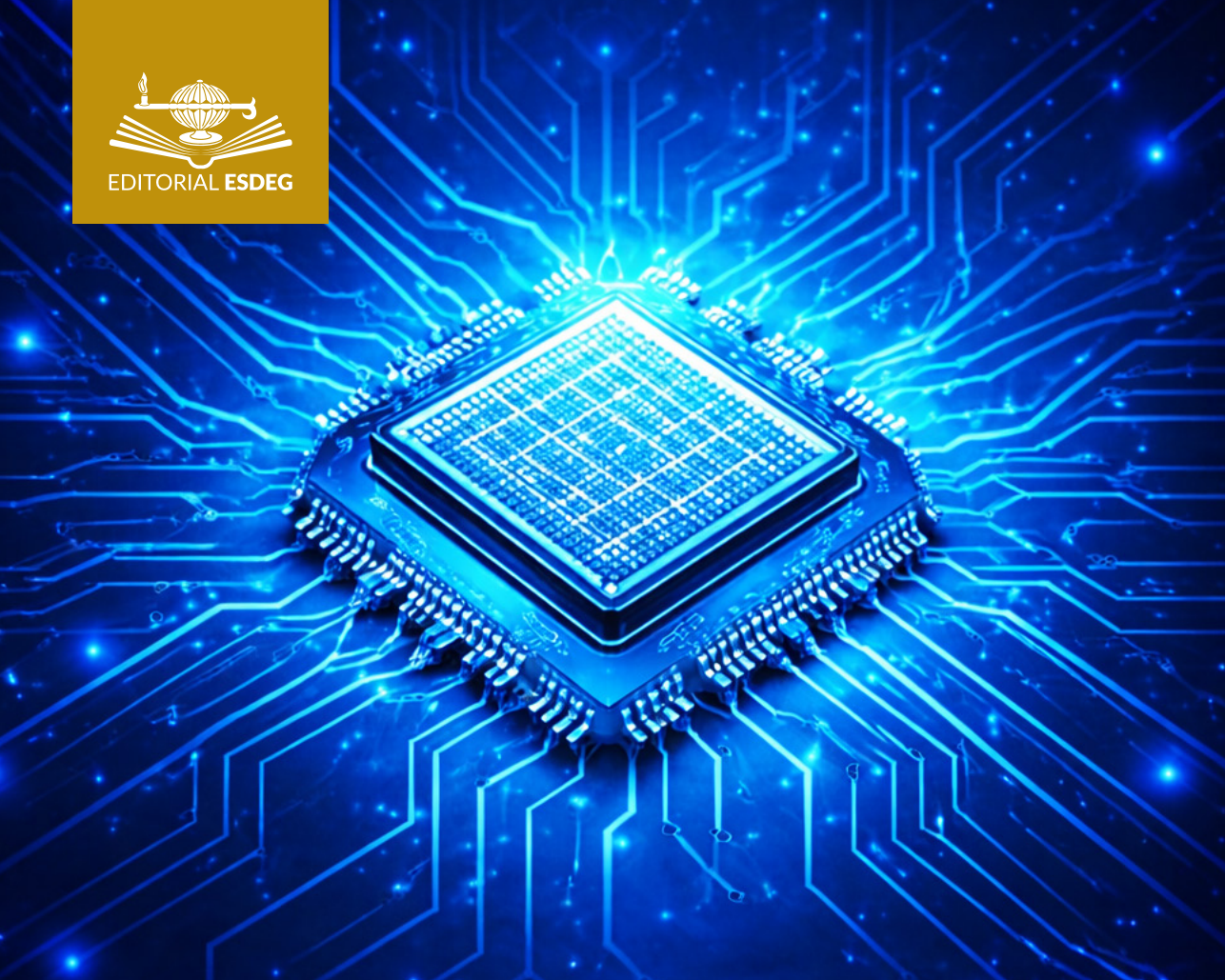




El campo de batalla digital: la defensa nacional en la era algorítmica

Infraestructuras de la guerra digital: computación, ciberguerra y defensa del ciberespacio

Colección
Seguridad y
Defensa

VOLUMEN I

Editor
Carlos Enrique
Álvarez Calderón

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



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

CARLOS ENRIQUE ÁLVAREZ CALDERÓN

(EDITOR)

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., 2026

Catalogación en la publicación – Escuela Superior de Guerra “General Rafael Reyes Prieto” (ESDEG)

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. – Carlos Enrique Álvarez Calderón, editor. Bogotá D.C.: Sello Editorial ESDEG, 2026.

408 páginas: ilustraciones y tablas; 24 cm.

Incluye referencias bibliográficas al final de cada capítulo

ISBN impreso: 978-628-7818-66-8

E- ISBN: 978-628-7818-70-5

(Colección Seguridad y Defensa)

1.Defensa nacional – Colombia 2.Seguridad – Estrategia – Colombia 3.Guerra algorítmica – Colombia 4.Ciberespacio – Colombia i.Sánchez Suárez, Pedro Arnulfo (prólogo) ii.Caro Cancelado, Fabio Leonardo, Mayor General, (prefacio) iii. Álvarez iv.Calderón, Carlos Enrique, v.(autor) Linares Vásquez, Mario, (autor) vi. Niño Zea, Rafael Enrique, (autor) vii.Vega Pulido, Óscar, (autor) viii. Cabuya Padilla, Diego Edison (autor) ix.Ochoa Góez, Hernán Darío (autor) x. Colombia Escuela Superior de Guerra “General Rafael Reyes Prieto”(ESDEG).

SCLC U167.5 .C92
SCDD 355.028

Registro Catalográfico SIBFuP 991410033907231



Archivo descargable en formato MARC en: <https://tinyurl.com/esdeg991410033907231>

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

Primera edición, 2026

Editor:

Carlos Enrique Álvarez Calderón

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

Cubierta:

Lina María Marcela Lozada con base en imágenes de Gemini IA.

2026 Escuela Superior de Guerra

“General Rafael Reyes Prieto”

Vicedirección de Investigación

Sello Editorial ESDEG

Carrera 11 N°. 102-50 Bogotá D.C., Colombia

www.esdeglibros.edu.co

Colección Seguridad y Defensa

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

Libro electrónico publicado a través de la plataforma

Open Monograph Press.

Tiraje de 100 ejemplares

Impreso en Colombia

Libro resultado de investigación de la Escuela Superior de Guerra “General Rafael Reyes Prieto”.

El contenido de este libro corresponde exclusivamente al pensamiento de los autores y es de su absoluta responsabilidad. Las posturas y aseveraciones aquí presentadas son resultado de un ejercicio académico e investigativo que no representa necesariamente la posición oficial ni institucional de las instituciones participantes, la Escuela Superior de Guerra “General Rafael Reyes Prieto”, las Fuerzas Militares de Colombia y el Ministerio de Defensa Nacional.



Los libros publicados por el Sello Editorial ESDEG son de acceso abierto bajo una licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

<https://creativecommons.org/licenses/by-nc-nd/4.0/>



Mayor General
Fabio Leonardo Caro Cancelado
DIRECTOR

Brigadier General
Jaime Andrés Valencia Monsegny
SUBDIRECTOR

Coronel
Aldemar Serrano Cuervo
VICEDIRECTOR DE INVESTIGACIÓN



Coronel
Aldemar Serrano Cuervo
JEFE SELLO EDITORIAL ESDEG

Erika Ramírez Benítez
EDITORA LIBROS ESDEG

Gustavo Patiño
CORRECTOR DE ESTILO

Lina Marcela Manrique Lozada
DIAGRAMADORA

Contenido

Prólogo	IX-XII
Pedro Arnulfo Sánchez Suárez	
Prefacio	XIII-XIV
MG. Fabio Leonardo Caro Cancelado	
Introducción	XV-XVI
BG. Jaime Andrés Valencia Monsegny	
Nota del editor	XVII-XVIII
Capítulo 1	
Computación, cibernética y guerra: una coevolución estratégica	01-78
Carlos Enrique Álvarez Calderón	
Mario Linares Vásquez	
Capítulo 2	
Mapeando el ciberespacio: cartografías de poder y soberanía digital en el siglo XXI	79-176
Carlos Enrique Álvarez Calderón	
Capítulo 3	
La arquitectura ilícita del ciberespacio: cibercrimen y ecosistemas de la <i>dark web</i>	177-236
Carlos Enrique Álvarez Calderón	
Capítulo 4	
El auge de la ciberguerra en guerras de quinta generación: estrategias, herramientas y amenazas	237-316
Carlos Enrique Álvarez Calderón	
Rafael Enrique Niño Zea	

Capítulo 5

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

Carlos Enrique Álvarez Calderón

Óscar Vega Pulido

317-378

Capítulo 6

El intercambio de información de ciberseguridad y ciberdefensa en las Fuerzas Militares de Colombia

Diego Edison Cabuya Padilla

Hernán Darío Ochoa Góez

379-408

Prólogo

Pedro Arnulfo Sánchez Suárez

Ministro de Defensa Nacional de la República de Colombia

En esta nueva era, la defensa de la nación se ha convertido, ante todo, en un ejercicio de anticipación estratégica frente a lo intangible. En un mundo profundamente interconectado, las amenazas estatales y no estatales ya no se despliegan únicamente en los espacios físicos tradicionales, sino que operan a través del ciberespacio y del ecosistema informacional, donde sus efectos —aunque inmateriales— pueden resultar más disruptivos que los daños físicos convencionales. Campañas de desinformación, ataques cibernéticos, operaciones de manipulación cognitiva y estrategias de influencia digital poseen la capacidad de erosionar la soberanía, debilitar la seguridad y fracturar la cohesión nacional sin necesidad de recurrir a la fuerza armada directa.

La defensa contemporánea de una nación, por lo tanto, ya no puede limitarse a la protección de sus fronteras geográficas. Exige, además, infraestructuras tecnológicas resilientes, capacidades avanzadas de ciberseguridad y, sobre todo, una ciudadanía capaz de interpretar de manera crítica, reflexiva y responsable la información que recibe. La seguridad del Estado depende hoy tanto de la solidez de sus instituciones en la era digital, como de la resiliencia cognitiva de su sociedad, entendida como la capacidad colectiva para resistir la manipulación, preservar la deliberación racional y sostener la cohesión frente a intentos sistemáticos de destabilización informacional.

El campo de batalla digital: la defensa nacional en la era algorítmica constituye, en este contexto, un aporte excepcional al pensamiento estratégico colombiano. Su publicación coincide con una etapa de transformación decisiva, en la que el sector Defensa avanza hacia modelos más integrados, interdisciplinarios y preparados para enfrentar amenazas híbridas que combinan acciones en el ciberespacio, manipulación informativa y operaciones de influencia.

El volumen I, *Infraestructuras de la guerra digital: computación, ciberguerra y defensa del ciberespacio*, examina los diferentes sistemas tecnológicos que

sostienen la vida nacional: computación, cibernética, inteligencia artificial, redes de comunicaciones, seguridad de infraestructuras críticas y lucha contra el cibercrimen. Estos temas no son meros dominios técnicos; son pilares de la seguridad nacional. Un ataque cibernético a un sistema energético, financiero o estatal puede afectar tanto la estabilidad del país como una agresión física. La ciberdefensa es, sin duda, un imperativo estratégico del siglo XXI.

El volumen II, *Guerra cognitiva: la mente como campo de batalla del siglo XXI*, se adentra en el dominio cognitivo del conflicto contemporáneo. En dicho volumen se analiza cómo la información, las narrativas y las emociones pueden convertirse en instrumentos de poder capaces de influir en percepciones colectivas, erosionar consensos y condicionar decisiones políticas. En las guerras contemporáneas, la batalla por la interpretación de la realidad puede resultar tan decisiva como la batalla por los territorios.

El volumen III, *Armas de la mente: guerra memética y manipulación informativa en la quinta generación de la guerra*, examina las formas operacionales que adopta esta disputa cognitiva en el entorno digital contemporáneo. Desde la propaganda computacional hasta la circulación viral de narrativas y memes políticos, este volumen explora cómo las plataformas digitales, los algoritmos y las dinámicas de viralidad se han convertido en instrumentos estratégicos dentro de los conflictos del siglo XXI.

Por lo anterior, deseo resaltar de manera especial el papel de la Escuela Superior de Guerra “General Rafael Reyes Prieto” y de su Maestría en Seguridad y Defensa Nacionales, instituciones que históricamente han sido el centro de pensamiento estratégico de Colombia. Esta obra es una muestra del rigor académico, la capacidad analítica y el compromiso que caracterizan a la ESDEG y a su comunidad académica. En un entorno de amenazas emergentes, la formación de altos oficiales, profesionales civiles y servidores públicos exige no solo experiencia operativa, sino también una comprensión profunda de los nuevos dominios del conflicto. La ESDEG y su Maestría cumplen un rol esencial en este propósito: generar conocimiento, fortalecer capacidades y proyectar liderazgo intelectual para el sector Defensa.

El trabajo desarrollado por el editor y autor principal de esta obra, el profesor Carlos Enrique Álvarez Calderón, junto a destacados coautores, contribuye significativamente a la consolidación de una doctrina moderna y multidimensional de seguridad. Este libro es más que un ejercicio académico: es una herramienta para la toma de decisiones, la planeación estratégica y la adaptación institucional que el país requiere frente a un panorama global en constante transformación.

Desde el Ministerio de Defensa Nacional reafirmamos nuestro compromiso con la modernización tecnológica del sector; el fortalecimiento de las capacidades de ciberdefensa; la protección de la soberanía digital y cognitiva, y la consolidación de una fuerza pública preparada para operar eficazmente en todos los dominios: físico, digital e informacional. La defensa del campo de batalla digital no es un desafío futuro; es una misión presente, urgente y colectiva. Invito a los lectores y a las lectoras a asumir esta obra como un referente doctrinal y una guía para comprender la complejidad de los conflictos contemporáneos. En un mundo donde los ataques pueden ser invisibles y las amenazas inmateriales, el conocimiento es la primera línea de defensa.

Prefacio

Mayor General Fabio Caro Cancelado

Director de la Escuela Superior de Guerra "General Rafael Reyes Prieto"

Comprender el carácter de la guerra ha significado siempre comprender la época que la genera. En cada momento de la historia, las sociedades han librado sus conflictos utilizando los recursos, los lenguajes y las tecnologías que definieron su tiempo. La era digital no es la excepción; sí representa, en cambio, como pocas veces antes, una ruptura estructural en la manera como se conciben el poder, la seguridad y la vulnerabilidad. Hoy, el campo de batalla se extiende simultáneamente sobre infraestructuras físicas, sistemas informáticos, redes globales y arquitecturas algorítmicas que conectan y exponen a individuos, organizaciones y Estados.

El campo de batalla digital: la defensa nacional en la era algorítmica invita al lector a adentrarse en esa transformación. A lo largo de sus tres volúmenes, el lector encontrará un recorrido que va desde los fundamentos conceptuales de la computación y la cibernética, hasta las formas contemporáneas de conflicto que se despliegan en el ciberespacio y en el dominio informacional. Esta aproximación no se limita a describir los hitos tecnológicos, sino que busca interpretarlos como procesos que reorganizan la estructura misma del poder militar y civil. En este sentido, la obra expone algo esencial: la revolución digital no solo cambió las herramientas: cambió la manera de pensar el carácter y la conducción de la guerra.

La Escuela Superior de Guerra "General Rafael Reyes Prieto" ha concebido siempre su misión como un puente entre la tradición militar y el pensamiento estratégico contemporáneo. En nuestros programas académicos, especialmente en la Maestría en Seguridad y Defensa Nacionales, insistimos en que la defensa del Estado solo puede comprenderse si se analizan las dinámicas tecnológicas, económicas, sociales y cognitivas que configuran los conflictos actuales. Esta obra es fruto de ese esfuerzo colectivo por comprender, investigar y enseñar las nuevas lógicas de la seguridad en un entorno global profundamente interdependiente.

Las páginas que conforman esta obra invitan a reflexionar sobre un aspecto crucial: el ciberespacio no es únicamente un entorno técnico, sino un ecosistema

de interacción humana, institucional y estratégica. Sus vulnerabilidades afectan la estabilidad política; su protección demanda coordinación interinstitucional; su explotación maliciosa puede escalar desde el delito oportunista hasta operaciones que comprometen la seguridad nacional. Ciberguerra, *dark web*, riesgo sistémico, intercambio de información, algoritmos y sistemas de comando y control son más que conceptos especializados: son expresiones de un nuevo orden estratégico en que la información es simultáneamente recurso, vector y objetivo.

Los autores de esta obra académica (militares, investigadores y profesionales del sector Seguridad) han logrado articular una mirada interdisciplinaria que combina genealogía histórica, análisis doctrinal y reflexión tecnológica. Su trabajo es testimonio de la capacidad intelectual que hoy caracteriza a nuestra ESDEG, y de la importancia de producir conocimiento que no solo describa el entorno, sino que oriente la acción. En un país que enfrenta amenazas híbridas, organizaciones criminales altamente adaptativas y un entorno geopolítico en constante cambio, comprender el ciberespacio y el dominio cognitivo se convierte en una tarea estratégica de primer orden.

Este libro es, por lo tanto, una invitación a pensar la guerra del siglo XXI con profundidad, sin tecnicismos vacíos y sin simplificaciones. A entenderla como un proceso histórico en gestación, donde las decisiones de hoy definirán la seguridad del mañana. A asumirla como un desafío que exige creatividad, doctrina y cooperación. Y, sobre todo, a concebirla como una responsabilidad compartida: entre quienes investigan, quienes diseñan políticas, quienes operan sistemas críticos y quienes defienden al país desde cada uno de sus dominios.

Presento esta obra con la convicción de que se convertirá en un referente para académicos, profesionales civiles y para los hombres y mujeres que integran la comunidad de seguridad y defensa del país, y que contribuirá significativamente a fortalecer la capacidad estratégica del Estado colombiano frente al vasto y desafiante campo de batalla digital.

Introducción

Brigadier General Jaime Andrés Valencia Monsegny

Subdirector Escuela Superior de Guerra "General Rafael Reyes Prieto"

Cada época ha construido sus propias metáforas para describir la guerra. Hubo un tiempo en que la fuerza se midió en caballos y acero; otro, en el que los cañones definieron los límites del poder, y más tarde, otro, cuando la industrialización impuso su ritmo y la guerra se volvió una maquinaria que avanzaba entre fábricas, rieles y líneas de suministro. Hoy, en esta era de conexiones invisibles, la guerra ya no se oye ni se ve con facilidad. Se esconde en pulsos eléctricos, en rutas de datos que cruzan continentes, en servidores que sostienen nuestra vida cotidiana sin que reparemos en ellos. La guerra digital es simultáneamente silenciosa y omnipresente; intangible, pero decisiva.

Este primer volumen, *Infraestructuras de la Guerra Digital: Computación, Ciberguerra y Defensa del Ciberespacio*, invita a recorrer el trasfondo de ese nuevo escenario. Nos recuerda que antes de que existieran las amenazas cibernéticas, existieron las ideas que dieron origen a las máquinas: la lógica simbólica, las primeras tentativas de automatizar el pensamiento, la intuición de que la información podía convertirse en un instrumento de poder. Ni la computación ni la cibernética nacieron de un afán tecnológico aislado, sino de una necesidad humana más profunda: comprender, predecir y dominar la complejidad del mundo. En tal sentido, este libro es también una historia sobre cómo la humanidad aprendió a hablarle al universo en el lenguaje de los algoritmos.

Desde la Escuela Superior de Guerra y su Maestría en Seguridad y Defensa Nacionales, entendemos que estudiar la defensa del Estado implica mucho más que analizar fuerzas y capacidades militares. Implica, sobre todo, comprender la arquitectura que sostiene la vida social: la energía que ilumina nuestras ciudades, los sistemas financieros que mueven la economía, las comunicaciones que enlazan instituciones y ciudadanos y, por supuesto, las redes digitales que conectan cada rincón del país con el resto del mundo. Cuando dichas infraestructuras fallan, o cuando son atacadas, la sociedad entera queda expuesta. Y es, precisamente,

en esa vulnerabilidad donde se manifiesta la verdadera naturaleza de la guerra en el siglo XXI.

El presente volumen nos guía a través de ese territorio, pero no como un mapa frío ni como un inventario de amenazas. Lo hace como un viaje intelectual que conecta la historia con el presente; la teoría, con la práctica, y la tecnología, con la estrategia. Cada capítulo amplía la mirada: desde la evolución conceptual de la computación hasta la cartografía del ciberespacio; desde los corredores ilícitos de la *dark web* hasta el surgimiento de la ciberguerra como instrumento de poder estatal; desde la fragilidad de las infraestructuras críticas hasta la necesidad de construir una cultura de intercambio de información dentro de las Fuerzas Militares.

En estas páginas se revela un mensaje perentorio: la guerra digital no es un conjunto de ataques y defensas dispersas, sino un ecosistema. Un entorno donde actores estatales, grupos criminales, organizaciones civiles y ciudadanos interactúan a velocidades que desafían los marcos tradicionales de seguridad. Un espacio donde los límites se difuminan y donde la frontera entre lo civil y lo militar, lo público y lo privado, lo nacional y lo internacional se vuelve cada vez más difícil de trazar.

Por eso, este volumen no solo explica la guerra digital: invita a pensarla. Nos pide mirar más allá de las pantallas, más allá de los dispositivos, más allá de los titulares. Nos pide ver el tejido invisible que sostiene a la Nación y reconocer que su defensa exige nuevas competencias, nuevas doctrinas y una comprensión más profunda de cómo opera el poder en la era algorítmica. La ESDEG, fiel a su tradición como centro de pensamiento estratégico, presenta este libro como una contribución al desarrollo de la doctrina nacional, pero también como una invitación al diálogo y a la reflexión. Deseamos que quienes lo lean (estudiantes, oficiales, investigadores, responsables de política pública) encuentren en él no solo información, sino claves para interpretar un mundo que cambia a la misma velocidad a la que fluyen los datos.

En la era digital, donde las infraestructuras cibernéticas sostienen la vida económica, política y social de las naciones, comprender el funcionamiento y la vulnerabilidad del ciberespacio se convierte en una condición indispensable para garantizar la seguridad del Estado y la continuidad estratégica de la Nación.

Nota del editor

El Campo de Batalla Digital: La Defensa Nacional en la Era Algorítmica ha sido concebido como una obra estructurada en tres volúmenes complementarios, cuyo propósito es examinar las transformaciones que la revolución digital ha introducido en la naturaleza del conflicto contemporáneo. La complejidad de este fenómeno exige abordarlo desde diferentes niveles de análisis. Por esta razón, la obra se organiza en tres tomos que exploran dimensiones distintas pero interrelacionadas del campo de batalla digital.

El Volumen I, *Infraestructuras de la Guerra Digital: Computación, Ciberguerra y Defensa del Ciberespacio*, examina las bases tecnológicas que sostienen el nuevo entorno estratégico. En él se analizan los fundamentos históricos de la computación y la cibernética, así como la evolución del ciberespacio como dominio operativo y los desafíos que estas infraestructuras plantean para la seguridad nacional.

El Volumen II, *Guerra Cognitiva: La Mente como Campo de Batalla del Siglo XXI*, aborda el dominio cognitivo del conflicto contemporáneo. Este tomo examina cómo la información, las narrativas y los procesos de percepción colectiva se han convertido en espacios centrales de competencia estratégica.

El Volumen III, *Armas de la Mente: Guerra Memética y Manipulación Informativa en la Quinta Generación de la Guerra*, analiza las formas operacionales que adopta esta disputa cognitiva en los ecosistemas informacionales actuales, incluyendo la propaganda computacional, la viralidad memética y las campañas de manipulación informativa amplificadas por plataformas digitales.

En conjunto, estos tres volúmenes buscan ofrecer una aproximación integral a los desafíos estratégicos que plantea el campo de batalla digital, integrando perspectivas tecnológicas, cognitivas e informacionales sobre la evolución del conflicto en el siglo XXI.

Capítulo 1

Computación, cibernética y guerra: una coevolución estratégica*

DOI: <https://doi.org/10.25062/9786287818705.01>

Carlos Enrique Álvarez Calderón

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Mario Linares Vásquez

Universidad de los Andes

Resumen: Este capítulo hace una reconstrucción histórico-tecnológica de la computación y la cibernética, desde sus antecedentes conceptuales en la Antigüedad hasta su consolidación como infraestructuras estratégicas en el ámbito militar contemporáneo. Mediante una genealogía crítica, se exploran hitos fundamentales como la lógica simbólica, las máquinas de cálculo mecánico, la máquina universal de Turing, la teoría matemática de la información y el surgimiento de la cibernética como ciencia de los sistemas de control retroalimentados. Se analiza cómo estas tecnologías emergieron en un contexto de guerra, sobre todo durante la Segunda Guerra Mundial, y cómo fueron instrumentalizadas en doctrinas como C2 y C4ISR. Se demuestra que la computación es no solo una invención exclusivamente técnica, sino una arquitectura de poder, codificada por lógicas militares, epistémicas y políticas. Aunque se presentan estudios comparativos sobre desarrollos en Estados Unidos, la Unión Soviética (URSS), Chile y China, el énfasis recae en la transformación del pensamiento estratégico a partir del paradigma informacional. En última instancia, se argumenta que la cibernética y la computación transformaron no solo la guerra, sino también la forma como las sociedades piensan, gobiernan y se defienden en la era digital.

Palabras clave: cibernética; doctrina militar; informática; teoría de la información.

* 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, y del proyecto de investigación "Computación para la Seguridad y la Defensa", del grupo de investigación TICSw: Tecnologías de Información y Construcción de Software de la Universidad de los Andes, categorizado como A1 por MinCiencias y registrado con código COL0017478. 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

Mario Linares Vásquez

Doctor en Ciencias de la Computación, William and Mary University. Ingeniero de sistemas y computación y magíster en Ingeniería de Sistemas y Computación, Universidad Nacional de Colombia. Investigador Senior MinCiencias y profesor asociado, Universidad de los Andes. Miembro, sala de modernización tecnológica del Consejo Asesor del Sistema Estadístico Nacional. Profesional Oficial de Reserva, Fuerza Aeroespacial Colombiana. Asesor, Jefatura de Educación, Jefatura de Inteligencia y SEMEP, Fuerza Aeroespacial Colombiana.

