafío persistente en términos de cobertura y especialización.

Aún se observa una brecha considerable en la disponibilidad de personal calificado en áreas clave como seguridad de la información, análisis forense digital, ciberinteligencia, respuesta a incidentes, protección de IC y gobernanza de datos. Esta brecha es sobre todo notoria en entidades civiles, territoriales y empresas estratégicas que carecen de cuadros técnicos suficientes para anticipar, contener y recuperar sus operaciones frente a ataques sofisticados. Frente a ese panorama, se propone la creación de un Sistema Nacional de Formación en Ciberseguridad, articulado entre universidades, centros de investigación, instituciones de formación técnica y tecnológica, y las Fuerzas Militares. Dicho sistema debería estar basado en un enfoque por competencias, alineado con estándares internacionales, y orientado tanto a la formación inicial como a la actualización continua de los profesionales de los sectores público y privado.

Además, una arquitectura educativa así debe incorporar una estrategia nacional de cultura digital, orientada a fortalecer la conciencia ciudadana sobre los riesgos del entorno digital y promover prácticas seguras desde la educación básica. La alfabetización en seguridad digital, el uso ético de la tecnología, la protección de datos personales y la prevención del delito cibernético deben formar parte del currículo escolar y de las campañas de comunicación institucional. En conjunto, estas iniciativas permitirán consolidar un ecosistema de talento humano capaz de sostener, expandir y adaptar la defensa cibernética del país ante escenarios de alta complejidad y evolución constante.

Una arquitectura nacional de ciberseguridad debería también fomentar el desarrollo de ecosistemas de cooperación público-privada, basados en la confianza, el intercambio de información y la corresponsabilidad frente a los riesgos digitales, ya que los ataques más devastadores no distinguen entre sectores estatales y privados, y su mitigación depende de la capacidad conjunta para prevenir, detectar y responder con rapidez. Para ello, se requiere establecer los CSIRT sectoriales críticos (interconectados al ColCERT), con protocolos de actuación estandarizados y plataformas seguras de intercambio de datos. Asimismo, debe consolidarse una red nacional de inteligencia de amenazas cibernéticas, que reúna capacidades del sector defensa, agencias civiles, empresas de ciberseguridad y universidades, bajo estrictos criterios de gobernanza, respeto a la privacidad y principios democráticos. Esta red será clave para anticipar nuevas amenazas, identificar patrones de ataque, y alimentar sistemas de alerta temprana y toma de decisiones basadas en evidencia.

La soberanía tecnológica debería ser otro componente clave de la arquitectura nacional. Como lo señalan Calderaro y Craig (2020), las democracias emergentes enfrentan asimetrías estructurales en acceso a tecnologías avanzadas, plataformas seguras y capacidades de defensa digital. En este contexto Colombia debe priorizar el desarrollo de una estrategia de innovación en ciberseguridad, centrada en el fomento de capacidades nacionales en criptografía, detección de intrusos mediante IA, seguridad de redes 5G, protección de sistemas SCADA y soluciones específicas para infraestructuras críticas. Para ello se propone crear un Fondo Nacional de Innovación en Ciberseguridad y Ciberdefensa, con recursos públicos y privados, destinado a financiar proyectos de investigación aplicada, pruebas de concepto, *startups* tecnológicas y asociaciones universidad-empresa, que permitan construir soluciones adaptadas al contexto nacional. Ese fondo debe estar acompañado por incentivos fiscales a las empresas que desarrollen o implementen tecnologías de protección digital de alta criticidad.

Finalmente, la arquitectura nacional debe vincularse de manera activa a los mecanismos regionales e internacionales de cooperación en ciberseguridad. Colombia debe fortalecer su participación en iniciativas como el Foro Global sobre Respuesta a Incidentes y Seguridad (en inglés, FIRST, por las iniciales de Forum of Incident Response and Security Teams), así como la exploración de acuerdos bilaterales en ciberdefensa con socios estratégicos, especialmente en el hemisferio occidental. La dimensión transnacional de las amenazas cibernéticas (como los ciberataques de *ransomware* de origen externo o las campañas de desinformación patrocinadas por Estados) exige respuestas coordinadas, interoperables y basadas en normas comunes. Colombia puede desempeñar un papel propositivo como líder regional en ciberseguridad en América Latina compartiendo buenas prácticas, promoviendo marcos regulatorios convergentes y facilitando redes de respuesta ante crisis.

Disuasión, resiliencia y persistencia ofensiva en el contexto colombiano

El ataque a la IC de un Estado no es una práctica novedosa: por el contrario, ha sido una constante histórica en el arte de la guerra. En los conflictos más relevantes del siglo XX las fuerzas militares han buscado sistemáticamente degradar las capacidades estructurales del adversario para sostener el esfuerzo bélico a largo plazo. Un ejemplo paradigmático es la Segunda Guerra Mundial, donde el poder aéreo aliado se empleó con un enfoque estratégico orientado a inutilizar el aparato industrial y económico del Tercer Reich. Como señalan Álvarez et al. (2017), la doctrina estadounidense de bombardeo aéreo se centraba en la destrucción selectiva de las IC alemanas (como plantas eléctricas, fábricas de armamento, centros logísticos y vías férreas), con el objetivo de paralizar la producción y socavar la moral y resistencia del adversario. Esta campaña, combinada con la acción del poder naval, neutralizó la amenaza submarina alemana y japonesa, y otorgó superioridad decisiva en los frentes marítimo y aéreo. En tierra, el poder aéreo también resultó clave al facilitar el avance de las tropas aliadas.

Hoy, los objetivos estratégicos de la ciberguerra (infligir daño asimétrico, interrumpir funciones vitales, debilitar estructuras de comando y control o afectar la resiliencia económica) son funcionalmente comparables a los del bombardeo estratégico, la guerra submarina o las operaciones especiales. Las vulnerabilidades informáticas se han convertido en nuevos puntos neurálgicos, equiparables a las antiguas vulnerabilidades físicas de las IC. Así, los ataques cibernéticos buscan no

solo sabotear sistemas digitales, sino hacer colapsar la infraestructura nacional interdependiente, evidencia de una continuidad histórica en la lógica de atacar los nodos vitales de un Estado para debilitarlo estructuralmente.

Según Clark y Hakim (2017), las IC de los Estados están cada vez más conectadas al ciberespacio, siguiendo la misma tendencia global de digitalización. Esa integración responde, en primer lugar, a razones de eficiencia y costo, ya que administrar sistemas complejos de manera remota mediante *software* especializado y protocolos de red resulta más rentable y operativo. Sin embargo, esa conectividad expone nuevos vectores de vulnerabilidad, pues muchos de los dispositivos que componen la infraestructura física tienen capacidades informáticas limitadas, y ello dificulta implementar mecanismos robustos en materia de ciberseguridad (como los cortafuegos²⁸ avanzados o la autenticación multifactor). Además, algunas funciones requieren respuestas automáticas e inmediatas, y por eso no siempre es factible que un operador humano intervenga o autorice cada comando en tiempo real.

La situación se agrava por el hecho de que gran parte de las IC no se hallan bajo control estatal directo. En la mayoría de países, incluyendo Colombia, dichas redes están en manos de actores privados, lo que plantea desafíos adicionales en términos de gobernanza, interoperabilidad y soberanía tecnológica. Por ejemplo, los proveedores de servicios de internet suelen arrendar sus líneas de comunicación tanto al Gobierno como a empresas privadas, mientras que las corporaciones satelitales ofrecen servicios de ancho de banda a múltiples Estados de forma simultánea. En el caso colombiano, la carencia de algunas capacidades espaciales autónomas (como satélites propios para comunicaciones) limita significativamente la proyección de una ciberdefensa integral²⁹ (Álvarez et al., 2019).

Históricamente, las IC fueron diseñadas para resistir fallas humanas, e incluso, desastres naturales. Sin embargo, en un entorno de creciente interdependencia digital, dichas infraestructuras se han vuelto más susceptibles a amenazas no convencionales. Aunque un ciberataque por sí solo difícilmente alcanzaría la letalidad de un bombardeo aéreo (sobre todo, en una era de armas nucleares y municiones guiadas con precisión), su potencial disruptivo crece a medida que los Estados dependen

²⁸ Un cortafuegos (*firewall*), es la parte de un sistema informático o una red informática (*hardware* o *software*) diseñada para evitar que los usuarios de internet no autorizados tengan acceso a redes privadas conectadas a internet, especialmente *intranets*. Es decir, se trata de un dispositivo o conjunto de dispositivos que añaden una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente.

²⁹ De acuerdo al Ministerio de Defensa de Colombia, la ciberdefensa es el empleo de capacidades militares ante amenazas o actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales.

más de sistemas interconectados, como la banca electrónica, el control automatizado del tráfico aéreo o el Sistema de Posicionamiento Global (en inglés, GPS, por las iniciales de *Global Positioning System*). En ese contexto un ataque cibernético devastador contra la ICC no solo es técnicamente posible, sino que representa una amenaza significativa a la seguridad nacional, especialmente si se ejecuta de forma coordinada con las operaciones cinéticas tradicionales. La ciberdependencia, en ese sentido, se ha convertido en un nuevo talón de Aquiles estratégico.

En el panorama descrito, los organismos de seguridad del Estado colombiano deben prepararse para enfrentar ataques de DoS y DDoS durante las operaciones críticas, los cuales pueden abarcar desde técnicas tradicionales de *flooding* (inundación de red) hasta acciones más sofisticadas, como modificación de datos, destrucción física de componentes de *hardware* o, incluso, la utilización de interferencia electromagnética. Como advierten Clark y Hakim (2017), el acceso a redes de dispositivos comprometidos (*botnets*)³⁰, disponibles en la *darkweb*, ha democratizado el uso ofensivo del ciberespacio, hasta permitir que actores estatales y no estatales lancen ataques masivos con altos niveles de anonimato y bajo costo. Empero, la proliferación de TIC también ha fortalecido las capacidades defensivas. Actualmente, los sitios estratégicos pueden disponer de infraestructuras redundantes de comunicación (cableadas, inalámbricas y satelitales), que ofrecen niveles de resiliencia y continuidad operativa impensables en décadas anteriores. Esta diversificación tecnológica, bien gestionada, constituye un pilar de la ciberdefensa moderna y la protección de IC en escenarios de alta presión operativa.