<https://orcid.org/0000-0003-0161-2888> - Contacto: m.linaresv@uniandes.edu.co

Citación APA: Álvarez Calderón, C. E. & Linares Vásquez, M. (2026). Computación, cibernética y guerra: una coevolución estratégica. 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. 01-78). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818705.01>

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

La historia de la guerra es inseparable del desarrollo tecnológico; desde la domesticación del caballo hasta la energía nuclear, cada transformación técnica ha alterado los equilibrios estratégicos entre Estados y reconfigurado los escenarios del conflicto armado. En esa trayectoria, la computación representa un punto de inflexión sin precedentes, ya que no se trata de tan solo una nueva herramienta de guerra, sino de una revolución ontológica que ha transformado la forma como se concibe, se organiza y se ejecuta el poder militar. Computadores, dispositivos móviles, algoritmos, redes y demás tecnologías de computación y comunicaciones ya no son meros instrumentos, sino infraestructuras epistémicas que condicionan tanto la percepción como la acción en el campo de batalla. Esta observación lleva a formular la pregunta central de este capítulo: ¿cómo ha coevolucionado el desarrollo de la computación y la cibernética con la transformación doctrinal, operativa y estratégica de la guerra en los siglos XX y XXI?

Desde una perspectiva epistemológica, este capítulo se distancia explícitamente de cualquier forma de determinismo tecnológico que conciba a la computación o a la cibernética como fuerzas autónomas que, por sí mismas, transforman la guerra. Por el contrario, el análisis se inscribe en un enfoque constructivista sociotécnico, según el cual las tecnologías militares no determinan de manera lineal la conducta estratégica ni la forma de los conflictos, sino que coevolucionan con doctrinas, culturas organizacionales, estructuras de poder y marcos cognitivos específicos.

En este sentido, tanto la computación como la cibernética son entendidas no como causas independientes del cambio bélico, sino como artefactos sociotécnicos cuya adopción, significado estratégico y efectos operacionales dependen de los procesos históricos de interpretación, institucionalización y aprendizaje militar.

Por ende, la guerra, lejos de ser “transformada” mecánicamente por la tecnología, se reconfigura a través de interacciones complejas entre innovación técnica, pensamiento estratégico y práctica organizacional. Este encuadre permite analizar el vínculo entre computación, cibernética y guerra como una coevolución estratégica, más que como una sucesión de diversas revoluciones tecnológicas deterministas.

Responder a la pregunta del capítulo exige descentrar la mirada del mito fundacional de la “invención” del computador como un acto individual de genialidad, y reubicarla en un proceso histórico más amplio, donde confluyen diversas tradiciones intelectuales (matemáticas, lógicas, mecánicas y filosóficas), así como coyunturas políticas marcadas por la necesidad de procesar información bajo condiciones de extrema incertidumbre, como las guerras mundiales y la Guerra Fría. En este sentido, el surgimiento de la computación no puede disociarse de su genealogía militar. Como bien señalan Swedin y Ferro (2007), los primeros computadores electrónicos no fueron diseñados con fines civiles, sino con el objetivo de realizar cálculos balísticos, descifrar códigos y coordinar operaciones militares a gran escala.

El ciberespacio, como dimensión emergente en esta genealogía, tampoco es un producto neutro o espontáneo de la innovación tecnológica. Su consolidación responde a una larga historia de acumulación de redes, sistemas, protocolos y arquitecturas informacionales, que se desarrollaron inicialmente bajo auspicios militares y científicos. Desde la lógica formal de Boole y la máquina universal de Turing, pasando por el proyecto ENIAC y las redes descentralizadas de ARPANET, hasta los sistemas contemporáneos de vigilancia algorítmica y guerra cibernética, los sistemas basados inteligencia artificial (IA) generativa y la computación cuántica, existe una línea de continuidad donde la computación se vuelve inseparable de las lógicas del control, la predicción y la automatización del conflicto.

La cibernética, entendida como ciencia de los sistemas autorregulados basada en principios de retroalimentación e información, constituyó el lenguaje teórico que permitió articular estos desarrollos en una matriz coherente. Como lo advirtió Norbert Wiener (1948), la guerra moderna ya no consiste únicamente en el despliegue físico de fuerza, sino en la capacidad para anticipar, modular y redirigir el comportamiento del enemigo mediante el control de la información. De ahí que la cibernética se convirtiera en un campo interdisciplinar clave para entender la transición del paradigma bélico tradicional al paradigma informacional.

En las décadas posteriores a la Segunda Guerra Mundial esta convergencia entre computación, comunicaciones, teoría general de sistemas, cibernética y doctrina militar se profundizó. En efecto, la Guerra Fría actuó como un potente acelerador de tecnologías computacionales, no solo por la carrera armamentista entre las

superpotencias, sino también por la necesidad de construir sistemas de comando y control (C2) capaces de operar en entornos de alta complejidad e inmediatez decisional. La evolución hacia C4ISR (que incluye inteligencia, vigilancia y reconocimiento) representa una extensión doctrinal de esta lógica, en la que los datos y los algoritmos se convierten en recursos estratégicos tan importantes como los tanques o los misiles, o incluso, más importantes (Arquilla & Ronfeldt, 1997).

Pero esa historia no es exclusivamente occidental. Como lo demuestra Mullaney (2024), el desarrollo de la computación en la República Popular de China ha seguido un camino distintivo, profundamente vinculado a las estructuras de gobernanza, al lenguaje escrito y a las aspiraciones de control social del Estado. De igual modo, experiencias como Cybersyn, en Chile, o el OGAS soviético revelan intentos alternativos de utilizar arquitecturas cibernéticas para el planeamiento estratégico y el control sistémico a gran escala. Estas experiencias, aunque parcialmente fallidas o abortadas, ilustran el potencial transformador de una concepción de la computación como arte de gobierno.

El presente capítulo propone, por tanto, un recorrido crítico por esa coevolución estratégica. Analiza cómo la historia de la computación se ha visto marcada desde sus orígenes por necesidades militares; cómo la cibernética ha proporcionado las bases epistemológicas para el diseño de sistemas de mando y control en contextos bélicos; cómo distintas potencias (desde Estados Unidos hasta China y Rusia) han adaptado dichos modelos a sus propios contextos político-estratégicos, y finalmente, cómo esa transformación ha dado origen a un nuevo campo de batalla informacional, donde la guerra se libra en el espacio de los datos, las percepciones y las narrativas.

Al comprender esta coevolución entre computación y guerra, es posible no solo historiar críticamente el papel de la tecnología en la organización del conflicto, sino también reflexionar sobre los futuros posibles de la guerra en la era de la IA, la computación cuántica, la vigilancia total y la autonomía letal. ¿Nos dirigimos hacia un mundo donde el algoritmo reemplaza al general, y el dron, al soldado? Y, ¿qué implicaciones éticas, políticas y geoestratégicas se derivan de tal desplazamiento? Estas preguntas orientarán los análisis que se desarrollan a lo largo del capítulo.

Historia de la computación

La emergencia de los computadores (y por ende, del ciberespacio) constituye una de las transformaciones más profundas en la historia de la civilización humana. No

obstante, no puede comprenderse como el resultado aislado de la genialidad de un inventor en específico, como tampoco resulta históricamente riguroso hablar de la “invención” del computador o la “creación” del ciberespacio como si fueran eventos únicos y definidos. Por el contrario, ambos son el producto de una intrincada confluencia de saberes, tecnologías y aspiraciones humanas acumuladas a lo largo de siglos. Esta evolución no lineal responde a múltiples orígenes, que entrelazan avances en álgebra, lógica simbólica, matemáticas discretas, ingeniería, teoría de redes, filosofía y neurociencias, entre otras áreas de conocimiento, así como la necesidad constante de ampliar las capacidades de cálculo, almacenamiento y transmisión de información.

En este sentido, la revolución digital es fruto de innumerables contribuciones colectivas: desde los algoritmos de Al-Juarismi¹ y las tablas de navegación de los astrónomos babilónicos hasta los modelos matemáticos de Boole², las máquinas de Babbage y la computación universal de Alan Turing, al igual que los recientes avances en materia de computación cuántica. Este proceso tomó impulso durante la Revolución Industrial del siglo XIX, con la mecanización y automatización de procesos, y alcanzó plausibilidad teórica gracias a la consolidación de la lógica formal y las matemáticas abstractas. Y ya para el siglo XX, con la Revolución de la Información y la Segunda Guerra Mundial como catalizador, se volvió técnicamente viable; el proyecto ENIAC, la máquina de Turing, y luego ARPANET, marcaron hitos en el tránsito de lo teórico a lo operativo.

La computación moderna y el ciberespacio surgieron, por lo tanto, como una gigantesca síntesis civilizatoria, acelerada por las necesidades de guerra, comercio, ciencia y poder. Según Ning (2022), el ciberespacio no es una entidad que se haya “inventado”, sino una realidad emergente, producto de una acumulación prolongada de tecnologías convergentes y redes humanas interconectadas. Su consolidación se produjo cuando las sociedades industrializadas (impulsadas por la competencia científica, la innovación tecnológica y la carrera armamentista) lograron transformar ideas abstractas en redes funcionales de procesamiento y

¹ La obra de Al-Juarismi no solo sistematizó procedimientos algebraicos, sino que transformó el modo como Occidente concebía el cálculo numérico. La incorporación del sistema de numeración indoarábigo y la formalización de métodos para resolver ecuaciones constituyeron un punto de inflexión en la historia de la abstracción matemática, al desplazar progresivamente los sistemas numéricos romanos hacia estructuras más eficientes y escalables.

² El álgebra de Boole introdujo una formalización binaria de la lógica que permitió traducir proposiciones abstractas en operaciones matemáticamente manipulables. Este paso fue decisivo para la posterior arquitectura de los sistemas digitales, al ofrecer una estructura conceptual capaz de modelar decisiones computacionales mediante operadores lógicos discretos.

comunicación digital a escala planetaria. Hoy se entiende que el ciberespacio es un entorno digital de carácter multidimensional, compuesto por capas tanto físicas (cableado, satélites, servidores) como lógicas (protocolos, algoritmos, agentes de IA, *software*), informacionales (datos, contenidos) y humanas (usuarios, actores estatales y no estatales). Su funcionamiento se basa en principios técnicos heredados de las teorías de la información, cibernética, lógica computacional y arquitectura de redes. Pero también incorpora elementos de poder, control, regulación y resistencia, y se vuelve, por ello, un dominio disputado desde el punto de vista geopolítico, económico y militar.

En suma, ni los computadores ni el ciberespacio son el simple resultado de un momento de invención, sino la manifestación concreta de una aspiración civilizatoria que hunde sus raíces en la historia intelectual de la humanidad. Su consolidación como infraestructura global ha redefinido los límites de la soberanía, la seguridad y el conocimiento, y ha instalado una nueva geografía del poder basada en la información, la conectividad y el control del entorno digital.

Antecedentes antiguos y el deseo de automatizar el cálculo

La invención y posterior difusión de la computación representa uno de los procesos tecnológicos, sociales, económicos y geográficos más trascendentales de la segunda mitad del siglo XX. Los computadores y sus dispositivos asociados han otorgado a los seres humanos un aparente dominio ampliado sobre su entorno, sobre otras personas e, incluso, sobre su propia existencia. Empero, esta aspiración de control también trae consigo una paradoja fundamental: utilizar una herramienta implicaría también confiar en ella y que se alinee con los valores e intenciones de las personas (como en el caso de la IA y la eventual contención de una super IA). Así, el ideal de controlar el mundo mediante máquinas supone, inevitablemente, delegarles una parte sustancial de ese control. A medida que los computadores se han vuelto más potentes, más pequeños y más interconectados, las herramientas tecnológicas de las que depende la humanidad en el siglo XXI han adquirido niveles crecientes de autonomía; hoy la sociedad deposita su seguridad, su privacidad y buena parte de su operatividad cotidiana en dispositivos digitales, los cuales, a cambio, amplían las capacidades físicas, sensoriales y cognitivas del ser humano más allá de sus limitaciones biológicas.

En sus orígenes, las primeras versiones del computador eran esencialmente máquinas diseñadas para eliminar la carga de cálculos aritméticos repetitivos. Uno de los ejemplos más antiguos es la llamada tableta de Salamina, un artefacto

abilónico del año 300 a. C., tallado en mármol, que medía aproximadamente 1,49 m de largo por 0,75 m de ancho y 4,5 cm de grosor, y que contenía una serie de marcas organizadas en cinco grupos distintos (Rossi & Russo, 2017). De hecho, el propio término “cálculo” proviene del latín *calculus*, que significa “guijarro”, en alusión al uso de pequeñas piedras por parte de los romanos para enseñar operaciones aritméticas a sus hijos (suma, resta, multiplicación y división). Así pues, el “cálculo” fue, desde su concepción etimológica, una actividad profundamente material³.

En ese orden de ideas, el ábaco puede llegar a considerarse el primer dispositivo de cómputo de propósito general, creado para sistematizar operaciones matemáticas básicas⁴. Distintas versiones del ábaco han sido halladas alrededor del mundo⁵, lo que da cuenta de su universalidad como herramienta para liberar a la mente humana del esfuerzo repetitivo del cómputo manual (Ifrah, 2001). El término “ábaco” tiene diversos posibles orígenes etimológicos: en griego se usaba ἄβαξ (abax) o ἄβακος (abakos), que significaban “superficie plana” o “tabla”. Otro probable origen era la palabra fenicia de origen hebreo קבא (pronunciada 'ābāq), que en su significado moderno significa “polvo”⁶, mientras que en latín se empleaban los términos *abacus* y *abaci* (en plural). Si bien en las civilizaciones precolombinas se usaban hilos y nudos para contar (como el *quipu* andino⁷), estos dispositivos no pueden considerarse herramientas de cómputo, sino, más adecuadamente, instrumentos de almacenamiento de información.

Como ya se mencionó, el ábaco permitía calcular con facilidad sumas y restas, y con un poco de entrenamiento, multiplicaciones, e incluso, divisiones. En este sentido, el ejemplo más antiguo de un “computador de mano” fue el ábaco romano (Rossi & Russo, 2017). Estaba hecho de una placa de bronce de aproximadamente 115 mm × 90 mm, con nueve ranuras largas y ocho ranuras cortas. El *suan pan* chino era similar al romano y tan antiguo como aquel, y constaba de

³ El concepto de “cálculo” remite a la idea de un sistema formal compuesto por símbolos y reglas de manipulación que permiten transformar expresiones dentro de un dominio determinado. Más que un simple conjunto de operaciones, el cálculo representa la aspiración histórica de convertir el razonamiento en procedimiento. O sea, de traducir problemas complejos en secuencias de pasos susceptibles de ejecución mecánica. Esta lógica de formalización progresiva constituye uno de los pilares intelectuales sobre los que se edificaron tanto la computación como, posteriormente, la automatización estratégica en los sistemas militares contemporáneos.

⁴ Contrario a la creencia popular, un computador no necesariamente tiene que ser una máquina electrónica

⁵ En mandarín se conoce como *Suan Pan*; en japonés, como *Soroban*; en coreano, como *Tschu Pan*; en vietnamita, como *Ban Tien*; en ruso, como *Schoty*, y en turco, como *Coulba*, entre otros ejemplos.

⁶ Aunque en hebreo bíblico era usada para referirse a “granos” o “semillas”. Por consiguiente, las semillas, junto a pequeñas varillas y piedras, denominadas *calculi* en latín, y que se empleaban para calcular en el ábaco, fueron los primeros elementos empleados para realizar el cómputo en toda la historia de la humanidad.

⁷ El “quipus” es derivado del vocablo quechua *khipu*, que significa nudo, ligadura o atadura.

20 palos de bambú (diez en la parte superior y diez en la inferior), con los botones generalmente hechos de marfil; cada uno de los palos superiores e inferiores tenía dos botones. El *soroban* japonés era similar al chino, pero solo tenía un botón en los palos superiores⁸.

Es importante, sin embargo, precisar que algunos dispositivos como el ábaco no pueden ser considerados, en rigor, verdaderas “máquinas” calculadoras. Es decir, aunque instrumentalmente útiles, estos artefactos no ejecutaban operaciones de forma autónoma ni liberaban al operador de la carga cognitiva del cálculo. A lo largo de los siglos surgieron otros diversos mecanismos que ampliaron las capacidades aritméticas humanas, al permitirle no solo la suma y resta, sino también operaciones más complejas, como la multiplicación, la división, e incluso, el cálculo de logaritmos y de raíces cuadradas. Entre estos se destacan el ábaco neperiano (1617); las reglas de cálculo de Oughtred (1622); el multiplicador de Samuel Morland (1666); las máquinas de Perrault (1666), Caze (1720), y Kummer (1847); los aritmógrafos de Troncet (a inicios del siglo XX) y de Clabor (1906); el ingenioso dispositivo de Michel Rous (1869), que combinaba un ábaco chino con la estructura cilíndrica del ábaco neperiano; las varillas aritméticas de Lucas y Genaille; el sumador-multiplicador del general Sebert (1918), y la máquina de multiplicar y dividir de León Bollée (1893), entre otros ejemplos notables (Berlinghoff & Gouvea, 2019).

De nuevo, a pesar de que estos dispositivos facilitaban de modo considerable los procedimientos aritméticos, nunca los mecanizaron en el sentido moderno del término. Es decir, pese a que tenían engranajes, levas y otros elementos mecánicos, seguían requiriendo la intervención manual constante del usuario: desde la introducción de los datos hasta la interpretación final del resultado. No automatizaban el proceso de cálculo, sino que actuaban como extensiones físicas de la acción y del pensamiento humanos; en suma, eran instrumentos intermedios que, si bien ampliaban las capacidades de la mente y de la mano del ser humano, no llegaron a sustituir la lógica, ni el juicio ni el control del operador en la ejecución de las operaciones matemáticas. En ese contexto, puede afirmarse que la auténtica mecanización de la aritmética fue el resultado de una prolongada evolución

⁸ Durante la Edad Media el ábaco fue mucho más que una herramienta práctica de comercio: representó una etapa intermedia en la transición hacia formas cada vez más abstractas de cálculo. Gerberto de Aurillac, posteriormente papa Silvestre II, impulsó su uso en Europa occidental, por lo que contribuyó a la difusión de técnicas aritméticas heredadas del mundo islámico. Un punto de inflexión decisivo llegó con el *Liber Abaci* (1202), de Leonardo de Pisa (Fibonacci), obra que consolidó la introducción del sistema numérico indoarábigo y favoreció el desplazamiento progresivo del cálculo manipulativo hacia el cálculo escrito y simbólico, antecedente remoto de la formalización matemática que siglos después haría posible la computación.

histórica que se remonta a los primeros avances en tecnología mecánica, desarrollados por las civilizaciones más antiguas de la humanidad.

No obstante, la historia formal de la computación encuentra uno de sus pilares fundacionales en el periodo comprendido entre el siglo VI a. C. y el siglo III d. C., cuando floreció una destacada tradición de teóricos e ingenieros en el mundo griego. Los primeros algoritmos⁹ fueron descubiertos y propuestos por los griegos que ya usaban un concepto intuitivo de “computación” (Robič, 2020); por ejemplo, el algoritmo de Euclides, presentado alrededor del año 300 a. C., en su libro *Elementos*, da solución al problema de encontrar el máximo común divisor de dos números enteros. Otro ejemplo clásico es el algoritmo de Platón para generar triplas pitagóricas. El término “computación” se refiere a la ejecución concreta de un algoritmo: es decir, al proceso mediante el cual una secuencia definida de pasos se aplica a un conjunto de datos de entrada para producir una salida. En otras palabras, computar consiste en llevar a cabo (ya sea por un procesador humano o uno artificial) las instrucciones de un algoritmo diseñado para resolver un problema específico. Por ejemplo, al calcular el máximo común divisor de dos números se está ejecutando un algoritmo cuya serie de pasos, al aplicarse correctamente, genera la solución esperada.

Aunque el término “algoritmo” no proviene de la tradición griega, su origen etimológico rinde homenaje al matemático persa Muhammad ibn Musa al-Khwarizmi (conocido generalmente como Al-Juarismi, y latinizado Algorithmi). Considerado por muchos el “abuelo de la computación”, Al-Juarismi (780-850) fue clave en la difusión del sistema de numeración indoarábigo (0-9) en Occidente y en la formulación de métodos precisos para realizar operaciones básicas como la suma, resta, multiplicación y división utilizando notación decimal. Su tratado *Algoritmi de Numero Indorum* es la fuente del término moderno “algoritmo”. Y con el tiempo, el significado del término se fue ampliando, ya que pasó de designar reglas aritméticas específicas a entenderse como un procedimiento sistemático para resolver problemas matemáticos en un número finito de pasos. Hoy, su acepción más general lo define como un conjunto de instrucciones bien definidas y finitas para resolver un problema. Los algoritmos constituyen así el fundamento de la computación, ya que permiten (de forma manual o automatizada, mediante

⁹ El concepto de “algoritmo” remite a un procedimiento finito y formalizable mediante el cual un problema es reducido a una secuencia ordenada de operaciones capaces de transformar datos iniciales en un resultado evaluable. Su importancia histórica radica en que permitió trasladar el razonamiento humano a una estructura susceptible de ejecución mecánica, y así hizo posible que procesos lógicos pudieran ser automatizados y posteriormente integrados en máquinas de cálculo y sistemas computacionales.

computadores), abordar y resolver una amplia variedad de problemas. Es importante destacar que para un mismo problema pueden existir múltiples algoritmos posibles, con diferentes niveles de eficiencia o complejidad.

Durante el periodo entre el siglo VI a. C. y el siglo III d. C. también surgió una escuela de mecánicos que desarrolló componentes fundamentales para la automatización futura, tales como engranajes, poleas, levas y sistemas hidráulicos. Entre los representantes más destacables de esta tradición se encuentran Arquitas de Tarento (428-347 a. C.), Ctesibio de Alejandría (285-222 a. C.), Filón de Bizancio (280-220 a. C.) y Herón de Alejandría (10-70 d. C.), quienes sentaron las bases prácticas de la mecánica aplicada. Sin embargo, dos figuras sobresalen por su impacto duradero en la historia del pensamiento técnico: Aristóteles (384-322 a. C.), quien emprendió uno de los primeros estudios teóricos sistemáticos sobre la mecánica, y Arquímedes de Siracusa (287-212 a. C.), considerado el verdadero fundador de la ciencia mecánica. A Arquímedes se le atribuyen conceptos y principios fundamentales como el centro de gravedad, la ley de la palanca, el principio del plano inclinado y la ley de flotación de los cuerpos (hoy conocida como principio de Arquímedes), así como una serie de ingeniosos dispositivos mecánicos y máquinas de guerra que anticiparon con asombrosa precisión los principios de la ingeniería moderna.

Por su parte, el matemático Papo de Alejandría (290-350 d.C.) continuó la obra de Arquímedes y otros grandes pensadores de la escuela helenística. Sin embargo, su trabajo representa uno de los últimos destellos del legado científico de una civilización en declive. Aunque el esplendor intelectual de la antigua Grecia fue menguando, su herencia no desapareció por completo. Los griegos bizantinos conservaron parte del conocimiento técnico acumulado y, en cierta medida, actuaron como puente entre la escuela alejandrina y el naciente pensamiento mecánico de la Europa medieval. No obstante, fueron los sabios y mecánicos del mundo islámico quienes desempeñaron el papel más decisivo en la preservación, sistematización y transmisión del saber griego clásico, incluidas las contribuciones mecánicas y matemáticas (Ifrah, 2001).

A partir del siglo IX, se consolidó en el mundo árabe una destacada escuela de ingeniería mecánica que no solo recopiló, sino que también enriqueció, el legado grecolatino. Gracias a esta tradición, muchas de las ideas y tecnologías antiguas llegaron hasta los ingenieros del Renacimiento europeo, quienes desarrollaron nuevas aplicaciones e innovaciones en los campos de la mecánica y la precisión técnica, incluso creando autómatas mecánicos con diferentes propósitos. Figuras como Villard de Honnecourt, Giovanni de Dondi, Konrad Keyser, los hermanos

Banū Mūsā, Jean Errard de Bar-le-Duc, Roger Bacon, Alberto Magno, Leonardo da Vinci, Francesco di Giorgio Martini, Giuliano da Sangallo, Giovanni Fontana, Jean Fernel y Oreste Vanocci, entre otros, integraron este acervo heredado con una renovada creatividad, y sentaron las bases del pensamiento ingenieril moderno y del largo camino hacia la automatización del cálculo.

En consecuencia, los orígenes más directos del computador moderno pueden situarse en la Europa del Renacimiento, periodo en el que astrónomos, matemáticos e ingenieros empezaron a enfrentar desafíos de cálculo mucho más complejos como resultado del avance simultáneo en las ciencias matemáticas, la física y la tecnología aplicada. A diferencia de los periodos previos, cuando los cálculos eran relativamente simples y manuales, el auge de la navegación interoceánica, la astronomía y el uso de la artillería militar impuso nuevas exigencias de precisión y velocidad de procesamiento que desbordaban las capacidades humanas sin apoyo mecánico.

Aunque las civilizaciones griega y árabe destacaron notablemente en la invención y perfeccionamiento de dispositivos mecánicos, sus contribuciones al desarrollo de una teoría mecánica sistemática fueron, en comparación, limitadas (Ifrah, 2000). En Europa, hasta bien entrado el siglo XV, la comprensión de los fenómenos físicos seguía anclada en los postulados aristotélicos, cuyas obras dominaban el pensamiento científico medieval. Sin embargo, muchas de las ideas de Aristóteles sobre dinámica y mecánica contenían errores fundamentales y malinterpretaciones que obstaculizaban el avance hacia una comprensión cuantitativa y experimental del movimiento y la fuerza. Por ende, solo con el cuestionamiento de esos principios y la emergencia de nuevas visiones del mundo físico se habilitó el desarrollo de teorías que, posteriormente, servirían de base para la automatización del cálculo y la creación de dispositivos precursores de la computación moderna.

Por consiguiente, no fue sino hasta el siglo XVI cuando comenzaron a producirse los primeros avances significativos en el campo de la mecánica, lo cual marcó el inicio de una nueva era para el pensamiento científico occidental (Boyer, 1949). El matemático italiano Niccolò Tartaglia (1499-1557) dio un impulso clave a los estudios de mecánica y balística, mientras que Gerolamo Cardano (1501-1576) contribuyó con un tratado sobre mecánica e inventó la célebre junta cardánica¹⁰, que luego tendría amplias aplicaciones en la ingeniería moderna. Por su parte, Gianbattista Benedetti (1530-1590) formuló condiciones fundamentales

¹⁰ La junta universal (comúnmente denominada "cardánica") puede interpretarse como un mecanismo de acoplamiento que resuelve la discontinuidad geométrica entre ejes rotacionales no coaxiales. Su arquitectura, basada en una articulación cruzada apoyada en elementos de rodamiento, permite compensar desalineamientos angulares preservando la transmisión del par motor. Este tipo de solución mecánica evidencia cómo la ingeniería desarrolló tempranamente dispositivos capaces de mantener la coherencia cinemática en sistemas dinámicos no lineales.

para el equilibrio de los momentos, y el flamenco Simon Stevin (1548-1620) publicó notables trabajos sobre el equilibrio de los pesos, sobre el equilibrio de los cuerpos en un plano inclinado y sobre la hidrostática, entre otros.

Dichos avances sentaron las bases para el giro decisivo protagonizado por Galileo Galilei (1564-1642), quien estableció las leyes fundamentales de la dinámica y rompió con el paradigma aristotélico que dominaba la física europea (Álvarez et al., 2019). Le siguió Christiaan Huygens (1629-1695), cuyas contribuciones incluyen el descubrimiento de la fuerza centrífuga, la definición del momento de inercia y el desarrollo de la teoría del movimiento de un péndulo, todos ellos elementos centrales en la física clásica (Berlinghoff & Gouvea, 2019).

En 1671 el matemático y astrónomo inglés Robert Hooke (1635-1703) formuló su famosa ley de elasticidad, y fue también el primero en postular que el movimiento de los cuerpos celestes debía comprenderse como un problema mecánico, anticipando el concepto de fuerza de atracción a distancia, que se convertiría eventualmente en la base de la teoría de la gravitación de Isaac Newton. Durante el mismo período matemáticos como John Wallis (1616-1703) y Christopher Wren (1632-1723) desarrollaron estudios sobre las leyes de la hidrostática, mientras que Giovanni Alfonso Borelli (1608-1679) intentó aplicar las leyes dinámicas de Galileo a los movimientos astronómicos.

Todos estos esfuerzos convergieron en la obra monumental de Sir Isaac Newton (1642-1727), quien sistematizó el conocimiento mecánico en sus célebres tres leyes del movimiento¹¹, que constituyeron el fundamento de la física clásica y del pensamiento científico moderno (Christianson, 2005). En su obra fundamental, *Philosophiæ Naturalis Principia Mathematica* (1687), Isaac Newton no solo formuló las leyes clásicas del movimiento, sino que también introdujo (en un lenguaje geométrico), los principios y métodos del cálculo diferencial e integral que él mismo había descubierto y desarrollado de manera independiente.

Estos métodos matemáticos resultaron esenciales para resolver los problemas más complejos de la mecánica y permitieron a Newton elaborar su famosa ley de la gravitación universal¹². Gracias al uso del cálculo, Newton demostró que

¹¹ Estos son (Christianson, 2005): 1) que la velocidad de una partícula de materia permanece constante a menos que una fuerza externa actúe sobre ella; 2) que la tasa de cambio del momento de una partícula sobre la que actúa una fuerza está en la misma dirección e igual a la fuerza; 3) que si una partícula ejerce una fuerza sobre otra, la otra partícula ejerce una fuerza igual y opuesta sobre la primera (acción y reacción son iguales y opuestas).

¹² Con la formulación de la gravitación universal Newton introdujo un principio según el cual la atracción entre cuerpos no depende de cualidades intrínsecas distintas de su masa, sino de una relación matemática precisa: la intensidad de la interacción crece con el producto de las masas involucradas y decrece conforme aumenta la distancia que las separa, siguiendo una ley de tipo inverso-cuadrático. Esta formulación permitió matematizar el movimiento celeste bajo los mismos principios que rigen los fenómenos terrestres.

su sistema mecánico y sus tres leyes del movimiento podían explicar y predecir con precisión el comportamiento de una amplia gama de fenómenos naturales: desde el movimiento de los cuerpos terrestres y las mareas hasta el movimiento de cuerpos extraterrestres como los cometas, lunas, planetas y estrellas. En palabras de Álvarez et al. (2019b), dichas leyes “podían explicar y predecir el movimiento, no solo de la Tierra, sino también de las mareas, cometas, lunas, planetas y estrellas; en otras palabras, del movimiento en todas partes” (p. 122).

El desarrollo de la mecánica teórica avanzó significativamente gracias a las contribuciones de matemáticos suizos como Jacob Bernoulli (1654-1705) y su hermano Johann Bernoulli (1667-1748), quienes ampliaron los métodos analíticos aplicados a la dinámica. Ambos resolvieron problemas fundamentales en la física matemática, como el de la braquistócrona y el estudio del movimiento de partículas bajo diferentes condiciones de fuerza, y sentaron así las bases de la mecánica analítica que dominaría el siglo XVIII. En paralelo, el matemático francés Pierre Varignon (1654-1722) formuló el teorema de los momentos, mientras que Leonard Euler (1707-1783), también suizo, consolidó el enfoque analítico en la mecánica con su obra *Mechanica: sive Motus scientia analytica exposita* (1736), en la cual abordó la teoría del movimiento mediante el simbolismo del cálculo infinitesimal (O'Reilly, 2008).

Con el tema ramificándose en múltiples direcciones, se hizo necesaria una síntesis conceptual. Esta llegó primero con *Traité de dynamique* (1743), de Jean Le Rond d'Alembert (Le Rond d'Alembert, 1967), pero sería Louis de Lagrange (1736-1813) quien lograría unificar los avances en un sistema general de ecuaciones basado en un único principio: el de las velocidades virtuales. Dicho principio, cuyas raíces pueden rastrearse hasta Galileo, fue formulado sistemáticamente en su obra *Mécanique analytique* (1788), donde la mecánica se consolidó como un cuerpo doctrinal rigurosamente formalizado (Ifrah, 2001).

Sobre estas bases, desde el siglo XVII empezaron a desarrollarse máquinas de cómputo mecánicas (también conocidas como computadores mecánicos) capaces de mecanizar algoritmos para resolver algunos problemas de interés. Por ejemplo, en 1642 Blaise Pascal, matemático y filósofo francés, creó la *Pascaline*, una máquina del tamaño de una caja de zapatos equipada con ruedas dentadas interconectadas, capaz de realizar sumas y restas de números de hasta seis cifras (Adamson, 1994). En 1673 Gottfried Wilhelm Leibniz, basándose en las ideas de Pascal, creó la primera versión de su *Staffelwalze*, que fue la primera calculadora mecánica capaz de realizar las cuatro operaciones matemáticas básicas (suma, resta, división y multiplicación).

Ya en el siglo XIX Charles Babbage, inventor británico, diseñó, junto con Ada Augusta Byron (también conocida como Ada Lovelace, hija del poeta Lord Byron), los planos para el *motor analítico*, una compleja máquina de vapor del tamaño de un campo de fútbol que sería capaz de ejecutar algoritmos y, por ende, de resolver varios tipos de problemas computacionales. Sin embargo, las limitaciones tecnológicas de la época impidieron su construcción (Rossi & Russo, 2017). En Estados Unidos, el ingeniero Herman Hollerith desarrolló, hacia finales del siglo XIX, una máquina de tabulación basada en tarjetas perforadas y circuitos eléctricos, destinada a procesar los datos del censo de 1880. Su éxito fue tal que fundó su propia empresa: la International Business Machines (IBM), la cual se convertiría en uno de los pilares más icónicos de la revolución computacional del siglo XX.

De la lógica simbólica a la máquina universal de Turing

La historia de la computación moderna se halla estrechamente ligada al desarrollo de la lógica matemática, a encontrar lenguajes simbólicos para expresar enunciados matemáticos y a la necesidad de formalizar los procesos de razonamiento humano. Esta transición, que va desde la lógica simbólica al concepto de la máquina universal de Turing, representa un momento clave en la evolución del pensamiento científico y tecnológico del siglo XX. La historia empieza con George Boole, quien en 1847 publicó su obra *The Mathematical Analysis of Logic*, donde propuso una lógica simbólica que permitía representar proposiciones mediante variables algebraicas. Esta “álgebra booleana” fue realmente revolucionaria, pues trasladaba el razonamiento lógico al terreno de las operaciones matemáticas. Según O'Regan (2016), el trabajo de Boole estableció “una estructura formal que posteriormente sería utilizada para construir los fundamentos de la lógica computacional y los circuitos digitales” (p. 10).

Durante la segunda mitad del siglo XIX y principios del siglo XX, figuras como Gottlob Frege, Giuseppe Peano, Bertrand Russell, Alfred Whitehead y David Hilbert continuaron el trabajo de Boole intentando crear un sistema formal completo para las matemáticas. El objetivo era establecer una base axiomática coherente que garantizara la verdad matemática mediante reglas de inferencia precisas. Hilbert, en particular, desarrolló un ambicioso programa formalista: pretendía demostrar que todas las verdades matemáticas podían ser derivadas a partir de un conjunto finito de axiomas utilizando reglas lógicas bien definidas (Bernhardt, 2016).

Sin embargo, esta aspiración de completitud fue socavada por el trabajo de Kurt Gödel, quien en 1931 publicó su famoso teorema de incompletitud. Gödel demostró que cualquier sistema formal suficientemente complejo para incluir la aritmética

contiene proposiciones verdaderas que no pueden ser demostradas dentro del sistema. Esta conclusión, profundamente contraintuitiva, puso en duda los fundamentos del programa de Hilbert. Como indican Swedin y Ferro (2022), “Gödel destruyó la esperanza de una máquina lógica perfecta al mostrar que siempre existirían verdades fuera del alcance de cualquier sistema finito de axiomas” (p. 35).

Este descubrimiento dejó una pregunta abierta: ¿es posible definir una noción formal de procedimiento o cálculo que permita determinar automáticamente la veracidad de proposiciones lógicas? Esta es, precisamente, la cuestión que intenta responder Alan Turing en su artículo de 1936 “On Computable Numbers, with an Application to the Entscheidungsproblem”. El *Entscheidungsproblem*, o “problema de decisión”, había sido planteado por Hilbert y Wilhelm Ackermann como parte de su programa lógico, y consistía en determinar si existía un procedimiento mecánico (algoritmo) que pudiera decidir, para cualquier proposición matemática formal, si esta era o no demostrable. Mientras que Alonzo Church abordó el problema mediante el cálculo lambda¹³, Alan Turing optó por un enfoque radicalmente distinto: construir un modelo de máquina ideal que representara el acto mismo de calcular (Bernhardt, 2016). Ambos, Church y Turing, demostraron en 1936 que es imposible escribir un algoritmo para el problema de decisión, y contribuyeron de forma independiente a la formalización de la noción de algoritmo.

Turing razonó que cualquier proceso algorítmico podía ser descompuesto en una secuencia finita de pasos simples que una persona (idealmente) podría realizar con lápiz y papel. A partir de este principio, ideó un dispositivo teórico compuesto por una cinta infinita dividida en celdas, un cabezal lector-escritor y una tabla finita de reglas de transición. Este dispositivo, ahora conocido como la “máquina de Turing”, podía simular cualquier cálculo efectivo. Según Campbell-Kelly et al. (2023), “Turing no sólo respondió al problema de decisión, sino que redefinió lo que significa computar” (p. 77).

Pero lo más revolucionario en el trabajo de Alan Turing no fue simplemente el diseño de una máquina capaz de ejecutar algoritmos, sino el concepto de una máquina universal que pudiera simular cualquier otra máquina de cálculo efectivo. Por ende, ese modelo anticipó la idea del computador de propósito general, cuya

¹³ El “cálculo lambda”, también conocido como λ -cálculo, es no solo una herramienta técnica, sino una propuesta radical sobre la naturaleza misma del cómputo. Al reducir los procesos computacionales a operaciones de abstracción y aplicación funcional, Church demostró que el cálculo podía concebirse como transformación simbólica pura, independiente de soporte físico alguno. Esta idea resultó decisiva para la posterior formalización de la noción de algoritmo y para el desarrollo de lenguajes de programación funcionales, así como para el debate fundacional sobre los límites de lo computable.

funcionalidad no está fijada físicamente, sino que puede modificarse mediante un programa. Como lo explica Bernhardt (2016), "Turing mostró que no se necesita una máquina distinta para cada tarea computacional; es posible construir una sola máquina que simule a todas las demás mediante la codificación adecuada de sus instrucciones" (p. 91). Esta noción de programación almacenada (la idea de que los datos y los programas pudieran residir en la misma memoria) es la base de la arquitectura de von Neumann, que sería implementada décadas más tarde en los primeros computadores digitales.

El paso de una máquina diseñada para realizar una operación específica (como las calculadoras mecánicas de Babbage o los tabuladores de Hollerith) a una máquina universal de propósito general marcó un punto de inflexión en la historia de la tecnología. Como lo resumen Campbell-Kelly et al. (2023), "la universalidad de la máquina de Turing permitió concebir la informática no como una rama de la ingeniería, sino como una ciencia formal autónoma" (p. 73). Al mismo tiempo que estas ideas maduraban, comenzaron a materializarse en dispositivos físicos. Por ejemplo, para 1940, Howard Aiken, un matemático de la Universidad de Harvard, hizo el siguiente gran avance cuando creó un computador electromecánico que funcionaba con números binarios. Dicho dispositivo, denominado Mark I, medía 15 m de largo y 2,5 m de alto, y constaba de 75.000 partes (Ifrah, 2001).

Durante la Segunda Guerra Mundial la Marina de los Estados Unidos (a través de su Oficina de Buques, establecida en 1940) aprovechó los avances tecnológicos en computación para enfrentar desafíos técnicos complejos. Uno de los hitos más relevantes fue el uso del Mark I, también conocido como ASCC (por las iniciales en inglés de *Automatic Sequence Controlled Calculator*), desarrollado por IBM. Este computador electromecánico fue empleado para realizar cálculos esenciales, como la elaboración de tablas balísticas y otras aplicaciones técnicas clave para el diseño de armamento naval, incluidos torpedos y detectores submarinos.

El Mark I no solo revolucionó el procesamiento de datos en el ámbito militar, sino que también se convirtió en una cantera de talento científico y técnico. Una de las figuras más destacadas al respecto fue Grace Hopper, matemática pionera en computación y oficial de la Reserva Naval. Al incorporarse a la Marina durante el conflicto, Hopper fue asignada al equipo que operaba el Mark I en la Universidad de Harvard, y su carrera sería decisiva para el desarrollo de lenguajes de programación modernos. Entre sus contribuciones más importantes se encuentra la creación del primer compilador, una herramienta capaz de traducir instrucciones en lenguaje humano a código máquina, y su participación en el desarrollo del

Common Business-Oriented Language (COBOL), uno de los primeros lenguajes de programación de alto nivel orientados a la gestión empresarial. COBOL se consolidó como un estándar en aplicaciones financieras, bancarias y administrativas, y aún sigue en uso en numerosos sistemas institucionales de todo el mundo.

Paralelamente a los avances estadounidenses, en Europa el ingeniero alemán Konrad Zuse desarrolló, en 1941, el Z3, considerado por muchos el primer computador electromecánico totalmente funcional. Esta máquina era capaz de realizar operaciones aritméticas en punto flotante utilizando lógica binaria, lo que la convertía en un instrumento pionero en términos de procesamiento numérico complejo. El Z3 y el Mark I tenían una tecnología común: ambas funcionaban mediante relés, interruptores electromecánicos que permiten abrir o cerrar circuitos eléctricos automáticamente utilizando una pequeña corriente para controlar otra de mayor intensidad. Estos relés posibilitaron la representación de datos mediante un sistema de codificación binaria (ceros y unos), lo que sentó las bases del lenguaje con el que operan los computadores digitales clásicos (una arquitectura que, salvo por la irrupción reciente de la computación cuántica, sigue siendo la base estructural de los sistemas informáticos modernos). Así, tanto el Mark I en Estados Unidos como el Z3 en Alemania marcaron el inicio de una revolución técnica sin precedentes, en la que la guerra impulsó la transición de los cálculos manuales a la automatización computacional y dio origen a una nueva era en la ciencia, la industria y la estrategia militar.

El avance en la automatización del cálculo no se detuvo ahí. Unos años más tarde, en 1945, un equipo de ingenieros liderado por John Mauchly y J. Presper Eckert en la Universidad de Pensilvania dio un paso decisivo con la construcción del ENIAC¹⁴ (por las iniciales de *Electronic Numerical Integrator and Computer*), considerado el primer computador totalmente electrónico. A diferencia de sus predecesores (como el Mark I y el Z3, que aún dependían de relés electromecánicos), el ENIAC empleaba tubos de vacío para realizar operaciones a una velocidad sin precedentes. No obstante, su escala era monumental, pues ocupaba dos pisos, pesaba alrededor de 30 toneladas y requería más de 18.000 tubos de vacío, lo que generaba un alto consumo energético y frecuentes fallas por recalentamiento (Ifrah, 2001).

A pesar de su potencia, el computador ENIAC representaba una etapa de transición tecnológica. Estas primeras máquinas eran implementaciones parciales de

¹⁴ El ENIAC fue concebido en un principio para hacer cálculos de tablas balísticas utilizados por el Laboratorio de Investigación en Balística del Ejército estadounidense.

las ideas propuestas por Alan Turing en su concepto de máquina universal, pero aún no incorporaban uno de los principios clave: el almacenamiento interno de programas: es decir, la capacidad para que las instrucciones del *software* residieran en la misma memoria que los datos. Esta innovación llegaría poco después, con la llamada arquitectura de John von Neumann, quien, tras incorporarse al equipo del ENIAC en calidad de consultor técnico, retomó las ideas de Turing y definió una estructura lógica y física que aún subyace en la mayoría de los computadores modernos. Al constatar las limitaciones del modelo existente (que requería reconfigurar físicamente el *hardware* para cada nueva tarea), von Neumann propuso un rediseño radical del concepto de computador. En su influyente documento de 1945 titulado *First Draft of a Report on the EDVAC* formalizó lo que hoy se conoce como la arquitectura de programa almacenado: un esquema en el que los datos y las instrucciones residen en una memoria común, lo cual permite modificar el comportamiento de la máquina simplemente cambiando el *software*, sin alterar el *hardware*.

Aunque el informe fue firmado solo por von Neumann, varios contemporáneos, como Stanley Frankel, señalaron que su propuesta se basaba en gran medida en las ideas ya formuladas por Alan Turing, particularmente en su artículo de 1936¹⁵. Como indica Bernhardt (2016), muchos reconocieron que la arquitectura von Neumann no era sino una formalización práctica de los principios de la máquina de Turing, aunque esta influencia no fuera explícitamente reconocida en el informe original. Uno de los aportes más significativos que comparten ambos modelos es el tratamiento de las instrucciones como datos, lo cual habilita una computación verdaderamente universal. Es decir, la posibilidad de crear compiladores, sistemas operativos y programas autorreferenciales¹⁶, así como estructuras lógicas capaces de modificar su propio código.

¹⁵ Aunque el artículo de Turing fue publicado en 1936, su impacto fue inicialmente limitado a los círculos de la lógica matemática. Fue durante la Segunda Guerra Mundial cuando su genio teórico encontró una aplicación práctica decisiva. En Bletchley Park, el centro de inteligencia británico, Turing lideró el desarrollo de sistemas criptográficos para descifrar los mensajes alemanes codificados con la máquina Enigma. Su trabajo resultó esencial para acortar la guerra y sentó las bases para la construcción del Colossus, considerado uno de los primeros computadores electrónicos digitales (Swedin & Ferro, 2022). En palabras de Bernhardt (2016), “la guerra permitió a Turing demostrar que sus ideas no eran solo especulaciones filosóficas, sino herramientas de inmenso poder práctico” (p. 150). A partir de ese momento la distinción entre computación teórica y computación práctica empezó a disolverse.

¹⁶ La noción de programa autorreferencial resulta en especial relevante en entornos de inteligencia artificial y sistemas autónomos, donde el *software* no solo ejecuta instrucciones, sino que evalúa, optimiza o reconfigura su propio comportamiento en función del entorno. En estos casos, la autorreferencia constituye el fundamento lógico de la adaptabilidad algorítmica y de la autonomía operacional en sistemas militares ciber físicos.

La arquitectura propuesta por von Neumann marcó un punto de inflexión en la historia de la computación al establecer un modelo funcionalmente dividido en cinco unidades básicas: unidad de control, unidad aritmético-lógica, memoria, entrada y salida. Esta organización, inspirada en la lógica simbólica y con ciertos paralelos funcionales con el cerebro humano, permitió transformar los computadores de autómatas rígidos en máquinas reprogramables y adaptables (O'Regan, 2016; Swedin & Ferro, 2022). Dicha estructura posibilitó implementar el concepto de programa almacenado (en el cual tanto datos como instrucciones se ubican en una memoria común), una innovación que permitió que los algoritmos fueran codificados mediante lenguajes simbólicos, almacenados y ejecutados repetidamente, y que abrió el camino hacia la programación moderna y el desarrollo de lenguajes de alto nivel.

Además, la terminología técnica se redefinió en este nuevo paradigma. Por ejemplo, el término "memoria" reemplazó al de "almacenamiento", usado desde los tiempos de Babbage, lo que reflejaba una comprensión más dinámica y funcional del procesamiento de información (Campbell-Kelly et al., 2023). Otro cambio sustancial fue el paso del sistema decimal del ENIAC (que requería diez *flip-flops* por dígito) a una codificación binaria mucho más eficiente en el EDVAC, que empleaba un solo *flip-flop* por bit. Esta elección, promovida por von Neumann, no solo simplificó el diseño físico de los computadores, sino que incrementó exponencialmente su capacidad de procesamiento y consolidó los principios lógicos de la máquina de Turing en una arquitectura realizable y escalable.

Cabe destacar que el aporte de von Neumann fue más una síntesis conceptual que una invención aislada. Como señala Davis (2018), la difusión del informe del EDVAC fue tan amplia que puso en el dominio público muchas de las ideas que Eckert y Mauchly (dos de los creadores de la máquina ENIAC) pensaban patentar. Esto generó tensiones entre los ingenieros (que se enfocaban en resolver los desafíos técnicos) y los lógicos (que desarrollaban el diseño teórico), tensiones que perdurarían en la historia de la computación. Lo cierto es que la convergencia entre la máquina universal de Turing y la arquitectura de von Neumann no solo definió la era de los computadores electrónicos, sino que también habilitó el ascenso de la programación moderna, los lenguajes algorítmicos y, eventualmente, la inteligencia artificial. Fue una transición desde una concepción determinista del cálculo a una visión flexible, adaptativa y universal del procesamiento de información, cuyo origen se encuentra en los debates lógicos de la primera mitad del siglo XX.

En resumen, el impacto de la máquina de Turing excede lo meramente técnico. Turing abrió un debate profundo sobre los límites de la mente humana y la

posibilidad de inteligencia artificial. Su célebre test de Turing, propuesto en 1950, ofrecía una forma pragmática de evaluar si una máquina podía considerarse pensante: si era capaz de mantener una conversación indistinguible de la de un humano, entonces merecía el título de "inteligente" (Bernhardt, 2016). Este experimento mental no solo influyó en la naciente disciplina de la inteligencia artificial, sino que también provocó discusiones en epistemología, filosofía de la mente y neurociencia. Como afirman Swedin y Ferro (2022), "el éxito de la computadora como metáfora del cerebro ha transformado incluso la manera en que entendemos el pensamiento humano" (p. 225).

Por ende, las ideas de Turing siguen siendo vitales para las ciencias de la computación. La tesis de Church-Turing, formulada independientemente por ambos autores, sostiene que cualquier función que pueda considerarse computable por medios efectivos puede ser calculada por una máquina de Turing. Este principio no es una ley matemática, sino una hipótesis filosófica que ha resistido la prueba del tiempo. De hecho, la teoría de la complejidad computacional (que clasifica los problemas según los recursos necesarios para resolverlos) se fundamenta en las máquinas de Turing como modelo estándar de computación. Además, el trabajo de Turing llevó al desarrollo de conceptos fundamentales como el problema de la parada (*halting problem*), la indecidibilidad y la incompletitud computacional. Estos conceptos no solo delimitan lo que es posible computar, sino que también permiten comprender qué problemas están fuera del alcance de cualquier sistema automático. En las palabras de Campbell-Kelly et al. (2023), "la máquina de Turing no fue un invento aislado, sino el inicio de una revolución científica que transformó a las matemáticas, la ingeniería, la economía y las ciencias cognitivas" (p. 78).

Entonces, la trayectoria que va desde la lógica simbólica de Boole hasta la máquina universal de Turing revela una profunda transformación del conocimiento moderno. Este tránsito no solo redefinió el concepto de computación, sino que sentó las bases teóricas, filosóficas y prácticas del mundo digital en que vivimos hoy. Al formular una teoría formal del cálculo mecánico, Turing no solo resolvió (negativamente) un problema lógico planteado por Hilbert, sino que inauguró una nueva era en la historia de la humanidad. Su legado sigue vivo en cada computador, cada algoritmo y cada línea de código que define el presente de la humanidad.