La guerra cibernética en Oriente Medio y Europa del Este ha demostrado que los conflictos en la era digital pueden internacionalizarse rápidamente, y así traspasar fronteras y afectar a actores que no participan directamente en el campo de batalla físico. Uno de los primeros indicios de esta dinámica ocurrió cuando el Club Hackerz, de Pakistán, penetró los servidores de la influyente organización proisraelí AIPAC, con sede en Estados Unidos, y publicó correos electrónicos confidenciales, números de tarjetas de crédito e información personal de sus miembros. En el mismo contexto, la empresa AT&T (considerada un proveedor global de servicios críticos) fue blanco de ataques por haber prestado apoyo técnico al Gobierno israelí durante la crisis. Los ciberataques contra IC nacionales no son una amenaza futura, sino una realidad presente y en expansión global (Geers, 2009). En 2006, durante un pico de tensión entre Israel y Hamas, grupos de *hackers* propalestinos

³⁰ Hace referencia a un conjunto de robots informáticos, o *bots*, que se ejecutan de manera autónoma y automática, y al hacerlo permiten controlar de forma remota todos los computadores/servidores infectados.

lograron inutilizar 700 dominios israelíes, incluyendo el Banco Hapoalim y marcas globales como BMW, Subaru y McDonald's en su operación en Israel³¹.

Un año después, en 2007, un supuesto ciberataque precedió a un bombardeo de la Fuerza Aérea Israelí sobre un presunto reactor nuclear en Siria, lo que evidenció el vínculo directo entre ataques cibernéticos y operaciones cinéticas. Ese mismo año Estonia fue víctima de un ataque masivo de DDoS, luego de que el Gobierno trasladó un monumento soviético en Tallin, lo cual desató la ira del Kremlin y de la población rusoparlante local. Durante casi tres semanas el Gobierno estonio, así como sus bancos, medios de comunicación y portales oficiales, fueron desconectados. Dado que más del 98 % de las transacciones bancarias en Estonia se realizan de forma electrónica, los efectos fueron inmediatos y paralizantes. Incluso, se manipuló el sitio web del primer ministro publicando una disculpa falsa por haber movido la estatua. Estos casos demostraron que los ciberataques pueden desencadenar efectos caóticos en el mundo físico, al interrumpir el comercio electrónico, paralizar servicios públicos esenciales y deteriorar la comunicación entre el Estado y sus ciudadanos.

En 2021 el grupo ruso DarkSide ejecutó un ataque de *ransomware* contra Colonial Pipeline, la red de oleoductos más grande de Estados Unidos, responsable del 45 % del combustible en la costa este. La empresa se vio obligada a pagar millones de dólares en rescate y cerrar operaciones por once días, y afectar así el suministro de gasolina en más de 10.000 estaciones de servicio. Otro caso paradigmático fue el ataque del grupo ruso Sandworm contra la red eléctrica ucraniana, en octubre de 2022. Mediante técnicas de *living-off-the-land* a nivel de tecnologías operativas (en inglés, OT, por las iniciales de *Operative Technologies*), lograron activar disyuntores de subestaciones eléctricas y causar apagones que coincidieron con bombardeos rusos. La intrusión en el sistema SCADA había empezado meses antes, y culminó con eventos disruptivos masivos que causaron víctimas civiles y dejaron sin energía a varias regiones. Este caso reflejó la sinergia operativa entre guerra cibernética y fuego convencional, donde los efectos digitales amplifican el daño físico.

En noviembre de 2023 el grupo iraní Cyber Av3ngers comprometió el sistema de control de una planta de agua en Pensilvania, a la que obligó a pasar a operaciones manuales. Si bien no se reportaron daños a la población, el ataque

³¹ En ese momento Israel estaba más conectado a internet que todos sus vecinos combinados, por lo que no había escasez de objetivos. Además, el dominio del país ".il" proporcionó una lista bien definida que los *hackers* propalestinos trabajaron metódicamente.

logró vulnerar un controlador lógico programable (en inglés, PLC, por las iniciales de *Programmable Logic Controller*) conectado a internet, y encargado de regular la presión del agua en una estación de bombeo. El incidente demostró cómo IC tradicionales como el agua potable pueden ser blanco de agresiones digitales silenciosas, pero potencialmente devastadoras. En Europa los sistemas de energía también han sido vulnerables. En 2024 dos *hackers* éticos del Dutch Institute for Vulnerability Disclosure descubrieron seis fallas críticas de tipo *zero-day* en dispositivos Enphase IQ Gateway (críticos para el funcionamiento de paneles solares domésticos), que habrían permitido a actores maliciosos tomar el control de millones de sistemas en más de 150 países. En caso de haberse materializado un ataque, las consecuencias habrían incluido apagones masivos, pérdidas económicas y amenazas a la seguridad nacional. Este caso subraya la fragilidad de las nuevas infraestructuras verdes interconectadas, como la energía solar, frente a amenazas digitales.

En años más recientes, la escala y sofisticación de los ataques se ha multiplicado. Según un informe de KnowBe4 (2024), entre enero de 2023 y enero de 2024 se registraron más de 420 millones de ciberataques contra infraestructuras críticas a nivel global, lo que equivale a trece ataques por segundo. Aunque Estados Unidos fue el principal objetivo, se identificaron intentos de ataque en 163 países, con alta participación de actores vinculados a China, Rusia e Irán. En febrero de 2024 el sistema de pagos de salud más grande de Estados Unidos, operado por Change Healthcare, fue víctima de un ataque de *ransomware* por parte del grupo ruso BlackCat/ALPHV. El sistema colapsó por más de 30 días, lo que afectó 14 mil millones de transacciones anuales y paralizó la emisión de recetas, chequeos médicos, atención de emergencias y tratamientos esenciales. Finalmente, desde el inicio de la guerra en Ucrania el grupo KillNet ha liderado una ofensiva cibernética prolongada mediante DDoS contra aliados occidentales. Sus ataques han afectado hospitales en Estados Unidos y Países Bajos, la red eléctrica de Lituania y más de una docena de aeropuertos estadounidenses. Aunque el DDoS es técnicamente rudimentario, ha sido usado como cortina de humo para ataques más sofisticados, como *malware* destructivo o intrusiones prolongadas. En conjunto, los mencionados ejemplos demuestran que la guerra cibernética no es una hipótesis estratégica, sino una forma actual de confrontación interestatal e híbrida, capaz de infligir daño sistemático a las funciones vitales de un Estado. La IC (en todas sus formas) se ha convertido en el campo de batalla digital por excelencia del siglo XXI.

Colombia no ha sido ajena a la creciente ola global de ciberataques dirigidos contra infraestructuras críticas, tanto en el ámbito público como en el privado. Un

primer antecedente de importancia ocurrió en el primer semestre de 2011, cuando el grupo hacktivista Anonymous logró inhabilitar durante varias horas los sitios web de la Presidencia de la República, el Senado, Gobierno en Línea y varios ministerios, incluyendo los de Defensa, Interior y Justicia (DNP, 2011). Aunque el impacto fue simbólico, el episodio marcó el inicio de una era de mayor exposición digital del Estado colombiano. Casos más recientes han evidenciado la gravedad de la amenaza. El grupo RansomHouse, por ejemplo, vulneró los sistemas de Keralty, matriz de EPS Sanitas y Colsanitas, afectó la prestación de servicios médicos y expuso hasta 3 *terabytes* de información sensible, según los propios atacantes. Empresas Públicas de Medellín (EPM) también fue blanco del grupo BlackCat, que desactivó portales y aplicaciones de sus filiales y robó, presuntamente, 15 *terabytes* de datos, posteriormente filtrados en la web profunda.

Varios actores nacionales (como Audifarma, Viva Air, Universidad Javeriana, Caracol Televisión, Corferias y Famisanar) han sufrido ataques de *ransomware*, ejecutados por grupos internacionales como Lockbit, Hive, Qilin, ViceSociety, KelvinSecurity, entre otros. A nivel institucional, el Invima y la Fiscalía General de la Nación también han sido objeto de secuestros masivos de información, con filtraciones que superan los 5 *terabytes* de contenido clasificado. La situación más crítica se vivió en 2023 y 2025, cuando grupos criminales transnacionales y disidencias armadas lograron acceder a documentos de inteligencia reservados de las Fuerzas Militares, incluyendo ubicaciones de unidades, despliegues tácticos, inventarios de armamento, y registros sobre aeronaves, incluso no tripuladas, asignadas al Comando Aéreo de Combate N.º 2. Según fuentes de inteligencia, los ataques fueron atribuidos a actores ubicados en Venezuela y Rusia, lo que evidencia el carácter híbrido, regionalizado y geopolítico de la amenaza.

Estos acontecimientos exponen una falla estructural en la arquitectura de ciberseguridad nacional. La creciente adopción de Sistemas Ciberfísicos (SCF) y redes distribuidas ha ampliado la superficie de ataque. Si bien dichos sistemas permiten una mayor eficiencia operativa, como ya se ha señalado, igualmente generan nuevos vectores de vulnerabilidad, debido a su dependencia de infraestructuras digitales interconectadas. Como advierten Gritzalis et al. (2019), los SCF se ven expuestos a fallos en la red de comunicaciones, especialmente cuando operan sobre internet. Por eso, preservar la conectividad segura es hoy un imperativo estratégico, particularmente en sectores como salud, energía, defensa y transporte. Además, los atacantes cibernéticos están empleando cada vez más técnicas de análisis de topologías de red para identificar nodos críticos que, una vez logren comprometer, maximicen el daño con un mínimo de recursos. De esa forma, la

seguridad depende no solo de la protección perimetral o de las prácticas internas, sino de una visión sistémica del riesgo cibernético, basada en la comprensión estructural de las redes nacionales.

En el escenario descrito la resiliencia por sí sola no basta. Colombia necesita articular una estrategia de disuasión cibernética creíble, que combine tres pilares:

1. Resiliencia activa, que busca no solo resistir el ataque, sino garantizar la continuidad operacional y recuperación rápida, mediante redundancia, segmentación y respuesta automatizada.
2. Persistencia ofensiva, entendida como la capacidad de las Fuerzas Militares, a través del CCOC, para identificar APT, anticiparse a campañas hostiles y degradar sus capacidades antes de que se materialicen en el entorno nacional. Esto requiere integrar inteligencia cibernética, capacidades ofensivas limitadas y doctrinas de ciberoperaciones con reglas claras de atribución, proporcionalidad y legitimidad.
3. Disuasión adaptativa, basada no solo en la amenaza de represalias, sino en el fortalecimiento visible de capacidades defensivas, cooperación internacional, gestión de crisis y transparencia estratégica. Una postura de disuasión en el ciberespacio debe persuadir a los adversarios de que los beneficios de atacar a Colombia no superan los costos.