Computación industrial y microprocesadores

Tras el establecimiento conceptual de la máquina de Turing y su realización en la arquitectura de von Neumann, el mundo fue testigo de una rápida transformación

de la computación, desde una herramienta científica y militar hacia una tecnología industrial, comercial y finalmente personal. Este tránsito fue acompañado por una revolución tecnológica en miniaturización, eficiencia energética y estandarización, cuya cúspide simbólica fue la invención del microprocesador.

Durante las décadas de 1950 y 1960 la computación electrónica se consolidó como infraestructura clave en gobiernos, industrias manufactureras, sistemas bancarios, laboratorios nucleares y agencias militares. IBM emergió como la corporación dominante del sector gracias a su visión estratégica y a su apuesta por el desarrollo de una arquitectura modular y escalable. Con el System/360, introducido en 1964, IBM ofreció por primera vez una familia de computadores compatibles entre sí, independientemente del tamaño o propósito (Campbell-Kelly et al., 2023). Esta compatibilidad permitió a las empresas proteger su inversión en *software*, y sentó, por eso, un precedente fundamental para la evolución del ecosistema informático. La computación, sin embargo, aún estaba restringida a entornos altamente especializados, debido a que los *mainframes* requerían salas acondicionadas, personal técnico cualificado y mantenimientos constantes. Como señalan Swedin y Ferro (2007), su adquisición implicaba una decisión estratégica de largo plazo, comparable a la construcción de una planta industrial.

Por ende, la revolución en *hardware* se inició con el reemplazo del relé por el tubo de vacío (1939); luego, por el transistor (1947), y posteriormente, por el circuito integrado (1958). Estos avances, liderados por ingenieros como Jack Kilby y Robert Noyce, permitieron construir dispositivos más pequeños, fiables y energéticamente eficientes (O'Regan, 2016). La miniaturización de componentes no solo aumentó la velocidad y capacidad de procesamiento, sino que redujo radicalmente el tamaño y el coste de los sistemas informáticos. En este nuevo contexto, organizaciones empresariales como *Digital Equipment Corporation* (DEC) lanzaron computadores cada vez más asequibles y compactos, como el PDP-8, de 1965, que marcó el nacimiento del minicomputador. Estos nuevos dispositivos encontraron su nicho en laboratorios universitarios, plantas de manufactura y entornos de automatización industrial. Como afirma Bernhardt (2016), "la minicomputadora abrió una brecha en el monopolio del mainframe al ofrecer potencia de cálculo a organizaciones de tamaño medio" (p. 122).

En este orden de ideas, el minicomputador representó un paso intermedio esencial entre el *mainframe* y el computador personal, y demostró así que la computación podía ser descentralizada y adaptada a tareas específicas. Este nuevo paradigma evidenció que era posible diseñar sistemas computacionales más

accesibles, escalables y personalizados según las necesidades del usuario. Tal evolución tecnológica y conceptual preparó el terreno para un avance aún más radical: la integración de la unidad de procesamiento en un único componente físico. Fue en ese contexto de progresiva miniaturización y modularidad donde surgió el microprocesador¹⁷, que llevaría la computación a una nueva era.

En 1971 Intel presentó el 4004, considerado el primer microprocesador comercial. Fue diseñado originalmente para una calculadora japonesa, pero sus creadores (Federico Faggin, Marcian Hoff y Stan Mazor) pronto comprendieron que el chip podía ser programado para ejecutar cualquier operación lógica. Así nació el concepto de computador en un solo chip, una síntesis perfecta de la idea de Turing materializada en silicio (Campbell-Kelly et al., 2023). La evolución siguió con procesadores más potentes, como el Intel 8008, el 8080, y el Zilog Z80, que empezaron a alimentar una nueva ola de dispositivos programables. Su bajo costo y escalabilidad los convirtieron en el motor de la revolución del *hardware* embebido, que abrió paso a la integración de capacidades computacionales en una variedad de productos: desde electrodomésticos y automóviles hasta maquinaria industrial y juguetes. El microprocesador permitió que los computadores dejaran de ser objetos únicos para convertirse en productos de consumo. Como destaca Davis (2018), "el microprocesador fue para la computación lo que la imprenta fue para la cultura: un catalizador de democratización" (p. 279). Esta capacidad para integrar inteligencia computacional en un formato compacto y económico transformó las posibilidades de diseño y producción de sistemas informáticos, y habilitó así una explosión de creatividad tanto en la industria como entre los entusiastas de la tecnología.

Fue precisamente en ese ecosistema emergente de innovaciones técnicas y acceso ampliado donde comenzaron a surgir los primeros experimentos de informática personal. Uno de los primeros hitos en la historia de la informática personal fue la aparición de la Altair 8800 (1975), considerado el primer computador personal accesible para aficionados y programadores. Aunque carecía de monitor, teclado o almacenamiento masivo, despertó un entusiasmo sin precedentes. Fue

¹⁷ El microprocesador era un circuito integrado muy avanzado, construido dentro de un volumen físico muy pequeño, que poseía una memoria, una instalación de entrada y salida, una instalación de procesamiento de datos y un sistema de programación, que podía aplicarse a la ejecución de ciertos tipos de tareas. Fue este avance el que, a su vez, dio lugar al desarrollo de lo que se conoce como tecnología de integración a gran escala, con la producción en masa de componentes altamente integrados, a partir de 1976. Esta tecnología transformó de manera radical una serie de actividades y, por lo tanto, la vida cotidiana de millones de consumidores; según Ifrah (2001), "ahora es posible incluir cientos de miles de ubicaciones de memoria en un circuito que ocupa un espacio más pequeño que una uña" (p. 303).

en este contexto en el que Bill Gates y Paul Allen desarrollaron un intérprete del lenguaje de programación BASIC para la Altair, lo que marcaría el inicio de Microsoft. Apple Computer, fundada por Steve Jobs y Steve Wozniak, llevó esta innovación un paso más allá con la Apple II (1977), un dispositivo con carcasa plástica, monitor integrado, teclado, y posibilidades de expansión. Como señalan Campbell-Kelly et al. (2023), "el Apple II introdujo el concepto de informática como experiencia personal y no solo como herramienta técnica" (p. 240).

En 1981 IBM ingresó al mercado con su IBM PC, acompañado por el sistema operativo MS-DOS. Con la aparición de diferentes modelos de computadores personales se promovió, entonces, un nuevo entorno de compatibilidad y competencia que, a su vez, aceleró el desarrollo tecnológico, abarató los costos de producción y estimuló la innovación tanto en el diseño de componentes como en las aplicaciones. A partir de entonces, la computación personal dejó de ser un privilegio de expertos o instituciones y empezó a penetrar de manera masiva en múltiples esferas sociales.

Durante las décadas de 1980 y 1990 la velocidad de los microprocesadores aumentó exponencialmente siguiendo la Ley de Moore¹⁸, al tiempo que el costo de fabricación disminuía. Esto permitió la expansión de la computación personal a sectores como la educación, la medicina, la ingeniería, las finanzas y el entretenimiento. Asimismo, la incorporación de interfaces gráficas, ratones, impresoras, módems y conectividad en red amplió aún más el campo de aplicación de los computadores personales, y el advenimiento de internet y la aparición de los navegadores web (Netscape, Internet Explorer) hicieron del computador una ventana al mundo y transformaron radicalmente el acceso a la información y al conocimiento.

¹⁸ La llamada Ley de Moore no solo describió un fenómeno técnico, sino que configuró la base material de la superioridad digital de Occidente a lo largo de la segunda mitad del siglo XX. La aceleración sostenida en la densidad de transistores permitió la expansión de capacidades de cómputo que, a su vez, hizo posible la revolución de internet, la IA temprana y la guerra basada en redes. Su eventual desaceleración marca no solo un límite físico, sino una transición geopolítica hacia nuevas arquitecturas tecnológicas, como la computación cuántica y los chips especializados para IA.

Tabla 1. *Fases históricas de la computación*

Fase	Periodo aproximado	Paradigma dominante	Hitos tecnológicos y científicos clave	Características principales
1. Fase mecánica y prelógica	Antigüedad-siglo XIX	Automatización del cálculo mecánico	Ábaco; regla de cálculo; pascalina; máquina de Babbage	Búsqueda de dispositivos físicos para representar operaciones numéricas
2. Fase lógica y algorítmica	Finales del siglo XIX-década de 1940	Formalización simbólica y computación teórica	Lógica booleana; máquina universal de Turing; teorema de Gödel	Fundamentos teóricos de la computación moderna; separación entre <i>hardware</i> y <i>software</i>
3. Fase electrónica e industrial	Década de 1940-década de 1990	Computación programable centralizada	ENIAC; transistores; circuitos integrados; microprocesador; IBM PC	Computadores electrónicos; nacimiento de la informática personal y corporativa
4. Fase conectiva y algorítmica	Década de 1990-década de 2010	Computación en red e inteligencia algorítmica	Internet; web; teléfonos inteligentes; IA; <i>big data</i> ; <i>cloud computing</i>	Computación distribuida, ubicua; aprendizaje automático; redes globales de datos
5. Fase cuántica y cognitiva (en desarrollo)	Década de 2010 en adelante	Supercomputación e inteligencia autónoma	Qubits; IA generativa; computación neuromórfica; biocomputación	Computación no clásica; dispositivos cognitivos; integración cuerpo-máquina; gobernanza algorítmica

Fuente: elaboración propia.

A partir de 2000 la miniaturización alcanzó nuevos límites con la proliferación de dispositivos móviles, tabletas, relojes inteligentes, asistentes digitales y dispositivos embebidos. El microprocesador pasó de ser el corazón de un computador a ser un órgano ubicuo en la vida cotidiana: desde los automóviles hasta los marcapasos, desde los electrodomésticos inteligentes hasta los sensores agrícolas. Por consiguiente, la evolución que conduce desde la computación industrial hasta la era de los microprocesadores constituye una trayectoria de convergencia entre teoría, tecnología e industria, tal como se sintetiza en la tabla 1.

Se trata de un proceso de desmaterialización progresiva en el que ideas inicialmente abstractas (como los modelos formales de Alan Turing o la arquitectura lógica propuesta por John von Neumann) encontraron su realización práctica en dispositivos cada vez más pequeños, eficientes y poderosos. Esta transición no solo transformó la naturaleza física de la computación, sino que redefinió los

límites de lo posible inaugurando un ecosistema digital capaz de integrar el cálculo, el almacenamiento y la comunicación a escalas antes inimaginables.

Computación contemporánea: inteligencia artificial y ubicuidad digital

El desarrollo histórico de la computación desde la lógica simbólica hasta el microprocesador abrió el camino para una nueva etapa, caracterizada por la interconectividad, la miniaturización extrema y el uso de algoritmos avanzados que permiten a las máquinas no solo procesar la información, sino también aprender de ella. Esta cuarta fase de la historia computacional (tabla 1) se define por la convergencia de tres grandes transformaciones: la computación ubicua, el *big data*, la IA y los avances tecnológicos en *hardware* para computación de alto desempeño. Cada una de estas transformaciones ha evolucionado en paralelo, pero profundamente interconectadas, y han dado lugar a nuevos modelos de arquitectura tecnológica y de interacción entre humanos y máquinas. La transición desde la computación personal hacia entornos distribuidos constituye el primer paso clave en esta nueva configuración.

A inicios del siglo XXI la computación personal dio paso a modelos distribuidos de procesamiento, gracias al crecimiento de internet y de las infraestructuras de centros de datos. El concepto de *cloud computing* (computación en la nube) permitió que los usuarios accedieran a aplicaciones, infraestructura, servicios de cómputo (almacenamiento, procesamiento) y servicios digitales (banca en línea) sin necesidad de dispositivos muy poderosos. Como explica Bernhardt (2016), este cambio representó una descentralización del procesamiento, en la cual “los dispositivos personales ya no necesitan hacer todo el trabajo, sino solo servir como terminales inteligentes” (p. 168). Empresas como Amazon Web Services, Google Cloud Platform y Microsoft Azure transformaron la lógica del procesamiento computacional mediante arquitecturas de servicios escalables y redes de servidores globales. Además, el modelo *as-a-service* cambió radicalmente el acceso a las capacidades computacionales sustituyendo la adquisición de infraestructura por el consumo bajo demanda de potencia, almacenamiento y funciones cognitivas, accesibles mediante interfaces de programación de aplicaciones (en inglés, API, por las iniciales de *Application Programming Interface*), que permiten integrar capacidades avanzadas de terceros en tiempo real. Esta flexibilidad democratizó el acceso a herramientas que antes estaban reservadas a grandes corporaciones.

Al mismo tiempo, la masificación de los teléfonos inteligentes, tabletas, dispositivos *wearable*, sensores interconectados, la mejora en las capacidades de

comunicación vía redes y, en general, la computación embebida a la disposición de todos originó el llamado Internet de las Cosas (en inglés, IoT, por las iniciales de *Internet of the Things*), una red global de objetos físicos que recopila, procesa e intercambia datos. Esto llevó a una expansión del concepto de computador más allá de su forma tradicional, hacia una presencia ubicua e integrada en el entorno físico. Las ciudades inteligentes, la automatización del hogar, los dispositivos vestibles y las plataformas de salud digital son ejemplos del impacto transformador de esta computación ubicua, o *pervasiva*. Empero, esta densificación del mundo digital trajo consigo un fenómeno colateral de gran magnitud: la generación constante y masiva de datos provenientes de millones de fuentes heterogéneas, así como la emergencia de riesgos asociados a su protección, integridad, disponibilidad y control. La capacidad para capturar información en tiempo real desde múltiples dispositivos desencadenó un nuevo desafío tecnológico y epistemológico: cómo gestionar, asegurar y extraer valor de esa avalancha de datos.

La interconexión global y la digitalización de procesos sociales, económicos y científicos generó una avalancha de datos sin precedentes. El fenómeno del *big data* no solo trajo consigo desafíos en términos de almacenamiento y procesamiento, sino que también estimuló el desarrollo de nuevas formas de análisis automatizado. La IA resurgió con fuerza gracias al aprendizaje automático (*machine learning*), en especial mediante el uso de redes neuronales profundas (*deep learning*), que permitieron avances sustanciales en áreas como el reconocimiento de voz, la visión por computador, la traducción automática y la conducción autónoma. Según Cooper y van Leeuwen (2013), “el modelo universal de Turing sirvió de base no solo para computadoras deterministas, sino también para aquellas máquinas capaces de adaptarse mediante experiencia acumulada” (p. 325).

Los algoritmos de aprendizaje profundo, ejecutados en unidades de procesamiento gráfico (en inglés, GPU, por las iniciales de *Graphics Processing Unit*), en unidades tensoriales (en inglés, TPU, por las iniciales de *Tensor Processing Unit*) o en unidades neurales (en inglés, NPU, por las iniciales de *Neural Processing Unit*), marcaron un nuevo paradigma, en el cual la capacidad de procesamiento se dirigía no solo a ejecutar instrucciones, sino a modelar y reconocer patrones complejos a partir de grandes volúmenes de información. Empresas como Google, OpenAI, Meta y Baidu han construido arquitecturas neuronales capaces de superar la precisión humana en tareas como diagnóstico médico, generación de texto y análisis semántico. El despliegue de modelos fundacionales como GPT, BERT o DALL-E ha transformado la manera como los seres humanos interactúan con la información, el conocimiento y los sistemas. De ser simples herramientas funcionales, los

computadores pasaron a ser actores cognitivos dentro de procesos creativos, científicos y sociales. En esta instancia hablamos de la IA Generativa: es decir, la evolución de los modelos de aprendizaje profundo, en modelos fundacionales (modelos grandes de lenguaje como GPT, Gemini, Claude), que son capaces de entender y generar contenido multimodal (texto, imágenes, voz, video), en diferentes idiomas.

Mientras estos modelos avanzados de IA reconfiguran los límites de lo computable dentro del marco clásico, otra línea de desarrollo más radical ha empezado a desafiar las bases mismas de dicho paradigma: la computación cuántica. Esta alternativa busca no solo mejorar el rendimiento, sino redefinir la naturaleza de la computación desde principios físicos completamente distintos a los de la computación clásica. En paralelo, el desarrollo de la computación cuántica propone una ruptura con el paradigma clásico de Alan Turing. A diferencia de los computadores digitales tradicionales, que procesan bits en estados 0 o 1, los computadores cuánticos utilizan *qubits*¹⁹, que pueden hallarse simultáneamente en múltiples estados, gracias al principio de superposición. Esto ofrece un potencial exponencial para resolver ciertos problemas, como la factorización de grandes números, la simulación de moléculas o la optimización de sistemas complejos (O'Regan, 2016).

La computación cuántica no busca reemplazar a la digital clásica, sino expandir sus capacidades en dominios muy específicos, donde los algoritmos convencionales son ineficientes. Empresas como IBM, Google, D-Wave y Honeywell han alcanzado hitos importantes en la estabilización y el control de los *qubits*, así como en la implementación de puertas lógicas cuánticas. La carrera por la supremacía cuántica (la demostración de que un computador cuántico puede resolver un problema inalcanzable para uno clásico) ha generado nuevas dinámicas de competencia geopolítica y científica. A nivel teórico, la computación cuántica plantea nuevas preguntas sobre los límites de la computación clásica, la seguridad de los algoritmos de cifrados actuales y las comunicaciones con tecnologías cuánticas. Si la máquina de Turing representaba una abstracción de la mente humana, el computador cuántico introduce en la informática conceptos tomados de la mecánica cuántica: incertidumbre, entrelazamiento, decoherencia e interferencia.

Mientras estas innovaciones amplían las fronteras del conocimiento y de lo tecnológicamente posible, también exponen nuevas tensiones entre desarrollo

¹⁹ Mientras que el bit clásico opera bajo una ontología determinista binaria, donde cada unidad de información adopta uno de dos valores posibles en cualquier instante (0 o 1), el *qubit* se describe como un vector normalizado en un espacio de estados cuánticos, capaz de existir en superposición coherente hasta el momento de la decoherencia inducida por la medición. Esta diferencia ontológica transforma no solo la capacidad de procesamiento, sino la arquitectura misma del cálculo.

técnico y gobernanza social. En efecto, el crecimiento exponencial del poder computacional no ocurre en un vacío: sus implicaciones éticas, políticas y geopolíticas se vuelven cada vez más visibles y controversiales. Desde el uso de algoritmos en procesos electorales hasta la vigilancia masiva y el uso de IA en decisiones judiciales o financieras, la relación entre poder computacional y poder social es cada vez más estrecha. Como advierte Ensmenger (2010), "el control del código es una forma contemporánea de control político, económico y cultural" (p. 211). El uso de sistemas algorítmicos en el gobierno, la policía predictiva, la publicidad personalizada y la moderación de contenido en redes sociales ha generado debates sobre discriminación algorítmica, manipulación de la opinión pública y erosión de la autonomía individual.

Además, la centralización del poder de cómputo en manos de pocas corporaciones plantea interrogantes sobre soberanía tecnológica, acceso equitativo, privacidad de los datos y el llamado capitalismo de vigilancia. En respuesta, han surgido movimientos a favor del *software* libre, la descentralización tecnológica y la alfabetización digital. También han proliferado marcos regulatorios, como el Reglamento General de Protección de Datos (en inglés, GDPR, por las iniciales de General Data Protection Regulation) en Europa, y propuestas de gobernanza de la IA centradas en el uso responsable, transparencia, explicabilidad y justicia algorítmica.

Otros frentes de expansión interesantes en la computación contemporánea son la IA con Agencia (IA Agéntica) y el entrelazamiento con las ciencias biológicas y cognitivas (es decir, la computación neuromórfica). En la IA Agéntica se utilizan agentes artificiales para realizar tareas de forma autónoma en nombre de un usuario u otro sistema. Estos agentes deben ser adaptativos y capaces de navegar entornos dinámicos para obtener los resultados deseados, con el propósito de lograr objetivos, tomar decisiones y ejecutar acciones de forma autónoma. Los agentes hacen uso de diferentes técnicas/modelos de IA con componentes como memoria, planificación, percepción del entorno, herramientas y mecanismos de control (o límites de seguridad), todo con el fin de cumplir tareas específicas y alcanzar metas definidas. No se deben confundir la IA Generativa y la IA con Agencia; los modelos fundacionales usados en la IA Generativa no poseen agencia propia. Es decir, actúan únicamente en respuesta a instrucciones o *prompts* proporcionados por humanos. Sin embargo, los modelos fundacionales son una herramienta súper útil para que agentes puedan entender y usar lenguajes humanos.

Por su parte, la computación neuromórfica intenta emular el comportamiento del cerebro mediante arquitecturas de procesamiento que imitan sinapsis y neuronas. Este enfoque busca desarrollar sistemas energéticamente eficientes y capaces

de aprender de forma continua, como el cerebro humano. Simultáneamente, la biocomputación explora el uso de ADN y moléculas como soportes de almacenamiento y procesamiento de datos. Experimentos en computación molecular han logrado realizar operaciones lógicas mediante reacciones químicas, lo que abre nuevas posibilidades para el diseño de sistemas híbridos entre biología y computación (Davis, 2018). La interfaz cerebro-computador, impulsada por tecnologías como las de Neuralink, propone una integración directa entre la actividad neuronal y los sistemas digitales. Esto plantea no solo nuevos horizontes en medicina (por ejemplo, en tratamientos para la parálisis), sino también desafíos éticos en torno a la manipulación de la conciencia, la memoria o la identidad.

Por lo tanto, la computación contemporánea se caracteriza por una paradoja: mientras sus orígenes teóricos continúan vigentes en los modelos de Turing y la arquitectura de von Neumann, sus aplicaciones se han expandido hacia dominios antes unimaginables. Desde asistentes virtuales hasta biocomputación, desde ciudades inteligentes hasta la computación afectiva, la informática moderna redefine lo posible. No se trata ya de una disciplina aislada, sino de un entramado de tecnologías, instituciones, culturas y poderes en constante evolución. El siglo XXI exige una reflexión crítica sobre el rumbo que tomará esta evolución. La capacidad de la computación para resolver problemas, amplificar capacidades humanas y reorganizar sociedades es inmensa, pero también lo son sus riesgos. Por ello, el futuro de la computación no depende únicamente de avances tecnológicos, sino también de decisiones filosóficas, éticas y políticas que moldearán su papel en el destino humano.

Cibernética y sistemas de control: el nacimiento de una nueva ciencia

Independientemente de su tamaño y capacidad de cálculo, las máquinas tratan sobre la "comunicación". De acuerdo con Rid (2016), un piloto necesita comunicarse con el avión para volarlo, pero la aeronave también necesita comunicarse con el piloto, por lo cual los dos formarían una sola entidad. Pero estas entidades hombre-máquina ya no están aisladas; es decir, ya no se limitan a un solo hombre y a una sola máquina con una interfaz mecánica, por cuanto es más probable que las máquinas contengan varios computadores conectados, a su vez, con otras máquinas en red. Esto significaría que muchas personas interactúan, en un momento determinado, con numerosas máquinas, por lo cual los aparatos electrónicos ya no serían simplemente extensiones de los músculos y cerebros humanos.

Con base en lo anterior, cabría señalar que el control y la comunicación comenzaron a cambiar de manera crítica durante la Segunda Guerra Mundial. Fue entonces cuando surgió un nuevo conjunto de ideas para el cambio: la cibernética. Se le adjudica la creación de este término a Norbert Wiener, un brillante matemático de Massachusetts Institute of Technology (MIT), aunque André-Marie Ampère fue en realidad el primero en usar el término “cibernética”, en 1834²⁰. No obstante, Wiener no sabía de ello en 1948, cuando introdujo el concepto en su obra *Cybernetics: Control and Communication in the Animal and the Machine* (Wiener, 1948), la cual estaba plagada de temerarias profecías sobre el futuro en relación con máquinas autoadaptativas que pensarían y aprenderían a ser más inteligentes que los seres humanos; en consecuencia, la opinión pública de la época celebraría a Wiener como el profeta de una segunda revolución industrial²¹.

El origen militar del concepto: Wiener y el control antiaéreo

La historia de la cibernética no puede comprenderse sin reconocer su raíz profundamente militar. Lejos de emerger en un vacío académico, la cibernética nació de una necesidad urgente: mejorar la eficacia del fuego antiaéreo aliado durante la Segunda Guerra Mundial. Esa necesidad estratégica marcó el inicio de un giro epistemológico que llevaría a Norbert Wiener y sus colaboradores a formular una teoría que unificó la biología, la ingeniería y las ciencias sociales bajo un mismo paradigma: el de los sistemas de retroalimentación. Esta urgencia bélica no solo puso a prueba los límites de la ingeniería armamentística, sino que también obligó a replantear la manera como se entendía la relación entre el ser humano, la máquina y el entorno. En ese contexto de presión tecnológica y necesidad táctica, la pregunta clave no era tan solo cómo disparar más rápido, sino cómo anticipar y corregir (en tiempo real) el comportamiento de un blanco móvil. Así, el campo de batalla se volvió un laboratorio de ideas, y la artillería antiaérea, en el catalizador de un nuevo marco conceptual que dio origen a la cibernética.

²⁰ Ampère (1843), físico y matemático francés, sugirió una clasificación terminológica ambiciosa de todo el conocimiento humano; al igual que Wiener más de un siglo después, obtuvo su inspiración del griego cuando propuso el término “cibernética”. En la antigua Grecia, los grandes barcos batallaban en el mar contra la lluvia, el viento y las mareas, cuestiones de ninguna forma predecibles. Sin embargo, si el hombre operando sobre el timón, podía mantener su mirada sobre un faro en la costa, podría manipular la caña del timón ajustándola constantemente en tiempo real, hasta alcanzar la luz emitida por el faro. Esta era la función del timonel, a quien los griegos designaban como *kybernetes*, que Wiener tradujo al inglés como “*cybernetics*”, y que en español se conoce como “cibernética”. Por lo tanto, el vocablo “cibernética” proviene del griego *kybernan*, que significa “dirigir”, “navegar” o “gobernar”.