Finalmente, para que dicha estrategia resulte realmente disuasiva, Colombia debe avanzar en el desarrollo y legitimación de capacidades ofensivas cibernéticas, orientadas a neutralizar amenazas persistentes avanzadas, interrumpir campañas hostiles antes de su ejecución y generar efectos estratégicos sobre redes o activos adversarios. La simple existencia de capacidades defensivas o resilientes no basta para disuadir a actores estatales o no estatales que operen con alto nivel de anonimato, motivación política o incentivos criminales. En el entorno digital la credibilidad de la disuasión exige la posibilidad real de infligir costos al agresor, incluso en tiempo real, mediante operaciones activas de degradación, denegación o manipulación de sus capacidades. Esta aproximación no implica militarizar el ciberespacio, sino integrarlo como un dominio estratégico dentro del marco legal nacional e internacional, donde el uso proporcional, legítimo y soberano de la fuerza cibernética contribuya a salvaguardar la estabilidad del Estado, proteger a la población y prevenir conflictos mayores. En consecuencia, una postura cibernética nacional creíble requiere no solo resiliencia y vigilancia, sino también voluntad y capacidad de actuar ofensivamente cuando el interés superior del país lo exija.

Conclusiones

El ciberespacio ha transformado la vida contemporánea reconfigurando no solo las dinámicas sociales y económicas, sino también la naturaleza y la conducta de la guerra. En este nuevo entorno, las amenazas a la IC ya no se limitan a los tiempos de conflicto armado tradicional, sino que también se presentan en contextos de paz y provienen de actores no estatales que pueden operar con total anonimato. En ese sentido, los acontecimientos recientes no dejan duda: la pregunta ya no es si los piratas informáticos lograrán vulnerar los sistemas críticos, sino cuándo lo harán y bajo qué circunstancias. La afectación o destrucción de una ICC colombiana (especialmente, las que sostienen los servicios esenciales para la población) puede tener graves consecuencias para la estabilidad del Estado, y comprometer incluso su gobernabilidad, en cuestión de minutos. Frente a dicho panorama se hace perentorio formular una Estrategia Nacional para la Protección de la ICC, que culmine un proceso ya realizado de catalogación con base en la gestión de riesgos de seguridad digital.

Para entender la magnitud de los riesgos y vulnerabilidades, es clave considerar las cuatro capas del ciberespacio. La capa física incluye elementos como cables de fibra óptica, satélites, torres de telecomunicaciones, computadores y servidores. Especialmente críticos son los cables submarinos que transportan datos a través del mundo y convergen en estaciones de aterrizaje, puntos vulnerables por su concentración y difícil reparación. La mayoría de estos cables submarinos carece de protección física, y existen muy pocas embarcaciones especializadas para repararlos, lo cual representa una debilidad estratégica para países como Colombia. Además, los sistemas de gestión de dichos cables de fibra óptica utilizan software basado en sistemas SCADA y operativos como Windows, los cuales presentan vulnerabilidades bien conocidas (Brenner, 2010).

La capa lógica del ciberespacio constituye el sistema nervioso que enruta los paquetes de datos a través de protocolos como el DNS o el HTTP. Si bien se han implementado mecanismos de resiliencia (como servidores redundantes), la amenaza de manipulación de longitudes de onda y de sistemas operativos comprometidos sigue vigente, como lo demostró el ataque a los trece servidores raíz de internet en 2002 (Borcuch, 2012). En tercer lugar, la capa de información, que comprende contenidos digitales como texto, imágenes o datos personales, y la capa de usuario, que se refiere a los actores que interactúan en línea, también pueden ser blanco de ataques. Empero, es más difícil lograr efectos estratégicos a gran escala en esos niveles, a menos que se trate de campañas de desinformación, propaganda o guerra psicológica.

El ciberespacio, en consecuencia, puede ser atacado en todas sus capas por una amplia variedad de actores (o “ciberagresores”), clasificados en cinco grandes categorías (Rattray, 2001): 1) los ciberterroristas, vinculados a actores estatales o no estatales, que utilizan el ciberespacio como campo de batalla para llevar a cabo actos de ciberguerra; 2) los ciberespías, dedicados a la infiltración de redes y al robo de información sensible con fines estratégicos, ya sean políticos, económicos o militares; 3) los cibercriminales, cuya motivación principal es el lucro, mediante ataques dirigidos a extorsionar, defraudar o sustraer activos digitales; 4) los cibersoldados, agentes estatales o paraestatales que desarrollan y ejecutan operaciones ofensivas en apoyo de los intereses geopolíticos de sus respectivos Estados, y 5) los ciberhacktivistas, que actúan movidos por motivaciones ideológicas, políticas o éticas recurriendo a la desfiguración de sitios web, la filtración de datos o el sabotaje digital como formas de protesta o disidencia.

Además, Arquilla y Ronfeldt (2001) identifican tres modalidades principales de ataques en el ciberespacio. En primer lugar, se encuentran los ataques mecánicos o cinéticos, como el bombardeo de centros de comando y control, o la destrucción deliberada de cables submarinos. Aunque poco frecuentes, dichos ataques son totalmente viables, sobre todo en escenarios de guerra interestatal. En segundo lugar, se ubican los ataques dentro del espectro electromagnético, que incluyen las explosiones electromagnéticas (PEM) o la interferencia intencional de frecuencias, capaces de inutilizar equipos electrónicos sin necesidad de contacto físico. En tercer lugar, están los ataques digitales, los más comunes, que consisten en la intrusión a sistemas informáticos y redes, con el objetivo de robar, alterar, interrumpir o destruir datos e IC. Cada una de estas formas de agresión puede dirigirse a distintas capas del ciberespacio: los ataques físicos apuntan principalmente a la infraestructura física. Los ataques electromagnéticos se sitúan en una zona intermedia entre la capa física y la lógica, al incidir sobre las longitudes de onda por las cuales se transmiten los datos. Mientras, los ataques digitales tienden a comprometer las capas lógica e informativa afectando el funcionamiento de protocolos, *software*, servidores o sistemas operativos.

A pesar de múltiples advertencias que durante años se han formulado respecto a la vulnerabilidad de sectores críticos, como los de energía, telecomunicaciones, banca y finanzas, transporte, alimentación, agua potable, servicios de emergencia, sistemas espaciales e infraestructuras gubernamentales, en Colombia persiste una brecha significativa en la reducción de riesgos asociados, sobre todo frente a la amenaza de PEM. La ausencia de medidas efectivas para mitigar los efectos de una posible agresión PEM plantea un serio desafío para la resiliencia nacional.

En este contexto, garantizar la operatividad plena del ciberespacio exige proteger tanto el espectro electromagnético como la infraestructura física y la capa lógica, ya que estos tres elementos constituyen el sistema circulatorio y nervioso de la sociedad digital contemporánea. La interrupción de cualquiera de estas capas (ya sea mediante sabotaje físico, interferencia electromagnética o intrusión lógica), podría desarticular redes enteras y generar efectos dominó a gran escala sobre el conjunto del sistema nacional.

Si bien Colombia ha hecho avances importantes (como el catálogo nacional de ICC y la "Estrategia Nacional de Seguridad Digital 2025-2027"), persisten desafíos estructurales en materia de coordinación, formación de talento humano, inversión en tecnologías de detección y respuesta, y actualización doctrinal. A ello se suma la necesidad de proteger los sistemas que operan sobre el espectro electromagnético, pues un ataque dirigido a estas longitudes de onda físicas (aunque invisibles) podría alterar o interrumpir gravemente el tráfico de datos y las capacidades críticas del Estado.

Por otra parte, mientras los países más desarrollados tecnológicamente gozan de ventajas competitivas en el ciberespacio, también enfrentan una mayor superficie de ataque. Internet ofrece a actores menos convencionales un medio asimétrico para desafiar a potencias militares superiores. Las victorias tácticas digitales, aunque limitadas en duración, pueden tener repercusiones significativas si logran paralizar IC como el suministro eléctrico, el transporte o los sistemas financieros. Frente a ese contexto Colombia debe asumir la defensa del ciberespacio como un imperativo estratégico de seguridad nacional. Para ello se requieren acciones concretas y sostenidas en varios frentes:

1. Fortalecer las capacidades nacionales de disuasión cibernética con base en una combinación de resiliencia, defensa activa y capacidad ofensiva creíble. La disuasión se logra no solo mostrando robustez en la defensa, sino también al demostrar la capacidad para responder proporcionalmente contra actores estatales y no estatales que atenten contra la seguridad digital del país.
2. Construir una arquitectura institucional especializada, mediante la creación de una Agencia Nacional de Ciberseguridad, con independencia del ciclo político, autonomía técnica y financiera, y con capacidad para coordinar transversalmente los sectores público, privado y académico en materia de prevención, respuesta y resiliencia.
3. Invertir proporcionalmente al nivel de dependencia digital del país. Esto implica financiar de forma sostenible los programas de ciberseguridad,

formar personal calificado en todo el ecosistema (desde ingenieros hasta estrategas) y fortalecer la cultura de seguridad digital desde la educación básica hasta las Fuerzas Militares.

4. Proteger las cuatro capas del ciberespacio y el espectro electromagnético con estrategias y tecnologías adaptadas a los nuevos desafíos, incluyendo IA, detección temprana, segmentación lógica, y segmentación geográfica de la IC.
5. Promover una visión integral y multinivel de la ciberseguridad que no se limite a lo técnico, sino que incorpore consideraciones geopolíticas, éticas, jurídicas y sociales, lo que incluye la participación del Estado en los foros internacionales de gobernanza del ciberespacio y lograr alianzas estratégicas para enfrentar una amenaza que, por definición, no conoce fronteras.

En conclusión, diseñar una robusta arquitectura nacional de ciberseguridad para Colombia exige una combinación de doctrina, regulación y estrategia que considere el riesgo sistémico de las infraestructuras interdependientes y el carácter transnacional de los ataques ciberfísicos, así como la dimensión geopolítica de la competencia digital. La defensa efectiva del ciberespacio no puede lograrse mediante soluciones fragmentadas o sectoriales: requiere una visión de Estado, una institucionalidad robusta, una cultura de seguridad digital y una inversión sostenida a la altura del desafío.