²¹ En la primera revolución, los motores y las máquinas de producción habían reemplazado los músculos humanos; en la segunda revolución, los mecanismos de control comenzarían a reemplazar los cerebros humanos.

Durante la Segunda Guerra Mundial los Aliados enfrentaron un desafío técnico apremiante: los cazas enemigos eran capaces de realizar maniobras evasivas con tal rapidez que el fuego de los cañones antiaéreos no lograba impactarlos con precisión. Los proyectiles requerían varios segundos en alcanzar la altitud deseada, lo cual implicaba que al momento de disparar, el objetivo ya habría cambiado de posición. Esta dinámica exigía un sistema capaz de predecir el futuro comportamiento del avión enemigo basándose en sus trayectorias pasadas. Wiener fue reclutado para abordar este problema como parte de un equipo interdisciplinario que incluía al fisiólogo Arturo Rosenblueth y al ingeniero Julian Bigelow. Este trío formó el núcleo inicial de lo que más tarde sería llamado pensamiento cibernético. Su tarea consistía en diseñar un sistema de control predictivo automático que ajustara el fuego antiaéreo en tiempo real. A través de este proceso concibieron el problema como una interacción de señales, entradas, salidas y correcciones: un sistema retroalimentado que podía adaptarse a los cambios del entorno (Cifuentes, 2021a).

Este enfoque marcó un punto de inflexión: al observar los sistemas desde la perspectiva de su comportamiento funcional, y no de su estructura interna, Wiener y su equipo abrieron la puerta a una analogía formal entre máquinas y organismos vivos. La necesidad práctica de interceptar aviones se transformó así en una reflexión teórica más amplia sobre cómo los sistemas (ya fueran humanos, animales o mecánicos) procesan información, toman decisiones y se autorregulan. Esta transición del problema técnico al modelo conceptual quedaría plasmada en su primera gran contribución teórica; el resultado inicial de sus investigaciones fue el artículo "Behavior, Purpose and Teleology", publicado en 1943, donde se introdujo el análisis del comportamiento como un proceso basado en entradas (*inputs*) y salidas (*outputs*), sin necesidad de conocer los mecanismos internos del sistema: lo que hoy se conoce como enfoque de "caja negra" (Rosenblueth et al., 1943).

Esta formulación permitía tratar por igual a sistemas artificiales y biológicos, al observar tan solo su comportamiento al responder a estímulos. Pero lo revolucionario fue que esta perspectiva permitió a Wiener y sus colegas describir al avión enemigo como un "ser intencional" cuyos movimientos podían entenderse como una forma de comportamiento dirigido. A su vez, los sistemas de control antiaéreo se entendieron como agentes que debían interpretar y responder a ese comportamiento corrigiendo constantemente su puntería a partir del error de predicción. Así nació el concepto de retroalimentación negativa, o el mecanismo mediante el cual un sistema se ajusta a sí mismo para lograr un objetivo deseado.

En sus memorias, Wiener explicaría que la idea de modelar al piloto enemigo y al artillero aliado como sistemas de retroalimentación simétricos fue decisiva

para comprender que el problema del control era, en última instancia, un problema de comunicación y transmisión de información (Cifuentes, 2021b). Este modelo operacional derivó en el libro *Cybernetics: Or Control and Communication in the Animal and the Machine*, donde Wiener (1948) generalizó estos principios hacia todos los sistemas que interactúan con su entorno y se autorregulan a través del procesamiento de información. Allí formuló uno de sus postulados más conocidos: "vivir efectivamente es vivir con información adecuada" (Wiener, 1948). Desde esta óptica, un sistema abierto (como un ser vivo o un computador) es el que reduce su entropía al incorporar y procesar información del entorno. Cabe señalar que esta noción tenía implicaciones filosóficas profundas: la cibernética implicaba una ontología de sistemas informacionales donde no existía diferencia fundamental entre una máquina antiaérea y un organismo biológico, ya que ambos podían describirse como entidades capaces no solo de aprender, sino también de adaptarse mediante circuitos de retroalimentación.

El desarrollo de esta teoría desde un contexto de guerra no fue una coincidencia. Como ha documentado Thomas Rid (2016), la cibernética nació como "una ciencia del conflicto", en un contexto donde la supervivencia nacional dependía de la capacidad para anticipar y responder al comportamiento enemigo. De ahí que conceptos como predicción, corrección, homeostasis y adaptación tuvieran una importancia tan decisiva. En otras palabras, la guerra no solo fue el terreno de aplicación de estas ideas, sino también su matriz intelectual, ya que la presión por desarrollar sistemas eficaces de defensa terminó convirtiendo a los modelos de retroalimentación en herramientas no solo técnicas, sino epistemológicas: es decir, instrumentos que permitían comprender la acción en contextos dinámicos e inciertos.

Así, lo que empezó como un esfuerzo por automatizar el control de tiro evolucionó hacia una teoría general del comportamiento adaptativo en sistemas complejos. Rid (2016) subraya que "la guerra no solo fue el telón de fondo, sino el catalizador del pensamiento cibernético" (p. 95), al obligar a los científicos a pensar en términos de sistemas dinámicos, incertidumbre y control en condiciones extremas. Es decir, el factor antiaéreo era no simplemente un problema técnico, sino el símbolo de un nuevo paradigma, donde la tecnología se pensaba como una extensión del conocimiento humano en el campo de batalla (Rid, 2016). De esta manera, el sistema de control predictivo no solo resolvía un problema táctico inmediato, sino que sentaba las bases de una nueva epistemología técnica. El antiaéreo se convirtió en el arquetipo de sistemas capaces de percibir, procesar y reaccionar frente a su entorno, y ello desplazó la visión mecanicista tradicional hacia una concepción más dinámica y adaptativa de las máquinas.

Esta reconceptualización sembró el terreno para aplicaciones mucho más amplias, cuyas ramificaciones se expandirían velozmente tras el conflicto. En efecto, el trabajo pionero de Wiener fue mucho más allá del control de tiro. El modelo cibernético se convirtió en una matriz teórica que influiría en campos tan diversos como la neurofisiología, la sociología, la ecología, la psicología conductual, la teoría de sistemas, la IA y la teoría de la información. La matriz epistemológica del control predictivo continúa informando los desarrollos contemporáneos en defensa y seguridad, desde los sistemas de radar y misiles teledirigidos hasta la guerra algorítmica y la vigilancia automatizada. En todos esos sistemas se preserva el núcleo original del modelo cibernético: anticipar el comportamiento de un adversario en tiempo real mediante la modelación matemática de sus acciones pasadas.

Pese a su origen militar, Wiener (1954) fue uno de los primeros en advertir los peligros de la aplicación irrestricta de la cibernética a la organización social. En *The Human Use of Human Beings* expresó su preocupación por una sociedad gobernada por autómatas sin ética. Insistió en que la cibernética debía servir a fines humanistas, y no deshumanizantes, y destacó que el conocimiento del control podía ser usado tanto para la opresión como para la emancipación (Wiener, 1963). Esta dualidad se halla presente desde los inicios del concepto, pues la misma teoría que permitía derribar aviones enemigos también podía inspirar la comprensión de sistemas humanos como las redes neuronales, los sistemas democráticos o las economías abiertas. En este sentido, la cibernética fue desde el inicio una ciencia ambigua: forjada en el conflicto, pero abierta al diálogo interdiscursivo.

La cibernética como teoría general de sistemas

Como ya se mencionó, tras su origen militar en el diseño de sistemas de control predictivo la cibernética dio un salto epistemológico para convertirse en una teoría general de sistemas adaptativos. Esta transición no fue una simple ampliación del campo donde se aplica, sino la cristalización de una nueva ontología científica: la que considera que los fenómenos naturales, técnicos y sociales pueden ser modelados como sistemas autorregulados de procesamiento de información. De acuerdo con Cifuentes (2021a), la cibernética no fue tan solo una ciencia de la regulación, sino una perspectiva del mundo que hizo del intercambio de información “la esencia de varios fenómenos” en las ciencias naturales y sociales.

El paso de la “primera cibernética” (centrada en el control y la homeostasis) hacia una teoría de sistemas más amplia se consolidó a través del trabajo interdisciplinario de las décadas de los 1950 y 1960, particularmente en las conferencias

Macy. Estas reuniones congregaron a biólogos, ingenieros, psicólogos, antropólogos y matemáticos, quienes compartían la convicción de que sistemas tan disímiles como una célula, una empresa o una máquina podían entenderse mediante los principios de la retroalimentación y la comunicación. Esta perspectiva fue la base del paralelismo entre cerebros, computadores y organizaciones sociales, ya que todos ellos son sistemas complejos, dinámicos y adaptativos (tabla 2).

Tabla 2. Las cuatro generaciones de la cibernética

Generación	Enfoque central	Metáfora / modelo	Dominio principal	Autores clave	Contribuciones destacadas
1ª cibernética (1943-1960)	Control; retroalimentación negativa; estabilidad	Termostato/ sistema homeostático	Ingeniería; fisiología; física	Norbert Wiener; Warren McCulloch; John von Neumann	Formalización del <i>feedback</i> ; analogía máquina-organismo; sistemas cerrados
2ª cibernética (1960-1980)	Autopoiesis; autoorganización; autorreferencia	El sistema que se observa a sí mismo	Epistemología; biología cognitiva; gestión organizacional	Heinz von Foerster; Humberto Maturana; Francisco Varela; Stafford Beer	Observador incluido; teoría de sistemas vivos; gestión viable
3ª cibernética (1980-2000)	Comunicación; sistemas sociales; complejidad reflexiva	Sociedad como sistema autopoietico	Sociología; teoría de medios; ciencias sociales	Niklas Luhmann; Klaus Krippendorff; Félix Geyer	Cibernética del discurso; teoría de sistemas sociales; reflexividad
4ª cibernética (2000-actualidad)	Computación distribuida; inteligencia artificial; hiperconectividad	Red algorítmica adaptativa/ sistemas no lineales	IA; <i>big data</i> ; gobernanza digital; filosofía de la tecnología	Donna Haraway; Shoshana Zuboff; Ben Grosser (entre otros)	Sistemas autónomos de decisión; vigilancia algorítmica; ética del código

Fuente: elaboración propia.

Simultáneamente, la teoría general de sistemas propuesta por Ludwig von Bertalanffy reforzó esta tendencia al ofrecer un marco epistemológico que aspiraba a superar la fragmentación disciplinaria de las ciencias. Según Bertalanffy (1968), “lo que es común a todas las ciencias puede convertirse en una teoría general de los sistemas” (p. 32). Desde esa óptica, la cibernética ofrecía no solo un modelo funcional de regulación, sino una arquitectura conceptual para estudiar las estructuras y procesos comunes a sistemas físicos, biológicos y sociales. En ese sentido, la cibernética se constituiría como una teoría general de las máquinas,

es decir, una disciplina científica que buscaba dominar el rápido aumento del progreso computarizado, y que, al constituirse en una ciencia interdisciplinar, estaría ligada a la física y al estudio del cerebro y de los computadores.

Según Beer (1995a), la cibernética estudiaría los flujos de información que rodean un sistema, y la forma como esta información es usada por el sistema como un valor que le permite controlarse a sí mismo, lo cual ocurre para sistemas tanto animados como inanimados. Esta visión integral permitió la expansión del pensamiento cibernético hacia campos como la biología del comportamiento, la organización empresarial, la psicoterapia, las ciencias de la computación, la ingeniería de sistemas y la automatización industrial. Pero pronto surgiría un giro más radical: la segunda cibernética, también conocida como cibernética de segundo orden, desarrollada por Heinz von Foerster.

Por consiguiente, la noción de sistema implicaba, en ese contexto, una serie de propiedades fundamentales, como la autorregulación, apertura al entorno, interdependencia de las partes, retroalimentación negativa (y más adelante, positiva), así como la capacidad de adaptación. El modelo cibernético enriquecía esta visión añadiendo una dimensión informacional, al concebir que el comportamiento de los sistemas dependía de su capacidad para recibir, procesar y responder a señales del entorno. En esta convergencia entre cibernética y sistemas se consolidó una lógica de causalidad circular, opuesta a los esquemas lineales y mecanicistas del pensamiento moderno. La retroalimentación negativa (clave en la termorregulación biológica) pasó a entenderse como una ley estructural de los sistemas dinámicos. Pero pronto surgiría un giro más radical: la segunda cibernética, desarrollada por Heinz von Foerster. Este enfoque reconocía que el observador no es externo al sistema observado, sino que forma parte de dicho sistema. La objetividad fue reemplazada por una epistemología constructivista donde el conocimiento es siempre una construcción situada, contextual y recursiva.

Foerster (2003) propuso que los sistemas que contienen descripciones de sí mismos (como los seres humanos y las instituciones sociales) requieren una lógica autorreferencial. Así, el observador ya no es un espectador neutro, sino, por el contrario, un participante activo que modifica el sistema con su propia intervención. En esta línea la cibernética dejó de ser solo una ciencia del control para convertirse en una ciencia de la observación de sistemas observantes. Esta ampliación abrió nuevas posibilidades en campos como la sociología, la terapia sistémica, la pedagogía y la teoría organizacional.

La confluencia entre teoría de sistemas, cibernética y constructivismo tuvo efectos duraderos. Según indica Bowker (1993), la cibernética actuó como una disciplina "trianguladora", que permitía a los investigadores legitimar sus enfoques al adoptar su lenguaje conceptual (mensaje, *feedback*, homeostasis, adaptación) y generaba así una red cognitiva entre campos disímiles. Por esa vía, se estableció una epistemología sistémica que perdura en los estudios contemporáneos sobre redes, resiliencia, inteligencia artificial, aprendizaje organizacional y gobernanza distribuida. En suma, la cibernética como teoría general de sistemas consolidó una matriz epistemológica que integra información, control y complejidad. Su legado reside no solo en sus aplicaciones técnicas, sino en haber producido una revolución conceptual en nuestra forma de comprender el mundo: ya no como un conjunto de entidades estáticas, sino como una compleja red de sistemas interconectados que aprenden, se regulan y se transforman a través del flujo constante de la información.

Shannon, bits e información como poder

No fue una coincidencia que la cibernética emergiera del contexto bélico de la Segunda Guerra Mundial. La aceleración del ritmo estratégico en los conflictos de tercera generación (impulsada, en gran medida, por el desarrollo del poder aéreo) exigió nuevas formas de pensar la coordinación, el control y la anticipación (Álvarez et al., 2017). Esta transformación coincidió con dos innovaciones clave que marcaron el umbral de una nueva era tecnológica: el transistor y el dígito binario. En 1948 los laboratorios de Bell Telephone anunciaron la invención del transistor, un pequeño semiconductor capaz de amplificar y conmutar señales eléctricas, lo que inició una revolución en la electrónica al sentar las bases de la miniaturización y la ubicuidad tecnológica. Sin embargo, como señala Gertner (2012), a pesar de su enorme impacto, el transistor no fue el avance más trascendental de ese año. Dicho lugar le corresponde a una idea mucho más abstracta, pero de consecuencias globales: la formalización del concepto de la información como entidad medible en bits, realizada por Shannon (1948) en su teoría matemática de la comunicación. Fue el nacimiento de la información como poder.

Para 1948 el sistema Bell gestionaba diariamente más de 125 millones de conversaciones, que transitaban a través de 222 millones de km de cable y 31 millones de teléfonos distribuidos en los Estados Unidos (Gleick, 2011). Sin embargo, tales cifras eran apenas aproximaciones físicas de un fenómeno más complejo: la comunicación. Por ende, ¿qué se estaba midiendo realmente en esa vasta red? No eran

conversaciones completas, ni palabras ni caracteres. Lo que se contaba era, en última instancia, la electricidad. Para los ingenieros de Bell, la electricidad representaba una forma abstracta del habla humana, una transducción de las ondas acústicas generadas por la voz en señales eléctricas que viajaban a través del cableado telefónico. Esta conversión eléctrica era, precisamente, lo que distinguía al teléfono de su predecesor, el telégrafo²², cuya lógica operaba mediante la codificación de información en secuencias discretas de puntos y rayas. Así, tanto el telégrafo como el teléfono compartían una premisa fundamental: la comunicación es posible gracias a una codificación de señales que pueda ser transmitida, decodificada y comprendida. Este sería un principio que Claude Shannon²³ llevaría al extremo teórico al postular que toda información podía ser cuantificada, medida y optimizada.

La formulación de la teoría matemática de la comunicación por parte de Shannon (1948) representa uno de los hitos más influyentes en la historia de la computación, la cibernética y la transformación digital del mundo contemporáneo. Esta teoría no solo ofreció una definición rigurosa del concepto de información, sino que sentó las bases técnicas y conceptuales que permitirían entender la transmisión de mensajes, la codificación de señales y la medición del contenido informacional de cualquier sistema comunicativo. En este marco, el bit²⁴ se convirtió en la unidad elemental de medida de la información, y transformó profundamente

²² El telégrafo desempeñó un papel estratégico decisivo en la historia militar moderna, en particular durante la Primera Guerra Mundial. Esta tecnología transformó de modo radical la forma como los estados mayores de las Fuerzas Militares comunicaban órdenes y recibían reportes desde el frente reduciendo drásticamente los tiempos de transmisión de información táctica y estratégica. Por ejemplo, durante la Primera Guerra Mundial la guerra de trincheras en el Frente Occidental dependía del telégrafo para coordinar los movimientos de tropas, artillería y suministros en una línea de batalla de más de 700 km (Álvarez et al., 2017). Asimismo, el uso de cables submarinos permitió a las potencias imperiales mantener contacto con sus colonias, aunque también se convirtieron en blancos estratégicos: al inicio de la guerra, Gran Bretaña cortó los cables submarinos alemanes, lo que obligó al Reich a depender de la radio, cuya señal era más fácil de interceptar. Así, el telégrafo no solo aceleró el mando y control, sino que también introdujo nuevas vulnerabilidades que anticiparían la guerra electrónica del siglo XX.

²³ Shannon fue influenciado ampliamente por el matemático inglés y descifrador de códigos Alan Turing, y por los matemáticos estadounidenses George Campbell y Norbert Wiener. Este último lo introdujo a la disciplina de la "cibernética", el estudio de la comunicación y el control (Sohni & Goodman, 2017).

²⁴ El término "bit" (del inglés *binary digit*) designa la unidad mínima de información en los sistemas digitales clásicos. Representa una distinción binaria entre dos estados posibles, convencionalmente codificados como 0 y 1, que en la práctica pueden materializarse como diferencias de voltaje, polaridad magnética o estados electrónicos en un circuito integrado. La arquitectura computacional moderna se fundamenta en la combinación masiva de dichos estados discretos permitiendo que toda forma de texto, imagen, sonido o cálculo lógico sea traducida a secuencias binarias. En este marco, el byte constituye una agrupación estandarizada de ocho bits, utilizada como unidad operativa básica para la representación simbólica de caracteres y estructuras de datos más complejas.

no solo el mundo de las telecomunicaciones, sino también las nociones de poder, control y conocimiento en la era digital.

Gracias a la teoría de la información, Shannon (1948) construiría un puente entre la información y la computación, al simplificar y medir en “pedazos” un concepto que hasta ese momento era intangible²⁵. La formalización matemática de la información sentó las bases para la creación de tecnologías como los discos compactos, las máquinas de fax, los computadores y, en última instancia, el ciberespacio. Conjuntamente con la revolución de la microelectrónica, la teoría de la información dio origen a nuevas formas de almacenamiento, procesamiento y recuperación de datos, y así propició el tránsito histórico de la humanidad desde las eras del Hierro y del Vapor hacia la denominada Era de la Información. Este giro epistémico no solo reconfiguró la infraestructura tecnológica, sino que también permeó transversalmente todas las ramas del conocimiento²⁶, al transformar la manera como se produce, organiza y comunica el saber científico.

El punto de partida de la teoría de Shannon fue una pregunta en apariencia sencilla, pero de implicaciones enormes: ¿cómo medir la cantidad de información contenida en un mensaje? Hasta ese momento la comunicación había sido estudiada en términos cualitativos o semióticos. Sin embargo, Shannon propuso una formalización cuantitativa, inspirada en modelos de la física estadística y la termodinámica, en particular en la entropía de Boltzmann. De allí surgió una definición de la información como una reducción de incertidumbre, cuantificable en bits (Shannon, 1948). La medida de entropía propuesta por Shannon, que expresa el grado de aleatoriedad o imprevisibilidad de un mensaje, permitió formalizar matemáticamente la noción de “información”. Como lo explican Soni y Goodman (2017), “el mensaje más informativo es el más improbable” (p. 112), y por ello la información se convierte en una propiedad estadística de las probabilidades

²⁵ Lo que los angloparlantes llaman “*Computer Science*”, los de habla castellana, francesa y alemana lo denominan “informática”, “*informatique*” e “*informatik*”, respectivamente.

²⁶ Por ejemplo, la economía se está reconociendo a sí misma en la actualidad como una ciencia basada en la información, ahora que las finanzas mundiales y el dinero fluyen cada vez más en bits y pueden ser almacenados en la memoria del computador. Pero incluso cuando el dinero parecía ser un tesoro material tangible, resguardado en bóvedas bancarias, en realidad siempre fue información, ya que las monedas y los billetes eran solo tecnologías de corta duración para generar información sobre quién poseía qué. Incluso la biología se ha convertido en una ciencia de la información, una materia de mensajes, instrucciones y código; los genes encapsulan la información y permiten procedimientos para leerla y escribirla, lo cual hace que el cuerpo mismo sea un procesador de información. En efecto, la memoria reside no solo en el cerebro, sino también en cada célula, por lo cual no es informático de extrañar que la genética floreciera junto con la teoría de la información; el ADN es la molécula de información por excelencia, el procesador de mensajes más avanzado a nivel celular: un alfabeto y un código de 6 mil millones de bits para formar un ser humano.

asociadas a cada símbolo del alfabeto comunicacional. Ese enfoque separó, por primera vez, la semántica del mensaje de su estructura, y así permitió tratar de forma unificada tanto las señales lingüísticas como los impulsos eléctricos, las imágenes o cualquier forma de comunicación codificada.

La conexión entre la teoría de la información y el procesamiento digital fue inmediata. Desde sus primeras investigaciones Shannon había demostrado que la lógica booleana podía implementarse mediante circuitos eléctricos binarios, un hallazgo presentado en su tesis de maestría en 1937, y considerado el origen del diseño de circuitos digitales modernos (O'Regan, 2012, p. 51). En ese sentido, Shannon no solo fundó la teoría matemática de la información, sino que también proporcionó el lenguaje lógico y técnico para la arquitectura de los computadores electrónicos. De esta forma, todo mensaje, sin importar su contenido, podía reducirse a una secuencia de bits procesables por máquinas digitales; según Nahin (2012), esta conceptualización permitió que "la lógica simbólica se convirtiera en ingeniería práctica" (p. 137), y que se uniesen de manera definitiva las matemáticas.

La teoría de Shannon explicó no solo cómo representar la información, sino también cómo optimizar su transmisión. Introdujo, además, el concepto de "redundancia" como parte inevitable de todo lenguaje, lo cual abrió el camino a técnicas de compresión de datos y corrección de errores. El uso eficiente del canal de comunicación (maximizando la tasa de transmisión sin aumentar la probabilidad de error) se convirtió en un principio técnico con enormes implicaciones económicas, militares y políticas. En sus desarrollos posteriores Shannon (1949) aplicó estas ideas a los sistemas de cifrado y seguridad introduciendo los conceptos de "confusión" y "difusión" como estrategias para dificultar el análisis criptográfico de mensajes cifrados, conceptos que hoy son fundamentales en el diseño de algoritmos criptográficos modernos (Dooley, 2013). Así, el control de la información ya no se limitaba a la transmisión, sino que se extendía a su protección, selección y manipulación. Como ha argumentado Rid (2016), la teoría de Shannon fue clave para transformar la información en un recurso estratégico, en tanto su gestión podía traducirse directamente en ventaja operacional.

Por lo dicho, no sorprende que la "revolución shannoniana" tuviese profundas consecuencias epistemológicas y políticas. Desde la perspectiva cibernética, la información se convirtió en la "sustancia" que atraviesa todos los sistemas vivos, técnicos y sociales; como escribió Wiener (1954), "la información es información, no materia ni energía" (p. 132), una afirmación que abría la posibilidad de construir un nuevo paradigma científico centrado en el flujo informacional como principio organizador de la realidad. Esta ontología informacional derivada de Shannon y

Wiener implica una visión del mundo en la cual los sistemas (desde el cerebro humano hasta una red de sensores) se definen por su capacidad para recibir, procesar y responder a la información. En palabras de Beer (1995b), "la cibernética estudia los flujos de información que rodean un sistema y la forma en que esta información es usada por el sistema como un valor que le permite controlarse a sí mismo" (p. 33). Este enfoque es en especial importante en contextos de control social, gestión organizacional y gobernanza automatizada.

Con el avance de las tecnologías digitales, los principios de Shannon fueron luego adoptados como base de las telecomunicaciones globales, almacenamiento de datos masivos, computación distribuida y sistemas inteligentes. En la actualidad, los algoritmos que rigen las plataformas digitales, la IA y la vigilancia masiva siguen principios que derivan directamente de esta teoría de la información. Como lo resume Arquilla (2021), "en el nuevo campo de batalla de la red, el dominio de la información equivale al dominio del poder" (p. 46). La digitalización global, que convierte todo evento en dato, y todo dato, en recurso, ha transformado los bits en una forma concreta de poder económico, político y militar. En este sentido, la teoría de Shannon explica no solo cómo funciona la tecnología digital, sino también cómo se configuran las relaciones de poder en la era informacional.