Referencias

- Álvarez, C. y Zambrano J. (2017). Globalización Desviada: Plataforma de Convergencia Criminal. En Álvarez, C. (Ed.), *Escenarios y Desafíos de la Seguridad Multidimensional en Colombia* (pp. 249-306). Sello Editorial ESDEG.
- Álvarez, C.; Rosanía, N.; Sánchez, D. y Jimenez, G. (2017a). Seguridad y Defensa: Conceptos en Constante Transformación. En Álvarez, C. (Ed.), *Escenarios y Desafíos de la Seguridad Multidimensional en Colombia* (pp. 29-84). Sello Editorial ESDEG.
- Álvarez, C.; Santafé, G. y Urbano, O. (2017b). *Metamorphosis Bellum: ¿Mutando a Guerras de Quinta Generación?*. En Álvarez, C. (Ed.), *Escenarios y Desafíos de la Seguridad Multidimensional en Colombia* (pp. 145-248). Sello Editorial ESDEG.
- Álvarez, C.; Corredor, C.; Quiroga, R. y Molano, A. (2019). Programa Espacial Colombiano, en Álvarez, C. y Corredor, C. (eds), *El Espacio Exterior: Una Oportunidad Infinita para Colombia, Volumen 2, El Cielo no es el Límite: El Futuro Estelar de Colombia* (pp. 267-294). Sello Editorial ESDEG.
- Arquilla, J. y Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. RAND Corporation.
- Borcuch, A. (2012). The Influence of the Internet on Globalization Process. *Journal of Economics and Business Research*, 18(1), 118-129.
- Brantly, A. y Brantly, N. (2024) The bitskrieg that was and wasn't: the military and intelligence implications of cyber operations during Russia's war on Ukraine. *Intelligence and National Security*, 39(3), 475-495.
- Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.
- Bronk, C. y Conklin, W. (2022). Who's in charge and how does it work? US cybersecurity of critical infrastructure. *Journal of Cyber Policy*, 7(2), 155-174.
- Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.
- Cabrera, J. (2024). Normatividad para la protección cibernética de la infraestructura crítica en Colombia. *Revista Ciberespacio, Tecnología e Innovación*, 3(5), 7-32.
- Calderaro, A. y Craig, A. (2020) Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 41(6), 917-938.
- Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43-62.
- Castells, M. (2009). *Communication Power*. Oxford University Press.
- Chenou, J. (2021) The contested meanings of cybersecurity: evidence from post-conflict Colombia. *Conflict, Security y Development*, 21(1), 1-19.
- Clark, R. y Hakim, S. (2017). *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*. Springer.
- Consejo Nacional de Política Económica y Social - CONPES (2020). *Política Nacional de Confianza y Seguridad Digital. Documento CONPES 3995*. Departamento Nacional de Planeación.

- Crowther, A.; Perera, F. y Fonseca, B. (2022). Cyber and Great Power Competition in the Western Hemisphere. En Farhadi, A.; Sanders, R. y Masys, A. (Eds.), *The Great Power Competition Volume 3: Cyberspace - The Fifth Domain* (pp. 99-132). Springer.
- DNP (2011). *Lineamientos de Política para Ciberseguridad y Ciberdefensa, Documento CONPES 3701*. Departamento Nacional de Planeación.
- DNP (2016). *Política Nacional de Seguridad Digital, Documento CONPES 3854*. Departamento Nacional de Planeación.
- Egloff, F. y Smeets, M. (2023). Publicly Attributing Cyber Attacks: A Framework. *Journal of Strategic Studies*, 46(3), 502-533.
- Gai, K.; Yu, J. y Zhu, L. (2024). *Introduction to Cybersecurity in the Internet of Things*. CRC Press.
- Galeotti, M. (2017). *Hybrid War or Gibrinaya Voyna? Getting Russia's Non-Linear Military Challenge Right*. Mayak Intelligence.
- Geers, K. (2009) The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal: A Global Perspective*, 18(1), 1-7.
- Gentry, J. (2023) Cyber Intelligence: Strategic Warning Is Possible. *International Journal of Intelligence and CounterIntelligence*, 36(3), 729-754.
- Gibson, W. (1984). *Neuromancer*. Ace Books.
- Gobierno de Colombia (2025). *Estrategia Nacional de Seguridad Digital de Colombia 2025-2027*. República de Colombia.
- González, J. y Acevedo, C. (2021). Aproximación al panorama actual de la protección de infraestructuras críticas en Colombia. En Erazo, L; Puche, O. y Hernández, A. (Eds.), *Panorama en seguridad y defensa visto desde las instituciones de educación superior de las fuerzas armadas, Volumen 1* (pp. 11-24). Sello Editorial ESMIC.
- Griffith, M. (2018). A comprehensive security approach: bolstering Finnish cybersecurity capacity. *Journal of Cyber Policy*, 3(3), 407-429.
- Gritzalis, D.; Theocharidou, M. y Stergiopoulos, G. (2019). *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*. Springer Nature Switzerland AG.
- Haber, M. (2022). Great Power Competition: Critical Infrastructure. En Farhadi, A.; Sanders, R. y Masys, A. (Eds.), *The Great Power Competition Volume 3: Cyberspace - The Fifth Domain* (pp. 3-26). Springer.
- Haber, E. y Topor, L. (2023). Sovereignty, Cyberspace, and the Emergence of Internet Bubbles. *Journal of Advanced Military Studies*, 14(1), 144-150.
- Henrie, M. (2013). Cyber Security Risk Management in the SCADA Critical Infrastructure Environment. *Engineering Management Journal*, 25(2), 38-45.
- Huang, H. y Li, T. (2018). A centralised cybersecurity strategy for Taiwan. *Journal of Cyber Policy*, 3(3), 344-362.
- IBM (2024). Cost of a Data Breach Report 2024. Obtenido de: <https://www.ibm.com/reports/data-breach>
- Katagiri, N. (2023). Hackers of Critical Infrastructure: Expectations and Limits of the Principle of Target Distinction. *International Review of Law, Computers & Technology*, 37(3), 274-293.

- KnowBe4 (2024). Cyber Attacks on Infrastructure: The New Geopolitical Weapon. https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf
- Kulkarni, L.; Karyakarte, M.; Agarkar, A.; Patil, M.; Talware, R. y Sule, B. (2025). Cyber warfare in the digital ecosystem mobile networks and attack-defense strategies for critical infrastructure. *Information Security Journal: A Global Perspective*, 34(4), 1-11.
- Lancelot, J. (2020) Cyber-diplomacy: cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*, 4(4), 240-254.
- La República (2025). Colombia fue el cuarto país con más ciberataques en la región, 36.000 millones en 2024. <https://www.larepublica.co/internet-economy/colombia-tuvo-36-000-millones-de-ciberataques-4178202>
- Lewis, T. (2015). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (2nd ed.). Wiley.
- Lonergan, E. y Lonergan, S. (2023). *Escalation Dynamics in Cyberspace*. Oxford University Press.
- McConnell, J. y Grzegorzewski, M. (2022). Cybersecurity and Strategic Deterrence: Changing Adversary's Risk versus Reward Calculations. En Farhadi, A.; Sanders, R. y Masys, A. (Eds.), *The Great Power Competition Volume 3: Cyberspace - The Fifth Domain* (pp. 49-68). Springer.
- Mattern, T.; Felker, J.; Borum, R. y Bamford, G. (2014). Operational Levels of Cyber Intelligence. *International Journal of Intelligence and CounterIntelligence*, 27(4), 702-719.
- Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press.
- MinTIC (2022). Decreto 338 de 2022. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866>
- MinTIC (2024). .CO, el dominio de los colombianos, generó ingresos para la Nación por más de \$500.000 millones. <https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/383360:CO-el-dominio-de-los-colombianos-genero-ingresos-para-la-Nacion-por-mas-de-500-000-millones>
- MinTIC (2025a). Boletín trimestral del sector TIC - Cifras cuarto trimestre de 2024. <https://colombiatic.mintic.gov.co/679/alt-article-400608.html>
- MinTIC (2025b). Ministerio TIC inauguró el Centro de Operaciones de Seguridad Nacional de Colombia (SOC) para blindar la ciberseguridad de las entidades del país. <https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/399740:Ministerio-TIC-inauguro-el-Centro-de-Operaciones-de-Seguridad-Nacional-de-Colombia-SOC-para-blindar-la-ciberseguridad-de-las-entidades-del-pais>
- Monteleone, C. y Rossi, R. (2024). Cybersecurity and Italian critical infrastructures: the return of the state? *Contemporary Italian Politics*, 1-17.
- Morgenthau, H. (1960). *Politics Among Nations: The Struggle for Power and Peace*. Alfred A. Knopf.
- Nguyen, L. y Sparks, J. (2020). Air, Space, and Cyberspace: Reinvigorating Defense of US Critical Infrastructure. *Air & Space Power Journal*, Fall, 44-53.
- Neilsen, R. y Pontbriand, K. (2025). "Hands off the keyboard": NATO's cyber-defense of civilian critical infrastructure. *Defence Studies*, 1-24.
- Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, 41(3), 44-71.

- Pascal, J. y Wieskamp, L. (2019). Cyber Intelligence Networks: A Typology. *The International Journal of Intelligence, Security, and Public Affairs*, 21(1), 4-24.
- Pesch-Cronin, K. y Marion, N. (2024). *Critical Infrastructure Protection, Risk Management, and Resilience*. Routledge.
- Pursiainen, C. y Kytömaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*, 8(1), 85-101.
- Quigley, K.; Bisset, B. y Mills, B. (2017). *Too Critical to Fail: How Canada Manages Threats to Critical Infrastructure*. McGill-Queen's University Press.
- Rattray, G. (2001). *Strategic Warfare in Cyberspace*. MIT Press.
- Rid, T. y Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1-2), 4-37.
- Sin, S. y Washburn, R. (2022). When the Levee Breaks: A Global Trend of Cyber-Physical and Cyber-Operational Attacks Against Critical Infrastructure and Future Implications on the Great Power Competition. En Farhadi, A.; Sanders, R. y Masys, A. (Eds.), *The Great Power Competition Volume 3: Cyberspace - The Fifth Domain* (pp. 133-156). Springer.
- Slayton, R. (2023). (De)Stabilizing Cyber Warriors: The Emergence of US Military Cyber Expertise, 1967-2018. En Chesney, R.; Shires, J. y Smeets, M. (Eds.), *Cyberspace and Instability* (pp. 177-216). Edinburgh University Press.
- Smith, M. (1999). *Communities in Cyberspace*. Routledge.
- Solar, C. (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, 5(3), 392-412.
- Stoddart, E. (2022). *Cyberwarfare: Threats to Critical Infrastructure*. Palgrave Macmillan.
- Sullivant, J. (2007). *Strategies for Protecting National Critical Infrastructure Assets: A Focus on Problem Solving*. John Wiley & Sons.
- Turner, S.; Hanel, R. y Klimek, P. (2018). *Introduction to the Theory of Complex Systems*. Oxford University Press.
- Timmers, P. (2018) The European Union's cybersecurity industrial policy. *Journal of Cyber Policy*, 3(3), 363-384.
- Wilner, A. (2017). Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application, and Limitation. *Comparative Strategy*, 36(4), 309-318.
- Weiss, M. y Jankauskas, V. (2019). Securing cyberspace: How states design governance arrangements. *Governance*, 32(2), 259-275.
- Weiss, M. y Biermann, F. (2023). Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform*, 26(3), 250-267.
- Work, J. (2020) Evaluating Commercial Cyber Intelligence Activity. *International Journal of Intelligence and CounterIntelligence*, 33(2), 278-308.
- Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, L.; Cetin, F. y Basim, H. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62(1), 82-97.