En consecuencia, el impacto de Shannon ha sido tal que hoy se habla de una "era de la información" para describir el periodo histórico inaugurado por sus hallazgos. Como afirman Soni y Goodman (2017), su legado reside no solo en sus fórmulas, sino en haber transformado una noción abstracta (la información) en una herramienta universal para comprender y modificar el mundo. Esta concepción ha permeado disciplinas tan diversas como la neurociencia, la sociología, la lingüística computacional y las ciencias militares. En el campo de la computación, su influencia se manifiesta en cada dispositivo que codifica y decodifica datos; en la arquitectura de internet, basada en paquetes de bits; en los algoritmos de compresión y encriptación, y en los modelos de aprendizaje automático que estructuran los sistemas inteligentes contemporáneos. Como lo resume Nahin (2012), "Shannon no solo creó una teoría, sino una nueva manera de pensar" (p. 189).

Computación y guerra: de Turing a ARPANET

La historia evolutiva de la computación moderna no puede comprenderse sin reconocer su íntima relación con el conflicto bélico, en especial con las guerras mundiales del siglo XX. Lejos de ser un producto exclusivo del progreso académico, el

computador nació en el crisol de la guerra, moldeado por las urgencias estratégicas, las necesidades de decodificación y el desarrollo acelerado de tecnologías orientadas al control, la vigilancia y la comunicación segura. Por ello y desde sus orígenes, la computación no ha sido una tecnología neutral, sino una herramienta estratégica moldeada por los imperativos de la guerra. Como subraya Gray (2004), “la computadora es tanto una creación de la guerra como una solución a sus dilemas” (p. 22).

Durante la Segunda Guerra Mundial las necesidades de calcular las trayectorias balísticas y mejorar el control antiaéreo impulsaron avances sin precedentes en la teoría computacional y en la ingeniería electrónica. De igual modo, avances en criptografía y telecomunicaciones generaron un nuevo campo de batalla invisible: el de la información. En este contexto, Bletchley Park, una antigua mansión rural inglesa, se convirtió en el centro de operaciones más importante para la inteligencia aliada. Allí, matemáticos, ingenieros y lingüistas británicos (bajo el liderazgo intelectual de figuras como Alan Turing y Gordon Welchman), descifraron los códigos secretos de la máquina Enigma y, más tarde, los complejos cifrados del sistema Lorenz, utilizado por el alto mando alemán. Este esfuerzo no solo cambió el curso del conflicto, sino que sentó las bases teóricas y prácticas de la computación digital (Copeland, 2006).

La posguerra no detuvo este vínculo. Por el contrario, la Guerra Fría hizo de la computación uno de los pilares de la estrategia de disuasión y del control militar. La amenaza de una guerra nuclear incentivó la creación de sistemas computacionales descentralizados, capaces de sobrevivir a un ataque y garantizar la continuidad del mando y control. En este contexto surgieron proyectos como SAGE, el sistema de defensa aérea de Estados Unidos, y más adelante, ARPANET, la red que daría origen a internet (Hafner & Lyon, 1998). Dichas infraestructuras fueron concebidas desde el principio como tecnologías duales: al servicio de la seguridad nacional, pero con potencial de reaprovechamiento civil.

Segunda Guerra Mundial, Bletchley Park y Enigma

La historia de la computación moderna está inextricablemente ligada a los imperativos militares de la Segunda Guerra Mundial. Aunque desarrollos teóricos como la máquina universal de Turing ya habían sido formulados en el plano matemático, fue el conflicto global lo que catalizó su concreción tecnológica. En este contexto, el criptoanálisis, particularmente el esfuerzo por descifrar los códigos de la máquina militar alemana Enigma, se convirtió en el campo de aplicación más importante para el desarrollo de computadores electromecánicos y electrónicos (Copeland,

2006). En el corazón de este esfuerzo estuvo Bletchley Park, una finca rural inglesa convertida en la sede del *Government Code and Cypher School (GC&CS)*, donde matemáticos, lingüistas, criptógrafos e ingenieros trabajaron con celo para romper los códigos cifrados del Tercer Reich, en particular los generados por la máquina Enigma. Entre ellos destacó Alan Turing, quien propuso un enfoque radicalmente nuevo para la decodificación sistemática construyendo máquinas electromecánicas conocidas como "bombas", que simulaban el funcionamiento de la máquina Enigma, lo que redujo millones de posibles combinaciones a un conjunto más manejable de soluciones plausibles (Turing, 2022).

La máquina Enigma, desarrollada originalmente por el ingeniero alemán Arthur Scherbius después de la Primera Guerra Mundial, fue adoptada por la *Wehrmacht* para cifrar sus comunicaciones militares. Su principio de funcionamiento se basaba en un sistema de rotores que transformaba los caracteres ingresados mediante un complejo patrón eléctrico y mecánico generando un alfabeto polialfabético altamente variable. Cada pulsación de tecla alteraba el estado de los rotores produciendo una nueva configuración criptográfica, lo cual hacía teóricamente imposible repetir un mensaje con la misma codificación dentro de un mismo día. Por ende, el cifrado de Enigma se consideraba prácticamente irrompible, ya que generaba a diario 150 trillones de combinaciones posibles (Hodges, 2014). Para los modelos militares, el número de configuraciones superaba los 10^{114} , especialmente cuando se añadía la variabilidad del *plugboard*, o tablero de conexiones (*Steckerbrett*), que intercambiaba pares de letras antes y después del paso por los rotores. Este grado de complejidad llevó a que las fuerzas del Eje confiaran ciegamente en su sistema.

Sin embargo, el primer gran avance para descifrar Enigma no vino del Reino Unido, sino de Polonia. En los años treinta, el matemático Marian Rejewski, apoyado por sus colegas Jerzy Różycki y Henryk Zygalski, desarrolló métodos algebraicos y máquinas llamadas *bomba kryptologiczna* para romper el cifrado. Gracias a información obtenida por los servicios franceses a través del espía alemán Hans-Thilo Schmidt, los polacos lograron un conocimiento operacional del sistema. En julio de 1939, ante la inminencia de la guerra, compartieron su trabajo con los británicos y franceses en una reunión secreta en Pyry, cerca de Varsovia.

En consecuencia, cuando el conflicto estalló, el Reino Unido organizó el centro de Bletchley Park para continuar el trabajo polaco y enfrentar la evolución técnica del Enigma alemán (Copeland, 2006). El matemático Alan Turing fue uno de los protagonistas principales en este nuevo capítulo, al diseñar una nueva máquina

electromecánica: la Bombe británica, que posteriormente sería mejorada por el ingeniero Harold Keen. La Bombe automatizaba la búsqueda de las configuraciones posibles de Enigma basándose en *cribs*: es decir, suposiciones conocidas sobre el contenido de los mensajes. Este uso sistemático de lógica matemática y principios estadísticos permitió reducir el tiempo de descifrado de semanas a horas (Gray, 2004). Por ende, la integración de lógica binaria, configuraciones de cableado, tambores giratorios y retroalimentación eléctrica transformó esta máquina en un precursor directo de la computación digital.

El trabajo en Bletchley fue obra no solo de genios individuales, sino también de una organización sistemática. Gordon Welchman, otro de sus matemáticos clave, introdujo mejoras organizativas al proceso de criptoanálisis, como la creación de redes de interceptación y la conexión más estrecha entre descifradores y las unidades militares que usaban la inteligencia generada. Según Copeland (2006), fue así como se formaron las célebres Huts, o secciones especializadas en diferentes ramas del esfuerzo, como la Marina (Hut 8) y el Ejército (Hut 6). Uno de los mayores retos fue romper también el cifrado naval alemán, particularmente el que usaban los *U-boats* del Atlántico, ya que estos submarinos hundieron centenares de embarcaciones de los Aliados durante los primeros años de la guerra, lo que puso en jaque la supervivencia de Gran Bretaña. Pero gracias a varias capturas de material cifrado en *U-boats* hundidos, como el U-559, y a las máquinas Bombe, el equipo de Turing logró romper este cifrado en 1941. El resultado fue inmediato: los convoyes aliados pudieron ser desviados, y así reducir dramáticamente las pérdidas.

En efecto, el impacto de estos logros fue enorme. Según Eisenhower, sin la labor de descifrado de Bletchley Park la guerra podría haber durado dos años más, con consecuencias devastadoras para Europa (Copeland, 2006). Pero más allá de su efecto estratégico inmediato, el proyecto Enigma estableció una arquitectura conceptual que marcaría el futuro de la computación: la idea de que una máquina puede operar de manera lógica sobre símbolos representativos de información. Este concepto se vería cristalizado posteriormente en la máquina de Turing y en las arquitecturas de von Neumann.

Paralelamente, el GC&CS se enfrentaba a un nuevo reto: el cifrado de alto nivel del ejército alemán con la máquina Lorenz SZ40/42, apodada "Tunny" por los británicos. A diferencia de Enigma, Lorenz no se usaba en campo de batalla, sino para comunicaciones estratégicas entre el alto mando alemán y sus unidades. Para romper este cifrado el matemático Bill Tutte dedujo su estructura lógica sin haber visto nunca una Lorenz, y el ingeniero Tommy Flowers diseñó el Colossus,

considerada por muchos el primer computador electrónico programable del mundo, específicamente para automatizar la tarea (Swedin & Ferro, 2022).

A diferencia de las Bombe, el Colossus era completamente electrónico, utilizando tubos de vacío para realizar operaciones lógicas a una velocidad sin precedentes (Copeland, 2006). La operación del Colossus requirió la lectura de cintas perforadas a velocidades superiores a los 5.000 caracteres por segundo, procesando patrones lógicos que evaluaban las probabilidades de clave correcta. Aunque no era un computador de uso general, introdujo muchos de los conceptos de la programabilidad y la manipulación de datos binarios en tiempo real (Turing, 2022). Estos desarrollos sentaron las bases para la computación electrónica de posguerra. Las experiencias adquiridas por ingenieros y matemáticos en Bletchley Park fueron cruciales para proyectos como ENIAC, en Estados Unidos, y para el desarrollo posterior de los primeros lenguajes de programación. La guerra no solo había exigido una revolución tecnológica: también había generado una nueva forma de concebir la información como un recurso militar crítico.

La historia de Enigma también ilustra la transición de la criptografía clásica al criptoanálisis computacional. A diferencia de los sistemas anteriores, basados en ingenio manual, los sistemas alemanes exigieron el desarrollo de herramientas técnicas avanzadas. En este sentido, Bletchley Park fue un laboratorio de innovación que combinó matemática, ingeniería, lógica y organización industrial. En síntesis, el episodio de Bletchley Park y la lucha contra Enigma representa uno de los momentos fundacionales de la historia de la computación. En medio del caos bélico, la información se transformó en un arma, y el pensamiento algorítmico, en una forma de poder. Como señala Arquilla (2021), la información es el nuevo dominio de la estrategia, una afirmación cuya genealogía comienza en gran medida en los pasillos secretos de Bletchley Park.

Guerra Fría, disuasión nuclear y redes descentralizadas

Desde su nacimiento, la computación ha estado profundamente vinculada a los intereses estratégicos, militares y geopolíticos de los Estados. Lejos de ser una herramienta neutral, la historia de los computadores y sus aplicaciones ha sido moldeada por imperativos de defensa, espionaje y disuasión. Tal como sostiene Gray (2004), la computación no solo ha sido "un instrumento de guerra", sino una transformación conceptual del campo de batalla, donde la información se convierte en un dominio decisivo de poder. Tras el uso de computadores como la Bombe, en Bletchley Park, para descifrar los mensajes alemanes codificados con Enigma,

los líderes militares y políticos comprendieron que el dominio de la información podría decidir el curso de una guerra; en efecto, Edwards (1996) ha documentado ampliamente cómo el desarrollo de la computación durante y después de la Segunda Guerra Mundial estuvo intrínsecamente ligado al desarrollo de capacidades de comando, control y comunicación, lo que en el argot militar se sintetiza como C3I.

En este contexto, el desarrollo del ENIAC, en Estados Unidos, no fue una coincidencia, sino una respuesta a las exigencias del cálculo balístico y la simulación de trayectorias de artillería. ENIAC, terminado en 1945, fue concebido sobre todo como una herramienta para calcular tablas de tiro para el Ejército, y aceleró así procesos que antes tardaban semanas. Su capacidad para hacer cinco mil sumas por segundo fue revolucionaria y sentó las bases para los computadores electrónicos modernos (Haigh et al., 2016).

La Guerra Fría amplificó esta tendencia, ya que los computadores se convirtieron en núcleos de los sistemas de vigilancia, alerta temprana y simulación nuclear. La doctrina de la destrucción mutua asegurada (en inglés, MAD, por las iniciales de *Mutually Assured Destruction*), se basaba en gran medida en la capacidad para detectar un ataque y responder en cuestión de minutos. Esto implicó el desarrollo de sistemas informáticos que pudieran integrar datos de radares, satélites y sensores en tiempo real; como señala Campbell-Kelly (2003), las necesidades del Pentágono fueron el verdadero motor de la industria computacional durante décadas, al financiar proyectos como SAGE (por las iniciales de *Semi-Automatic Ground Environment*), que integraba radares y centros de comando mediante redes de computadores.

Al mismo tiempo, la IA tuvo en sus orígenes apoyo en propósitos militares. El proyecto DARPA (por las iniciales de Defense Advanced Research Projects Agency), creado en 1958 como respuesta al Sputnik soviético, financió muchas de las primeras investigaciones en redes neuronales, aprendizaje automático y procesamiento del lenguaje natural. Según Arquilla (2021), la relación entre IA y guerra no es reciente, sino constitutiva del desarrollo tecnológico de la Guerra Fría, donde la capacidad para tomar decisiones automatizadas se volvió una ventaja competitiva crucial.

Asimismo, el espionaje electrónico se transformó con los computadores. Desde el procesamiento masivo de interceptaciones hasta el análisis criptográfico, agencias como la National Security Agency (NSA) y la *Komitet Gosudárstvennoy Bezopásnosti* (KGB) invirtieron enormes recursos en desarrollos algorítmicos. Esto incluía tanto el uso de la computación para descifrar comunicaciones enemigas

como para proteger las propias. El trabajo de Bamford (2001) sobre la NSA revela la magnitud del espionaje computacional desde la década de 1960 en adelante, cuando el procesamiento de datos se volvió un objetivo estratégico en sí mismo.

No menos importante fue el papel de la simulación en la planificación militar. Desde el modelado de explosiones nucleares hasta las proyecciones de escenarios de guerra, los computadores fueron esenciales para comprender y anticipar comportamientos complejos. Como explica Rid (2016), la cibernética, entendida como la ciencia del control y la comunicación, se volvió un lenguaje común entre ingenieros, militares y científicos sociales que colaboraban en el desarrollo de sistemas de comando y simulación. De esta manera, la computación pasó de ser una herramienta de cálculo a convertirse en una arquitectura de poder; como bien señala Lyon (2003), las tecnologías de la información no solo organizaron el conflicto, sino que también moldearon la forma como se entendía el mundo: un conjunto de sistemas que podían ser observados, modelados, previstos y controlados mediante algoritmos.

En resumen, la computación como arma estratégica no es una extensión accidental de la tecnología, sino una condición originaria de su propio desarrollo histórico. Desde Bletchley Park hasta los laboratorios de DARPA, los computadores han sido diseñados tanto para comprender como para dominar entornos conflictivos, y así hacer de la guerra un laboratorio para la innovación tecnológica. Este vínculo intrínseco entre computación y conflicto se volvió aún más evidente durante la Guerra Fría, cuando la carrera armamentista y la competencia ideológica entre Estados Unidos y la URSS catalizaron un salto cualitativo en la integración de las tecnologías digitales a los sistemas de defensa. La lógica de la disuasión nuclear, basada en la necesidad de garantizar una capacidad de respuesta incluso después de un ataque devastador, planteó nuevos desafíos estratégicos: ¿cómo asegurar las comunicaciones militares en escenarios de destrucción masiva? ¿Cómo construir infraestructuras resistentes, adaptables y autónomas frente a la amenaza existencial del colapso de mando y control?

Fue en este contexto donde surgió el paradigma de redes descentralizadas, una respuesta técnico-militar a un problema político-existencial. Así, la historia de la computación dio un giro estructural, pues pasó del cálculo centralizado de la Segunda Guerra Mundial al diseño de arquitecturas distribuidas concebidas para sobrevivir al apocalipsis nuclear. Es decir, la computación dejó de ser solo una herramienta de procesamiento para convertirse en una infraestructura crítica de comunicación, comando y coordinación estratégica; la historia de ARPANET,

el Videotex y la web se inscribe, por tanto, en esta evolución geoestratégica del pensamiento técnico.

El desarrollo de las redes informáticas modernas no puede entenderse sin el impacto geopolítico del lanzamiento del Sputnik 1, por parte de la URSS, en 1957. Este hito, que convirtió al dispositivo en el primer satélite artificial en órbita, provocó una conmoción estratégica en Estados Unidos, al revelar que el país no lideraba (como se creía hasta entonces) la carrera global por la supremacía tecnológica y científica (Álvarez et al., 2019a). En respuesta, el Gobierno estadounidense intensificó significativamente su inversión en ciencia aplicada y creó la Advanced Research Projects Agency (ARPA)²⁷, institución que desempeñaría un papel crucial en el desarrollo de la computación en red.

A comienzos de la década de 1960 el mundo vivía bajo la sombra de una confrontación nuclear inminente, exacerbada por eventos como la crisis de los misiles en Cuba. Estados Unidos y la URSS estaban en plena carrera por desplegar sistemas de misiles balísticos intercontinentales (en inglés, ICBM, por las iniciales de *Intercontinental Ballistic Missiles*), y los planificadores estratégicos empezaron a preguntarse cómo podrían garantizarse las comunicaciones militares en un eventual escenario posnuclear. En concreto, preocupaba que la red telefónica nacional (altamente centralizada), no sobreviviera a un primer ataque, pues, aunque muchas líneas podrían mantenerse intactas, los centros de conmutación principales serían blancos prioritarios y fácilmente destruibles.

Fue en este contexto donde Paul Baran, investigador de RAND Corporation, propuso una solución revolucionaria. Su enfoque se basaba en un principio técnico y estratégico fundamental: eliminar los puntos únicos de fallo a través de una arquitectura distribuida. Baran imaginó una red de comunicaciones digital, descentralizada y resistente, donde no existieran nodos centrales que pudieran colapsar el sistema completo en caso de destrucción. Su diseño, conocido como “comunicaciones distribuidas”, consistía en una red de nodos autónomos que funcionarían como enrutadores redirigiendo información desde un punto a otro mediante múltiples trayectorias posibles. En consecuencia, Baran concibió un sistema que no tenía nodos centralizados y podría funcionar incluso si muchos de sus enlaces y nodos de conmutación fueran destruidos. Además, introdujo el concepto de conmutación de paquetes, una innovación crítica en la historia de

²⁷ Ahora es denominada DARPA (*Defense Advanced Research Projects Agency*), la cual se constituye en una agencia del Departamento de Defensa de los Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar.

las telecomunicaciones. En vez de transmitir los mensajes como bloques únicos, estos serían fragmentados en pequeños paquetes independientes. Cada paquete seguiría una ruta autónoma hacia su destino²⁸, donde luego sería reconstruido en el mensaje original. Este diseño no solo ofrecía eficiencia y rapidez en el almacenamiento y reenvío (*Store and Forward*), sino que también garantizaba una resiliencia sin precedentes: si uno o varios nodos eran destruidos, los paquetes simplemente buscarían rutas alternativas (Hafner & Lyon, 1998). Esta concepción sentó las bases técnicas para lo que más tarde se convertiría en ARPANET, y posteriormente, en internet.

En 1969 el concepto de arquitectura distribuida ideado por Baran fue llevado a la práctica, por primera vez a gran escala, con el despliegue de ARPANET. El primer nodo operativo se instaló en la Universidad de California (UCLA), en Santa Barbara, seguido por otros en centros clave, como el Instituto de Investigación de Stanford. Posteriormente, vino el séptimo nodo, en la sede de RAND Corporation, en Santa Mónica. Financiado por ARPA, ARPANET fue concebido en sus orígenes como una herramienta para que científicos e investigadores compartieran remotamente recursos computacionales de alto costo. Tómese en cuenta que en esa época los computadores eran grandes y costosas unidades centrales que requerían un acceso físico directo mediante terminales ubicadas en el mismo edificio o a través de mecanismos mecánicos como tarjetas perforadas. Dado el elevado costo y la disponibilidad limitada de dichos sistemas, la idea de conectar computadores entre sí para permitir el acceso remoto a programas y capacidad de procesamiento ofrecía ventajas significativas. Así, ARPANET introdujo un nuevo modelo de computación distribuida, al permitirles a los usuarios interactuar con máquinas anfitrionas situadas a cientos de kilómetros de distancia.

No obstante, en un giro inesperado, y a dos años desde su creación, ARPANET empezó a ser utilizado no solo para compartir capacidad computacional, sino como una herramienta de comunicación entre personas. Los investigadores lo convirtieron en una especie de oficina de correos electrónica de alta velocidad, que facilitaba el intercambio de información técnica, académica e, incluso, personal. De esta forma, el correo electrónico emergió como una de las primeras aplicaciones no previstas y más exitosas de la red (Martin & Carey, 2013).

En 1983 el crecimiento exponencial de la red llevó a una reestructuración importante. ARPANET se dividió en dos: una parte civil, que conservó el nombre, y

²⁸ El británico Donald Davies creó independientemente un sistema muy similar, pero los llamó "paquetes de mensajes", un término que finalmente se adoptaría en vez de los "bloques de mensajes" de Baran.

una parte militar, denominada MILNET. Este fue un paso decisivo hacia la apertura de la red a nuevos usuarios más allá del ámbito estrictamente académico o gubernamental. Al final, en 1989 el nombre ARPANET cayó en desuso y fue reemplazado oficialmente por “internet”, reflejo de su carácter global y descentralizado (Adams & Warf, 1997).

Empero, es necesario señalar que el tránsito de ARPANET a internet fue facilitado por dos desarrollos tecnológicos clave. Primero, a comienzos de los años setenta, Vinton Cerf y Bob Kahn desarrollaron el conjunto de protocolos TCP/IP (por las iniciales en inglés de *Transmission Control Protocol/Internet Protocol*, o en español, protocolo de control de transmisión/protocolo de internet), lo cual permitió que computadores con diferentes arquitecturas y sistemas operativos pudieran comunicarse a través de redes de paquetes conmutados. Segundo, a fines de los años ochenta, Tim Berners-Lee y su equipo en la Organización Europea para la Investigación Nuclear (en inglés, CERN, por las iniciales de European Organization for Nuclear Research), diseñaron la *World Wide Web* (www): un sistema de hipertexto interconectado que hizo posible la navegación a través de documentos y sitios enlazados. Este avance representó una capa de abstracción superior sobre internet y se convirtió en el núcleo de lo que hoy entendemos como la Web moderna²⁹.

La *World Wide Web* fue probada por primera vez en 1991 y lanzada oficialmente para uso general en 1993 por el CERN. Ese mismo año un equipo del Centro Nacional de Aplicaciones de Supercomputación de la Universidad de Illinois desarrolló el Mosaic Browser³⁰, una interfaz gráfica de usuario (en inglés, GUI, por las iniciales de *Graphical User Interface*) que facilitaba enormemente la navegación por sitios web. Esta innovación sentó las bases para la futura expansión de la Web, sobre todo tras el lanzamiento comercial del navegador Netscape, que amplificó aún más el acceso del público general a internet. Sin embargo, más allá de la interfaz visual, el máximo aporte conceptual de este grupo fue la implementación de un

²⁹ La expansión de internet como dominio estratégico se apoyó en dos innovaciones fundamentales: la arquitectura hipermedial y el Sistema de Nombres de Dominio (en inglés, DNS, por las iniciales de *Domain Name System*). La primera introdujo una lógica reticular de organización del conocimiento permitiendo la interconexión dinámica de contenidos y la construcción de trayectorias de navegación no lineales, condición estructural para la viralización contemporánea. El DNS, por su parte, funciona como una infraestructura crítica de traducción simbólica: convierte direcciones numéricas en nombres reconocibles estabilizando la identidad digital de actores estatales, corporativos y sociales (por ejemplo, www.esdeg.edu.co). Por lo tanto, el control, manipulación o interrupción de estas capas (hipervínculos y resolución de nombres) tiene implicaciones directas para la soberanía digital y la seguridad nacional.

³⁰ Berners-Lee y sus colegas también habían desarrollado un navegador en 1991.

modelo descentralizado muy eficaz para el intercambio de información, que prescindía de un centro único de almacenamiento y distribución (Hafner & Lyon, 1998).

Como ya se señaló, ARPANET surgió originalmente como una red limitada a instituciones vinculadas al Departamento de Defensa de Estados Unidos: por ejemplo, la Universidad de California, RAND Corporation, el Instituto de Investigación de Stanford y la Universidad de Utah. Su propósito inicial fue permitir el intercambio remoto de recursos computacionales entre tecnólogos e investigadores especializados facilitando el acceso a programas de prueba, datos científicos y, poco tiempo después, servicios emergentes como el correo electrónico, foros técnicos y conferencias virtuales. Financiado por el gobierno federal, ARPANET excluía todo uso comercial: no se permitía su uso para publicidad ni lucro algunos, y el acceso estaba restringido a entidades académicas o gubernamentales (Martin & Carey, 2013).

Luego, a mediados de la década de 1980, y con el respaldo económico de la National Science Foundation (NSF), surgió National Science Foundation's Network (NSFNET) como sucesora natural de ARPANET. Esta red se convirtió en la columna vertebral de lo que pronto sería la infraestructura civil del internet moderno³¹. Según Hiltz y Turoff (1993), NSFNET representa uno de los ejemplos más destacados del impacto positivo de la inversión gubernamental sostenida en infraestructura informacional estratégica. No obstante, a pesar de su importancia como red troncal, NSFNET carecía en sus primeros años de muchos de los componentes que hoy se consideran esenciales en la experiencia en línea: por ejemplo, aún no incluía desarrollo de contenido multimedia, ni motores de búsqueda, ni comercio electrónico, ni publicidad dirigida ni interfaces pensadas para usuarios no técnicos.

La innovación en estas áreas procedió más bien de redes paralelas y servicios *online* comerciales que comenzaron a proliferar desde mediados de la década de 1980, pues tanto ARPANET como NSFNET coexistieron con otras plataformas que ofrecían una diversidad de servicios: bases de datos empresariales (más tarde ofrecidas también a consumidores), servicios de correo electrónico, conferencias informáticas, banca electrónica incipiente, sistemas de tableros de anuncios, plataformas educativas, redes sin fines de lucro y desarrollos emergentes en *video-text*, cada uno con su propio público objetivo.

Estos ecosistemas aportaron de manera sustantiva a la edificación del conocimiento técnico y de usuario que haría posible el posterior éxito tanto del correo

³¹ Si bien no está claro cuándo se empleó por primera vez la palabra "Internet", el término ya era de uso generalizado a principios de la década de 1990, para describir aquella "interconexión" de redes informáticas de entidades en muchos países.

electrónico como de la Web en la década de 1990 (Aumente, 1987). Sin embargo, el contexto sociotécnico de esos tiempos era radicalmente distinto del actual, ya que a finales de los años setenta y durante toda la década de 1980 solo una pequeña fracción de los hogares en América, Europa y Asia tenía computadores personales, y menos aún, módems para conectarse a través de líneas telefónicas. Las grandes *mainframes* y los minicomputadores eran propiedad de universidades, gobiernos o grandes corporaciones, y su acceso estaba reservado a técnicos especializados, lo que limitaba su uso masivo. Pese a ello, se reconocía ya el enorme potencial de los computadores personales para diversificar las aplicaciones en educación, administración, comunicación y entretenimiento.

Desarrollo de los “servicios en línea”: el Videotex

Hasta mediados de la década de 1980 en la mayoría de los países europeos y en Japón las compañías telefónicas nacionales funcionaban como monopolios bajo control estatal. Dichas redes, si bien robustas, permanecían subutilizadas fuera del horario laboral, lo que llevó a considerar los servicios en línea no solo como una estrategia para optimizar su uso, sino también como una herramienta para dinamizar el desarrollo económico nacional y posicionarse estratégicamente en el emergente mercado global de las telecomunicaciones (Elton & Carey, 2013).

En Estados Unidos la situación era similar, aunque con matices. La red pública de telecomunicaciones era controlada casi en su totalidad por Bell System (AT&T), un conglomerado altamente centralizado que ejercía dominio hegemónico sobre el sector. Sin embargo, presionado por el Departamento de Justicia bajo argumentos antimonopólicos, AT&T fue desmantelada en 1984. Esa reestructuración dio origen a una empresa de larga distancia con capacidad para ingresar al negocio de la computación, y a siete compañías regionales (conocidas como *Baby Bells*), encargadas de gestionar las redes telefónicas locales en diferentes regiones del país.

Frente a esta nueva configuración del mercado, tanto los antiguos monopolios como las nuevas compañías percibieron en el Videotex³² una posible fuente

³² El Videotex representó uno de los primeros intentos sistemáticos de integrar telecomunicaciones, televisión y procesamiento de información en un mismo ecosistema interactivo. Su lógica técnica consistía en conectar el receptor televisivo a la red telefónica mediante dispositivos auxiliares que permitían solicitar y recibir información textual en tiempo casi real. Aunque internet aún no existía como red global, la idea de distribuir contenidos digitales a usuarios remotos a través de infraestructuras de telecomunicaciones ya estaba en gestación. En el Reino Unido, a finales de los años sesenta, la BBC exploró sistemas de transmisión de datos que dieron origen a Ceefax (1972), un servicio unidireccional que permitía a los usuarios navegar información transmitida junto con la señal televisiva. ITV desarrollaría un sistema equivalente, ORACLE. Ambos formarían parte de lo que posteriormente se conocería como Teletext. Paralelamente, la General Post Office británica impulsó un modelo distinto, basado en comunicación bidireccional, denominado Viewdata. Dicho sistema

de ingresos alternativos. Ese sistema emergente de servicios interactivos transmitidos a través de redes telefónicas fue visto como una promesa tecnológica, aunque no sin controversia. Diversos actores del sector editorial, en particular los periódicos impresos, expresaron una profunda inquietud ante la posibilidad de que las compañías telefónicas tomaran la delantera en el naciente ecosistema de la información electrónica, y desplazaran así a las editoras tradicionales y alterasen radicalmente su modelo de negocio (Elton & Carey, 2013).

A pesar de las reservas iniciales, algunas compañías editoriales comenzaron a explorar las oportunidades que ofrecía la publicación electrónica. Sin embargo, había importantes desacuerdos sobre cuál debía ser el modelo de servicio más adecuado. ¿Debía concebirse el Videotex como una base de datos adaptada para uso doméstico? ¿Sería el periódico del futuro, o un híbrido que combinara múltiples formatos y funcionalidades? Incluso, se debatía si cada servicio de Videotex debía funcionar de manera autónoma o integrarse en una especie de “centro comercial digital” que reuniera múltiples ofertas bajo una sola plataforma.

Lo cierto es que, para la mayoría de los consumidores, dichas tecnologías eran completamente nuevas. La falta de familiaridad con las terminales interactivas, la baja penetración de computadores personales en los hogares y el escepticismo ante la idea de pagar tarifas elevadas por servicios aún desconocidos representaban barreras significativas para su adopción. Además, los usuarios carecían de hábitos de búsqueda de información o de comunicación electrónica con otras personas, lo que limitaba aún más la viabilidad de estos servicios en su etapa inicial (Dordick, 1985).

Por su parte, las bases de datos en línea tienen sus orígenes en la década de 1960, inicialmente enfocadas en recopilar información científica, técnica y bibliográfica, incluyendo artículos especializados en medicina y ciencias naturales (Williams, 1985). Posteriormente, su contenido se amplió, para abarcar también campos diversos, incluyendo artículos de prensa generalista y documentos de interés público. Aunque dichos sistemas anticipaban en cierta medida lo que hoy conocemos como servicios de información web, tanto su acceso como su presentación eran muy distintos de los actuales. El acceso se hacía mediante terminales conectadas a redes comerciales de conmutación de paquetes como Tymnet o Telenet, lo cual implicaba una infraestructura técnica relativamente compleja.

permitía que el usuario enviara solicitudes a servidores remotos a través de la red telefónica, anticipo de la lógica interactiva que caracterizaría posteriormente a internet. El nombre genérico Videotex terminó agrupando estos servicios, entre ellos Prestel, que constituyó uno de los primeros modelos comerciales de información electrónica en red.

Además, hacia finales de los años setenta las búsquedas de información eran costosas (en torno a los US\$100/hora, sin contar los cargos por comunicación) y requerían habilidades especializadas. Por ello, las consultas eran normalmente realizadas por profesionales capacitados que sabían cómo estructurar las búsquedas para maximizar la eficiencia y reducir costos. Con el tiempo, sin embargo, el desarrollo de interfaces más amigables y la reducción de los costos operativos permitió que usuarios no especializados accedieran a estos recursos de forma más directa y económica.

Para mediados de la década de 1980 el ecosistema digital global ya había experimentado un crecimiento considerable. Existían más de 2.500 bases de datos en funcionamiento, ofrecidas por alrededor de 1.300 organizaciones en todo el mundo, y utilizadas por más de un millón de usuarios pertenecientes a empresas, universidades y gobiernos (Aumente, 1987). En un intento por expandir su alcance, varios operadores de bases de datos empezaron a vincular sus servicios con plataformas de Videotex orientadas al consumidor. La idea era anticiparse a una demanda emergente de información personalizada, como la consulta de artículos periodísticos archivados, cotizaciones bursátiles en tiempo real u horarios de aerolíneas, todos ellos servicios que hoy resultan familiares en el entorno web.

Sin embargo, estos pioneros del acceso digital al conocimiento incurrieron en un error de cálculo económico. Asumieron que si las grandes corporaciones estaban dispuestas a pagar hasta 100 dólares por hora para acceder a información en línea, entonces una tarifa de 12 dólares por hora sería considerada una oferta atractiva para el usuario doméstico. Contrario a estas expectativas, el mercado de consumo mostró escaso interés en pagar esa cantidad, lo que limitó la masificación de dichos servicios en su etapa inicial (Elton & Carey, 2013). A pesar de estas dificultades, las bases de datos en línea sentaron las bases conceptuales y funcionales para los sistemas de información que posteriormente caracterizarían a la Web.

Las primeras conferencias digitales de los ochenta introdujeron herramientas que hoy son parte integral del entorno digital: correo electrónico, foros, mensajería instantánea individual y grupal³³, boletines electrónicos, blogs, canales RSS y documentos compartidos. De manera similar, muchas de las plataformas de educación en línea actuales tienen sus orígenes en servicios de enseñanza a distancia que utilizaban tecnologías de conferencias digitales. Según Vallée (1984), las conferencias digitales surgieron a partir de una iniciativa impulsada por la Oficina de

³³ La terminología era diferente en los primeros días de las conferencias digitales: por ejemplo, el "chat" de hoy se llamaba en su momento "conferencias sincrónicas".

Preparación para Emergencias de los Estados Unidos a finales de los años sesenta. El objetivo era aprovechar el bajo costo de transmisión de las redes de tiempo compartido junto con la capacidad de procesamiento y almacenamiento de los computadores, para facilitar una forma de comunicación interpersonal más sofisticada que el simple correo electrónico.

Entre estas herramientas, el correo electrónico adquirió una popularidad notable. Una de sus características distintivas (y precursoras de dinámicas sociales de la actualidad en la Web) era la posibilidad que brindaban varios sistemas de crear seudónimos, lo cual permitía a los usuarios ocultar su propia identidad o, incluso, desarrollar un alter ego digital (Johansen, 1984). Pese a diversos obstáculos como los elevados costos iniciales, la escasa disponibilidad de terminales y la falta de alfabetización tecnológica, el correo electrónico y otros servicios en línea empezaron a ganar terreno conforme los precios disminuían y los computadores personales se volvieron más asequibles para el público general. Además, servicios como la banca electrónica, si bien en algunos casos formaban parte de los sistemas de Videotex más amplios, también empezaron a operar como soluciones independientes de propiedad privada, y a anticipar así la futura diversificación de servicios digitales en la red global.

Según Elton y Carey (2013), el primer sistema de correo electrónico que utilizó un computador fue MIT Mailbox, desarrollado por Noel Morris y Tom Van Vleck en 1965. Para 1983 ya existían más de 70 proveedores de correo electrónico comercial en América del Norte y Europa³⁴, además de numerosos sistemas internos en uso dentro de empresas y organismos gubernamentales³⁵. Sin embargo, una limitación importante de estos servicios tempranos fue su falta de interoperabilidad. Durante la década de 1980 la mayoría de las plataformas de correo electrónico permanecían aisladas entre sí: los sistemas propietarios no se comunicaban con plataformas de Videotex ni con redes académicas como NSFNET, lo que restringía su utilidad y masificación.

³⁴ Cabría mencionar que, si bien internet se desarrolló por primera vez en Estados Unidos y se hizo popular a nivel global solo después del colapso de la URSS, los soviéticos albergaron durante la Guerra Fría un entramado de "redes ocultas". En efecto, entre las décadas de 1950 y 1980 un pequeño grupo de científicos y administradores soviéticos intentaron desarrollar una red informática nacional diseñada para la comunicación ciudadana. Y si bien la URSS nunca tuvo un internet como se conoce hoy, a principios de la década de 1960 los cibernéticos soviéticos diseñaron el más destacado de los proyectos de red de la URSS, conocido como el "Sistema Automatizado del Estado" (OGAS, por sus siglas en ruso). Su elaborada ambición tecnocrática era establecer redes, almacenar, transmitir, optimizar y administrar los flujos de información que constituirían la economía planificada del Estado, bajo la guía de Politburó soviético y en colaboración con trabajadores, gerentes y planificadores empresariales de todo el país (Peters, 2016).

³⁵ Algunos de los servicios de correo electrónico público más grandes incluyeron *Western Union Easy Link*, *ITT Dialcom*, *MCI Mail* y *Sprint Telemail*.

En paralelo, la banca electrónica surgió como una extensión lógica del proceso de informatización que la industria financiera había experimentado desde los años sesenta. Los primeros ensayos de *home banking* comenzaron hacia finales de los años setenta, tanto en Estados Unidos como en el Reino Unido. Algunas entidades bancarias optaron por integrarse a plataformas de Videotex ya existentes, mientras que otras desarrollaron sistemas propios. No obstante, la escasa penetración de computadores personales en los hogares llevó a experimentar con otras modalidades de acceso. Según Colton y Kraemer (1980), dos alternativas fueron evaluadas: una consistía en utilizar televisores para mostrar la información bancaria transmitida por línea telefónica (una opción que fracasó, debido a preocupaciones de seguridad y privacidad). La otra consistía en desarrollar teléfonos equipados con pequeñas pantallas de cuatro pulgadas, capaces de enviar y recibir datos. Aunque técnicamente viable y fácil de usar, esta segunda opción fue desestimada, por sus altos costos.

Ante estas limitaciones, las instituciones financieras optaron por esperar a que las computadoras personales se consolidaran en los hogares. Solo a partir de mediados de la década de 1990, cuando la adopción de *Personal Computers* (PC) se volvió masiva y los costos disminuyeron, los servicios de banca electrónica empezaron a expandirse significativamente. Aun así, muchas entidades financieras mantuvieron sus reticencias iniciales a ofrecer operaciones transaccionales en la Web, debido a preocupaciones persistentes sobre la seguridad digital. En consecuencia, la mayoría de los primeros sitios web bancarios se limitaron a ofrecer información institucional, sin funcionalidades de consulta de saldos o transferencia de fondos.

Durante los años formativos de los medios en línea las organizaciones sin ánimo de lucro también jugaron un papel clave en el desarrollo de contenidos y servicios de comunicación digital. En efecto, estas organizaciones adquirieron e implementaron una variedad de sistemas, desde *mainframes* y minicomputadores hasta redes de Videotex y tableros de anuncios montados sobre PC, para ofrecer servicios educativos, acceso a registros públicos, información especializada (como salud), recursos para el aprendizaje del uso de computadores y foros comunitarios (Hafner, 2001). Estas experiencias demostraron que los medios digitales podían beneficiar a grupos tradicionalmente excluidos del acceso a la información, y sentaron las bases para el posterior desarrollo de servicios en línea de interés público, como portales de información gubernamentales (por ejemplo, gobiernoenlinea.gov.co en Colombia).

En general, los sistemas de Videotex funcionaban bajo un modelo de acceso restringido: para ofrecer servicios o contenidos, los proveedores debían tener la

autorización explícita del operador del sistema. Un caso emblemático fue el de America Online (AOL). Aunque ingresó tardíamente al mercado del Videotex, AOL logró rápidamente superar a sus competidores, al alcanzar un pico de más de 30 millones de suscriptores a nivel mundial³⁶ (Munk, 2005). AOL operaba bajo un modelo cerrado, en el que controlaba tanto el contenido como los servicios disponibles, y simultáneamente se consolidó como el mayor proveedor de acceso a Internet en Estados Unidos durante los años noventa.

Ese estricto control por parte de los operadores del sistema respondía a diversas preocupaciones. Según Elton y Carey (2013), había tres razones principales para restringir el acceso: 1) evitar la distribución de contenido considerado ofensivo o inapropiado que pudiera alejar a los usuarios; 2) eludir eventuales responsabilidades legales derivadas de posibles difamaciones o errores contenidos en el material de los proveedores, y 3) proteger la reputación institucional de los operadores (especialmente, cuando se trataba de empresas de telecomunicaciones o editoriales) asegurando que el contenido cumpliera ciertos estándares éticos y de calidad. Asimismo, los usuarios estaban obligados a respetar códigos de conducta digital, y en algunos casos eran expulsados de la plataforma por comportamiento inapropiado.

Del Videotex a la Web

Tanto el número de usuarios de internet como el número de sitios en la Web crecieron a tasas asombrosas desde 1995, cuando internet³⁷ se abrió para uso comercial y la comunidad de consumidores y de negocios del Videotex empezó a fusionarse con la comunidad preexistente de internet, que comprendía en su mayor parte a los académicos, estudiantes y otros fuera del mundo corporativo. El

³⁶ A principios de la década de 1990, cuando millones de personas compraron sus primeros computadores, AOL se posicionó como un servicio para neófitos informáticos. Para 1996 la empresa ya contaba con 5 millones de suscriptores en los Estados Unidos, gracias a que su servicio era simple de usar y tenía categorías de contenido que atraían al público en general; además, el énfasis de AOL estaba en la comunicación, y no en la información, proporcionando un servicio de correo electrónico para las masas. Cuando llegó la Web, AOL dudó inicialmente de dejarla a disposición de sus suscriptores, pero pronto abrió las puertas a sitios seleccionados, y posteriormente, a toda la Web. Sin embargo, a mediados de la década de 2000 AOL perdió mucho terreno a medida que los suscriptores migraron a proveedores de servicios de internet de banda ancha.

³⁷ El 24 de octubre de 1995 el Consejo Federal de Redes de los Estados Unidos (en inglés, FNC, por las iniciales de *Federal Networking Council*) aprobó por unanimidad una resolución que definía el término "internet" como el sistema de información global que: 1) está lógicamente vinculado por un espacio de direcciones único globalmente basado en el Protocolo de Internet (IP) o sus extensiones/seguimientos posteriores; 2) puede admitir comunicaciones utilizando el conjunto de protocolos de control de transmisión/protocolo de Internet (TCP/IP) o sus extensiones/ seguimientos posteriores u otros protocolos compatibles con IP, y 3) proporciona, utiliza o deja a disposición, de manera pública o privada, servicios de alto nivel en capas en las comunicaciones y la infraestructura relacionada descrita en este documento.

24 de octubre de 1995 la Federal Networking Council (FNC), de Estados Unidos, aprobó por unanimidad una resolución que definía el término “internet” (Federal Networking Council, 1995):

Internet se entenderá como el sistema de información global que: (i) está lógicamente vinculado por un único espacio global de direcciones basado en el Protocolo de Internet (IP) o sus extensiones/seguimientos posteriores; (ii) puede admitir comunicaciones utilizando el conjunto de protocolos de control de transmisión/protocolo de Internet (TCP/IP) o sus extensiones y/u otros protocolos compatibles con IP; y (iii) proporciona, utiliza o pone a disposición, de manera pública o privada, servicios de alto nivel en capas en las comunicaciones y la infraestructura relacionada descrita en esta resolución.

La fusión progresiva entre los sistemas de Videotex e internet fue facilitada, en gran medida, por la creciente adopción de computadores personales y la expansión del conocimiento técnico entre los usuarios. A medida que más personas adquirirían competencias básicas en el uso de sistemas informáticos, el acceso a la red se volvió cada vez más asequible y atractivo. En este proceso la comunicación digital emergió como el principal motor del uso de internet. La existencia previa de una masa crítica de usuarios ya habituados a interactuar en línea (en particular, a través del correo electrónico) atrajo a nuevos participantes que, al menos en un inicio, se sumaron a la red motivados por el deseo de comunicarse.

Durante los primeros años posteriores a la apertura comercial de internet muchos operadores de servicios Videotex actuaron como puentes de transición: ofrecieron a sus suscriptores acceso a internet, y facilitaron así la migración de un número significativo de usuarios establecidos hacia los nuevos servicios en línea. Este fenómeno no solo incrementó el número de internautas, sino que también aportó valiosas lecciones sobre diseño de servicios digitales y preferencias de los usuarios. La experiencia acumulada con los sistemas de Videotex, así como con otras plataformas en línea de las décadas anteriores, proporcionó una base empírica para entender qué funcionaba y qué no en el mundo digital. Muchas de las aplicaciones web exitosas durante el periodo de transición (desde mediados de la década de 1990 hasta los primeros años del siglo XXI) derivaron directamente de servicios previos que habían demostrado su eficacia, o que al menos ofrecieron indicios sobre las necesidades reales de los usuarios.

Por ejemplo, ya era evidente que diversas formas de comunicación en línea (correo electrónico, foros de discusión, chats individuales y grupales) tendrían un

alto grado de aceptación entre los usuarios de internet. Asimismo, ciertos tipos de contenido informativo, como noticias del clima, resultados deportivos, reportes de actualidad y videojuegos en línea, ya habían probado su atractivo en contextos anteriores. Estas experiencias también mostraron que los consumidores estaban dispuestos a aceptar publicidad digital, siempre y cuando esta contribuyera a reducir el costo de los servicios, lo cual anticipaba uno de los modelos de sostenibilidad económica más influyentes en la era digital.

Una lección crucial surgida de esta evolución fue el reconocimiento de las limitaciones de las primeras bases de datos en línea. Aunque funcionales, estas eran demasiado complejas para el usuario promedio, lo que restringía su utilidad. La aparición de portales web y motores de búsqueda como Yahoo! durante el periodo de popularización de internet simplificó drásticamente el acceso a la información y abrió la puerta a una experiencia de navegación más intuitiva. De igual modo, investigaciones previas ya anticipaban que el comercio electrónico podía prosperar, siempre y cuando se cumplieran ciertos requisitos fundamentales: seguridad en las transacciones, marcas confiables, transparencia en las condiciones de venta, estándares de calidad en la oferta comercial, cumplimiento efectivo de los compromisos adquiridos y políticas claras y favorables de devolución para el consumidor. Estos elementos se convertirían, con el tiempo, en pilares de la economía digital emergente.

Muchos de los errores que obstaculizaron el éxito de las aplicaciones web en los primeros años del siglo XXI ya habían sido cometidos por los servicios en línea previos. Uno de los fallos más frecuentes fue la transposición acrítica de materiales impresos al entorno digital; en otras palabras, numerosas empresas replicaron sus folletos corporativos y piezas de *marketing* en sus páginas web sin hacer ajustes significativos al nuevo medio ni considerar las expectativas específicas de los usuarios en línea. De igual modo, periódicos y revistas provenientes del ecosistema mediático tradicional enfrentaron grandes dificultades para adaptarse a la lógica digital. Inicialmente, muchos medios optaron por publicar en la web el mismo contenido impreso³⁸, con idéntico formato y, en muchos casos, con posterioridad a la circulación de la edición física. Dicha estrategia, que ya había fracasado en

³⁸ Los ingresos por suscripción ocuparon un lugar destacado en los planes de negocios para servicios web durante este periodo de transición. Muchos editores de medios impresos (ignorantes de la historia de los servicios en línea anteriores) creyeron que los nuevos grupos de consumidores que ingresaban a la Web pagarían el contenido a través de suscripciones, de la misma forma como pagaban por los periódicos y revistas impresos. Sin embargo, al igual que los usuarios en línea anteriores, los nuevos usuarios de la Web no estaban dispuestos a hacerlo, con la excepción de algunas empresas que habían pagado por el acceso a bases de datos en línea y ahora pagaban por boletines en línea especializados, razón por la cual muchos periódicos y revistas ofrecerían eventualmente la mayor parte de su contenido en línea sin costo alguno.

el contexto del Videotex, volvió a demostrar su ineficacia durante el periodo de transición hacia la Web. En consecuencia, los medios de comunicación debieron rediseñar radicalmente sus versiones digitales adecuándolas a los hábitos de lectura en línea, a la demanda de actualización constante y al deseo de los usuarios de participar de forma activa mediante comentarios o retroalimentación (Pérez-Montoro, 2018).

En términos técnicos y de experiencia de usuario, los servicios de Videotex eran considerablemente más limitados, en comparación con los estándares actuales de la Web. La velocidad de transmisión era demasiado lenta, debido al uso de módems con capacidades reducidas, lo que se traducía en largos tiempos de espera para acceder a contenidos, especialmente aquellos con elementos gráficos. Muchos usuarios, enfrentados a demoras superiores al minuto o a laberintos de menús consecutivos, abandonaban el servicio por frustración. Además, el modelo de *hardware* del Videotex empezó con el uso de televisores y teléfonos de tonos como interfaces principales, antes de migrar a dispositivos más especializados y computadores personales (Dutton et al., 1986).

En cambio, internet se constituyó en una infraestructura diseñada para la transmisión eficiente y de bajo costo de datos³⁹, incluyendo texto, gráficos y, eventualmente, voz y video en tiempo real. Desde sus orígenes, el acceso a internet se articuló principalmente a través de computadores domésticos, pero con el tiempo se expandió hacia nuevos dispositivos: teléfonos móviles, consolas de videojuegos, tabletas y televisores inteligentes. Un punto de inflexión fue el éxito del servicio *i-mode*, de la compañía japonesa DoCoMo, que a partir de 1999 ofreció acceso móvil a internet para jóvenes japoneses que no tenían PC. Esta experiencia anticipó lo que más tarde se consolidaría como una tendencia global: en muchos países en desarrollo el teléfono móvil se transformó en el principal (y a menudo, en el único) terminal de acceso a la Web evitando completamente el uso de PC.

³⁹ Además, no estaba controlado por una autoridad central cuyo permiso era necesario antes de que los posibles proveedores de información pudiesen ofertar sus servicios en línea.

Tabla 3. Evolución de las redes informáticas

Etapas/ periodo	Nombre/tecnología clave	Características técnicas	Finalidad inicial	Impacto histórico/ ejemplos
Década de 1950	Redes de tiempo compartido (<i>Time Sharing Systems</i>)	Computadores centrales compartidos por múltiples usuarios mediante terminales	Optimizar recursos computacionales caros	Pioneras en universidades y laboratorios militares (MIT, RAND)
1969-1983	ARPANET (Red de la DARPA)	Comunicación de paquetes; enlaces entre nodos	Intercambio científico y comunicación militar descentralizada	Precursor directo de internet; introducción de protocolos como NCP, y luego, TCP/IP
Década de 1970	Redes privadas y Videotex	Redes cerradas o comerciales (X.25); líneas telefónicas; terminales interactivos	Información empresarial; banca; educación; servicios a consumidores	Minitel (Francia), Viewdata (Reino Unido), Videotex (Japón y Estados Unidos)
1983-1995	Internet (NSFNET)	Adopción del protocolo TCP/IP; interconexión global de redes universitarias	Reemplazo de ARPANET para usos civiles y académicos	Expansión del correo electrónico; FTP; Telnet, Gopher
1991-2005	World Wide Web	Documentos de hipertexto (HTTP, HTML); interfaces gráficas; navegadores	Democratización de la información; comunicación global	Mosaic; Netscape; Google; comercialización de la red; auge de portales y buscadores
2005-2015	Web 2.0 y redes sociales	Plataformas colaborativas; servicios en la nube; movilidad	Interacción social; contenido generado por usuarios; personalización algorítmica	Facebook; Twitter; YouTube; Gmail; auge de dispositivos móviles
2015-presente	Redes inteligentes, 5G y computación distribuida	IoT; redes neuronales; <i>Big Data</i> ; <i>edge computing</i>	Automatización; vigilancia; IA; ciberseguridad	Vehículos autónomos; <i>smart cities</i> ; guerra cibernética; redes militares adaptativas

Fuente: elaboración propia.

En retrospectiva, internet ha atravesado transformaciones profundas en sus casi tres décadas de existencia (tabla 3). Nacido durante la era de la computación de tiempo compartido, logró adaptarse a contextos tecnológicos sucesivos: la era de los PC, el modelo cliente-servidor, y más recientemente, la arquitectura basada en redes distribuidas. Aunque fue concebido antes de la generalización de las redes de área local (en inglés, LAN, por las iniciales de *Local Area Network*), internet se integró eficazmente a ellas, y posteriormente, también a tecnologías como ATM (*Asynchronous Transfer Mode*) y Frame Relay. Originalmente diseñado para

soportar una variedad de funciones (desde la transferencia de archivos y el inicio de sesión remota hasta el uso compartido de recursos y la colaboración entre nodos), internet no solo sobrevivió a sus paradigmas fundacionales, sino que los superó ampliamente, hasta convertirse en la plataforma universal que dio origen al correo electrónico, la World Wide Web⁴⁰ y, en última instancia, a la digitalización global de la vida social, política y económica.

Vietnam y la vigilancia computacional

La guerra de Vietnam no solo fue un conflicto militar asimétrico, sino también un laboratorio para la aplicación temprana de sistemas computacionales en tareas de vigilancia, inteligencia y contrainsurgencia. Durante ese periodo emergieron por primera vez modelos cibernéticos aplicados a la guerra irregular y sistemas de bases de datos destinados a gestionar grandes volúmenes de información sobre poblaciones civiles y actores insurgentes. Este fenómeno marcó un punto de inflexión en la evolución de la guerra, donde la capacidad para producir, procesar y aplicar datos se volvió un vector central de dominación militar y control social.

Uno de los primeros sistemas implementados fue el *Hamlet Evaluation System* (HES), desarrollado en 1967 por el Departamento de Defensa de los Estados Unidos. Dicho sistema consistía en una base de datos que recopilaba información demográfica y evaluaciones mensuales de seguridad y desarrollo en aldeas vietnamitas. El objetivo era medir el progreso de las operaciones de pacificación y contrainsurgencia. Sin embargo, el HES enfrentó críticas por su incapacidad para capturar la dinámica compleja del conflicto, como los movimientos de refugiados y la influencia política del Viet Cong. A pesar de las revisiones, las decisiones estratégicas se basaron en resultados altamente agregados, lo que limitó la efectividad del sistema (Feichtinger, 2022).

Uno de los ejemplos más significativos del uso de vigilancia computacional en Vietnam fue el Programa Phoenix, lanzado por la CIA y las Fuerzas Especiales estadounidenses en 1967. Su objetivo era identificar, capturar y neutralizar a miembros del Viet Cong Infrastructure (VCI), la red civil clandestina que sostenía la insurgencia. Para ello, se desarrollaron extensas bases de datos computarizadas

⁴⁰ Internet ya existía antes que la Web. Normalmente, cuando se visita una página web la dirección comienza con *www* (las siglas de *World Wide Web*); como ya se explicó, esta existe desde 1989, cuando Tim Berners-Lee, físico del CERN, presentó su primera propuesta para la Web. En ese orden de ideas, mientras que internet es una inmensa red de computadores conectados entre sí alrededor de todo el mundo, la *World Wide Web* (o la Web) es una enorme colección de páginas que se asienta sobre esa red de computadores, así que cuando se navega a través del celular o el computador se usa internet para acceder a la Web.

que catalogaban información personal, política y social de presuntos colaboradores, activistas y combatientes del VCI. Estas bases de datos alimentaban un sistema de "selección de objetivos" que, en muchos casos, derivaba en detenciones extrajudiciales, tortura o ejecuciones sumarias. Por ende, aunque logró neutralizar a numerosos miembros del Viet Cong, también fue objeto de controversia por las tácticas empleadas y las implicaciones éticas de su enfoque (Valentine, 2000).

Como señala Bass (1992), el corazón del Programa Phoenix era una base de datos nacional operada por computadores IBM en Saigón, llamada el File of Information on the VCI. Esta base reunía más de 300.000 expedientes individuales, con los que se construía un mapa sociopolítico digitalizado del enemigo interno. Cada registro contenía detalles como filiación ideológica, relaciones familiares, afiliaciones comunitarias, ubicación y nivel de implicación. Esa información era luego procesada para identificar patrones, conexiones y jerarquías dentro del aparato insurgente. En esencia, el objetivo era "sistematizar la eliminación" mediante tecnologías de la información. El académico Jeffrey Richelson (2008) destaca que "Phoenix representó la institucionalización de una forma tecnocrática de asesinato político, donde los procedimientos de inteligencia imitaban el funcionamiento de una máquina cibernética de selección y destrucción" (p. 117). Esta lógica funcionalista, heredera de la cibernética de primera generación, concebía el sistema insurgente como una red de nodos disfuncionales que podían ser identificados, aislados y eliminados para degradar el rendimiento del sistema global.

El uso de bases de datos en Vietnam se inscribe en un paradigma más amplio: la aplicación de la cibernética a la guerra. Como ha argumentado Edwards (1996), durante la Guerra Fría el pensamiento cibernético modeló tanto las estrategias de defensa nuclear como las doctrinas de contrainsurgencia. En vez de pensar la guerra como un choque de fuerzas, era concebida como un problema de regulación, *feedback* y control de sistemas complejos. La cibernética de Norbert Wiener, centrada en el control automatizado a través del procesamiento de información, sirvió como marco conceptual para diseñar modelos de "sociedades insurgentes" entendidas como sistemas termodinámicamente inestables que podían ser estabilizados por medio de intervenciones selectivas y disruptivas (Pickering, 2010).

En este sentido, Vietnam representó una "guerra de la información" en la que se intentó controlar no solo el territorio físico, sino también el comportamiento de una población, mediante algoritmos, perfiles y vigilancia permanente. La base técnica de esta vigilancia fue provista por tecnologías computacionales como las tarjetas perforadas de IBM, los sistemas de bases de datos en *mainframes* y los programas de correlación cruzada. Como lo señala Nathan Ensmenger (2010),

dichos sistemas requerían una “nueva clase de expertos: los operadores de sistemas de información, programadores y analistas de inteligencia digital” (p. 185). Así, la guerra moderna incorporaba al informático como un nuevo actor estratégico del campo de batalla.

Más allá del Programa Phoenix, otro experimento pionero de la guerra cibernética fue el proyecto Igloo White, desarrollado entre 1968 y 1973 por el Departamento de Defensa. Dicho sistema se diseñó para interrumpir la red logística del Viet Cong en la Ruta Ho Chi Minh, mediante sensores acústicos y sísmicos desplegados en el terreno, que enviaban señales a computadores ubicados en la base aérea de Nakhon Phanom (Tailandia). Estos datos eran procesados por un sistema computacional central, llamado Intelligence Surveillance and Target Acquisition Radar System (ISTARS), que decidía en tiempo real si debía enviarse una aeronave a bombardear un sector determinado. Aunque innovadora, la operación enfrentó desafíos en la precisión de los datos y la efectividad de las interdicciones (Prados, 2009). De acuerdo con Haigh, “Igloo White marcó la primera vez que se integraron redes de sensores, bases de datos y decisiones algorítmicas en una operación militar continua” (Haigh et al., 2016). El sistema sentó las bases de lo que hoy se denomina “centros de fusión de inteligencia” y prefigura las arquitecturas de vigilancia persistente actuales. Aunque la eficacia militar de Igloo White fue limitada, su relevancia tecnológica fue enorme: introdujo el principio de que las decisiones letales podían ser derivadas desde algoritmos, computadores y sistemas sensores sin intervención humana directa. De algún modo, Vietnam anticipó el modelo de guerra algorítmica que en el siglo XXI se materializa en drones, vigilancia masiva y misiones autónomas.

Los modelos cibernéticos aplicados en Vietnam no se limitaban al frente militar. También se implementaron sistemas de control poblacional. Uno de los más importantes fue el National Police Infrastructure Modernization Program, diseñado por la Agencia de Estados Unidos para el Desarrollo Internacional (en inglés, USAID, por las iniciales de United States Agency for International Development), que informatizó las estaciones de policía en todo el país para facilitar la identificación y seguimiento de opositores. Se instalaron bases de datos con huellas dactilares, antecedentes penales y registros de vigilancia, lo que dio lugar a una arquitectura de control burocrático sin precedentes. Este tipo de vigilancia sistémica derivó en una forma anticipada de vigilancia algorítmica, donde la población era gestionada como una red de nodos informacionales. Como señala James Der Derian, “la contrainsurgencia se convirtió en una ciencia de sistemas de información aplicada al control de poblaciones disidentes” (Der Derian, 2001, p. 172). En esa lógica, el

cuerpo humano se convirtió en una fuente de datos; la comunidad, en un espacio cartografiable, y la vida cotidiana, en una serie de patrones decodificables. Esta transformación antropotécnica de la guerra tuvo efectos devastadores sobre las poblaciones y consolidó una forma de “gubernamentalidad digital militarizada”.

En conclusión, esos sistemas computacionales aplicados durante la guerra de Vietnam inauguraron una forma de poder basada en el procesamiento masivo de información para fines estratégicos. Una lógica que se ha expandido hacia las guerras contemporáneas: desde las operaciones en Afganistán e Irak hasta el uso de IA en conflictos híbridos, vigilancia masiva y campañas de contrainformación. Como sugiere Bernhardt (2016), “los ordenadores nacieron en el campo de batalla y siempre han estado ligados a objetivos estratégicos, aunque los dispositivos hayan cambiado” (p. 89). Por lo tanto, la guerra de Vietnam permitió no solo experimentar con nuevos modelos de control computacional, sino también articular un imaginario militar-cibernético que hoy yace en el centro de la geoestrategia global.

Del C2 al C4ISR: cibernética y doctrina militar digital

Desde mediados del siglo XX el pensamiento militar ha transitado progresivamente desde el enfoque centrado en la estrategia operacional hacia formas cada vez más digitalizadas del control del conflicto. Dicho proceso ha sido impulsado por la convergencia de avances en teoría de sistemas, cibernética y computación, que reconfiguraron la relación entre mando, información y acción militar. Como señala Arquilla (2021), el dominio digital no es simplemente una extensión del campo de batalla, sino una transformación epistemológica de dicho campo, donde “el conflicto se convierte en una lucha por el control de la información y los algoritmos” (p. 88). Este giro se consolidó con la institucionalización de doctrinas como, por ejemplo, el C2 (*Command and Control*) y su evolución hacia C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*), un marco doctrinal que expresa la centralidad de la infraestructura informacional en la planificación y conducción de operaciones militares contemporáneas (Gray, 2004).

El desarrollo de sistemas de comando automatizados se remonta a la Guerra Fría, cuando Estados Unidos y la URSS empezaron a experimentar con la automatización de decisiones en tiempo real mediante redes computacionales. El modelo de C2 buscaba garantizar el flujo continuo de información entre los niveles estratégicos, operacionales y tácticos integrando sensores, plataformas de comunicaciones y centros de mando. Como señala Ensmenger (2010), los primeros intentos de sistemas automáticos en el Pentágono no se limitaron a la logística o la vigilancia, sino que también contemplaron escenarios de uso algorítmico en

la toma de decisiones bajo condiciones de guerra nuclear. A lo largo de los años sesenta y setenta, iniciativas como SAGE (*Semi-Automatic Ground Environment*) y el posterior desarrollo de ARPANET sentaron las bases técnicas y doctrinales para redes descentralizadas de comando. SAGE integraba radares, centros de procesamiento y estaciones de interceptación en un sistema cibernético que podía detectar, procesar y coordinar la respuesta contra amenazas aéreas en tiempo casi real. Campbell-Kelly et al. (2023) subrayan que ese sistema marcó un punto de inflexión en la historia del mando militar, pues demostró que el control automatizado podía ser confiable en contextos de alta presión operativa.

La consolidación doctrinal del C2 y su expansión hacia C4ISR reflejan una apuesta por el uso de arquitecturas digitales para el dominio del campo de batalla. El Departamento de Defensa de Estados Unidos definió tales sistemas como el “corazón neurálgico” de la guerra moderna, por cuanto permiten integrar sensores, plataformas de armas, recursos humanos y procesamiento algorítmico en una sola estructura operativa (Arquilla & Ronfeldt, 1997). Esta instrumentalización tiene un componente epistémico: asume que el conflicto es reducible a flujos de información y que el poder radica en la capacidad para visualizar, procesar y anticipar eventos con base en datos. Bernhardt (2016) lo explica a través del legado de Turing: “la idea de una máquina universal capaz de representar cualquier cálculo también sirvió como metáfora para pensar sistemas militares capaces de representar cualquier teatro de operaciones” (p. 114). Durante la década de 1980 el concepto de “Dominio de la Información” (*Information Dominance*) se volvió céntrico en la planificación militar estadounidense, al dar origen a estructuras como el *Global Command and Control System* (GCCS), que consolidaban distintas capacidades de vigilancia global, comunicaciones seguras y procesamiento de inteligencia en tiempo real. Ensmenger (2010) advierte que esta hegemonía algorítmica del poder militar también se acompañaba de una burocratización tecnocrática del conflicto, donde las guerras se “gestionaban” más que se “combatían”.

Mientras tanto, otros Estados también exploraban los modelos cibernéticos de planificación y control. Uno de los casos más paradigmáticos fue el proyecto chileno *Cybersyn*, impulsado por Stafford Beer, en colaboración con el Gobierno de Salvador Allende. Aunque *Cybersyn* no fue una iniciativa militar *per se*, su arquitectura cibernética buscaba aplicar principios de retroalimentación y control descentralizado a la gestión nacional, incluyendo el manejo de crisis y respuestas rápidas ante amenazas. *Cybersyn* demostró que la cibernética podía ser empleada como una herramienta para la planificación estratégica y la toma de decisiones bajo presión, y de ese modo anticipó muchas de las lógicas que más tarde

adoptaría el C4ISR. Como analiza Eden Medina (2011), *Cybersyn* constituyó “una red informacional que entendía la nación como un sistema adaptativo complejo, gestionado a través de flujos de datos y retroalimentación” (p. 192). En el caso soviético, los sistemas de vigilancia computacional también fueron empleados en estructuras como OGAS (Sistema Nacional Automatizado para la Contabilidad y el Procesamiento de la Información), que pretendían digitalizar toda la economía soviética mediante redes computacionales. Si bien nunca se implementó del todo, el proyecto reflejaba un enfoque integral que entendía la información como recurso estratégico. En los últimos años, Rusia ha retomado visiones cibernéticas aplicadas a la guerra informacional y la desinformación, en lo que Rid (2016) denomina “guerra por no-líneas”, donde el dominio de la narrativa, la información y la percepción reemplaza al control territorial como eje del poder.

El caso de la República Popular de China representa una evolución singular en la relación entre computación y control político. Como documenta Mullaney (2024), el desarrollo de la computación en China no siguió una simple adopción de tecnologías occidentales, sino que implicó una profunda hibridación cultural, lingüística y política. Desde los sistemas de entrada de caracteres hasta la vigilancia estatal algorítmica contemporánea, China ha desarrollado un modelo de información profundamente entrelazado con las estructuras del Partido Comunista. La consolidación del modelo de control total se hace evidente en iniciativas como el Sistema de Crédito Social y el uso extensivo de IA y reconocimiento facial para fines de seguridad nacional. Según Mullaney (2024), “la historia de la computación en China no puede desvincularse del proyecto de gobernanza y disciplinamiento social, donde el código opera como extensión del Estado” (p. 237). En este sentido, el modelo chino representa una forma avanzada de C4ISR aplicado no solo a la guerra, sino al control de la población civil estableciendo nuevas fronteras entre seguridad, vigilancia y política algorítmica.

En resumen, el impacto doctrinal del paso del C2 al C4ISR radica en una mutación del campo de batalla mismo. Como plantea Arquilla (2021), “ya no se trata de ganar en el terreno, sino de dominar la matriz informacional que produce percepción, narrativa y verdad” (p. 102). Este desplazamiento ha dado origen al concepto de campo de batalla informacional (*Information Battlespace*), donde los nodos, redes y algoritmos reemplazan al terreno, las trincheras y los frentes. La cibernética ha jugado un papel clave en esta transición. Wiener (1948) ya había previsto que el control del entorno mediante retroalimentación sería el nuevo principio de organización en la era de la información. Los sistemas actuales de guerra algorítmica, desde drones hasta plataformas de IA, no hacen sino materializar este principio.

La evolución desde el C2 hacia el C4ISR ha sentado las bases doctrinales de la ciberguerra, ya que la capacidad para integrar inteligencia, vigilancia, comunicaciones y procesamiento autónomo en tiempo real permite operar en dominios que van desde el ciberespacio hasta la guerra cognitiva. Como afirma Gray (2004), “el poder militar hoy no se mide por el tonelaje de las armas, sino por la velocidad y precisión de la información procesada” (p. 127). El poder algorítmico constituye la culminación de dicho proceso. Los algoritmos no solo ejecutan códigos, sino que estructuran el campo de posibilidades estratégicas. Desde los modelos predictivos de vigilancia hasta las armas autónomas letales, el control de los algoritmos se ha convertido en un eje de soberanía militar. Adicionalmente, la computación distribuida y las redes de última generación, combinadas con sistemas de C2 y C4ISR en los que se involucran máquinas y humanos en escenarios operaciones, han dado lugar a lo que se conoce “*Internet of Battlefield Things*” (Internet de las Cosas en el Campo de Batalla)⁴¹. En tal sentido, la computación no es una herramienta neutra: es un “lenguaje de poder” que redefine los límites entre guerra, tecnología y gobernanza (Ensmenger, 2010).

Implicaciones estratégicas de la coevolución entre computación, cibernética y guerra

El recorrido histórico y doctrinal que se desarrolló en el apartado anterior permite extraer una serie de implicaciones estratégicas de carácter general. Estas no constituyen conclusiones normativas ni recomendaciones operativas, sino destilaciones conceptuales que ayudan a comprender cómo la coevolución entre computación, cibernética y guerra ha reconfigurado las condiciones estructurales del poder militar contemporáneo.

En primer lugar, la historia de la computación aplicada a los asuntos militares muestra que la tecnología no sustituye a la estrategia, pero sí transforma profundamente el marco dentro del cual esta se formula y ejecuta. Los sistemas técnicos no reemplazan la decisión estratégica humana. Sin embargo, al acelerar

⁴¹ El *Internet of Battlefield Things* (IoBT) constituye una adaptación militar del paradigma del IoT, orientada a la integración operativa de plataformas físicas y sistemas digitales en entornos de combate. A diferencia del IoT civil, cuya finalidad principal es la eficiencia y automatización en contextos comerciales o domésticos, el IoBT articula sensores, plataformas tripuladas y no tripuladas, combatientes, sistemas de armas y nodos de comunicación dentro de una arquitectura de red táctica distribuida. Su lógica no se limita al intercambio de datos, sino que apunta a la construcción de un ecosistema cognitivo de combate, donde la información fluye en tiempo real para alimentar sistemas de mando y control, IA y procesos de decisión automatizados. En este entorno cada elemento del campo de batalla se convierte en un nodo productor y consumidor de datos, que amplía el conocimiento situacional y reduce los ciclos de decisión en operaciones de alta intensidad.

los ciclos decisionales, automatizar procesos de análisis y generar una creciente dependencia de infraestructuras informacionales complejas, alteran las condiciones de mando, planificación y control. En escenarios de alta complejidad, el rol del comandante ya no se define tan solo por su capacidad de concentración de fuerza, sino por su habilidad para operar dentro de entornos informacionales densos, dinámicos y parcialmente automatizados.

En segundo término, el poder militar contemporáneo descansa cada vez más en lo que pueden denominarse infraestructuras epistémicas: sistemas capaces de producir, organizar y explotar conocimiento operacionalmente relevante. En la guerra informacional la ventaja estratégica no proviene tan solo de la superioridad cinética, sino de la capacidad para integrar datos, inteligencia, vigilancia y procesamiento algorítmico en tiempo real. La computación, en este sentido, se convierte en una infraestructura crítica del poder, comparable al territorio, la industria o la logística, y su vulnerabilidad o resiliencia adquiere una dimensión estratégica central.

Asimismo, el legado de la cibernética consolida una comprensión sistémica de los conflictos armados, ya que, al introducir principios de retroalimentación, autorregulación y anticipación, el pensamiento cibernético desplaza la concepción de la guerra como un fenómeno lineal hacia la idea de un sistema adaptativo complejo. En el marco descrito, el objetivo estratégico no se limita de manera exclusiva a la destrucción física del adversario, sino que se orienta crecientemente al control, la influencia y la gestión de dinámicas, comportamientos y percepciones dentro de sistemas interconectados.

Esta coevolución sociotécnica, lejos de producir trayectorias homogéneas, genera asimetrías estratégicas persistentes. La adopción y el empleo de tecnologías computacionales están mediadas por culturas organizacionales, estructuras políticas y tradiciones estratégicas específicas, lo cual explica por qué distintos actores (estatales y no estatales) internalizan de manera disímil las mismas herramientas técnicas. Dichas diferencias producen ventajas y vulnerabilidades estructurales que pueden ser explotadas estratégicamente, incluso por actores con capacidades materiales limitadas.

Finalmente, la convergencia entre computación, cibernética y guerra ha contribuido a una expansión del campo de batalla hacia el dominio informacional y cognitivo. Los datos, los algoritmos y las percepciones se constituyen en objetivos estratégicos en sí mismos, y la disputa por la arquitectura que sostiene la toma de decisiones adquiere una centralidad comparable a la del control del espacio físico. La guerra ya no se libra únicamente sobre territorios, sino también sobre sistemas de información que modelan la voluntad, la comprensión y la acción de los actores en conflicto.

Conclusiones

La cibernética y la computación no solo transformaron las lógicas operativas del conflicto armado, sino que reconfiguraron profundamente las formas de pensar, organizar y ejercer el poder en las sociedades contemporáneas; en efecto, al introducir principios como la retroalimentación, el control automatizado y el procesamiento de información en tiempo real, la cibernética permitió concebir tanto a los sistemas militares y a las instituciones sociales como a estructuras dinámicas, adaptativas e interconectadas. En consecuencia, esta lógica sistémica ha venido desplazando los modelos jerárquicos tradicionales y dado paso a arquitecturas de mando distribuidas, inteligencia descentralizada y vigilancia algorítmica. En el ámbito estratégico, esas transformaciones consolidaron un nuevo tipo de guerra: la "guerra cognitiva", en la que el control del flujo de datos, la anticipación de patrones y la manipulación de percepciones son tan decisivos como el uso de la fuerza física.

En paralelo, el advenimiento de la computación ha impulsado una mutación epistémica que reformula el modo como las sociedades se gobiernan y se protegen. El paso de los archivos físicos a las bases de datos digitales, de la planificación centralizada a la simulación computacional y de la diplomacia estatal al "ciberpoder" revela un proceso en el que la computación se ha vuelto el fundamento de la toma de decisiones públicas y privadas. Estados, empresas y ciudadanos operan cada vez más dentro de infraestructuras informacionales que condicionan sus capacidades de acción, sus márgenes de libertad y sus modos de interacción. Así, la cibernética y la computación no solo dotaron a la guerra de nuevos instrumentos, sino que instauraron una racionalidad técnica que redefine el sentido mismo de la seguridad, la gobernanza y la soberanía en el siglo XXI.

Por consiguiente, la historia de la computación, desde los dispositivos de cálculo manual hasta las arquitecturas digitales contemporáneas, ha sido no solo una narrativa de progreso técnico, sino una profunda transformación del pensamiento estratégico, de las estructuras de poder y del campo de batalla. Como se ha demostrado en el presente capítulo, la coevolución entre computación, cibernética y doctrina militar no es una mera coincidencia, sino el resultado de una larga genealogía en la que las necesidades de la guerra han actuado como catalizador de las más radicales innovaciones tecnológicas. Sin embargo, este proceso histórico parece entrar hoy en una nueva fase, marcada por una disrupción potencialmente mayor que la vivida con la digitalización: la irrupción de la computación cuántica.

La computación cuántica representa un quiebre epistemológico y técnico frente al paradigma clásico de la máquina de Turing. Basada en principios como

la superposición, el entrelazamiento y la interferencia cuántica, esta tecnología propone un modelo de procesamiento radicalmente distinto, con implicaciones profundas para el cálculo, la criptografía, la IA, la logística militar y la simulación de sistemas complejos. Mientras los computadores digitales procesan información en bits, unidades binarias de 0 y 1, los computadores cuánticos utilizan *qubits*, los cuales pueden existir simultáneamente en múltiples estados. Esa capacidad de "paralelismo cuántico" podría permitir la resolución eficiente de problemas que hoy son computacionalmente intratables para supercomputadores más avanzados.

En el ámbito militar, esta disrupción se perfila como una revolución silenciosa. De acuerdo con Kott y Alberts (2021), los avances en computación cuántica podrían alterar profundamente las capacidades de detección, navegación, cifrado, optimización táctica y planeamiento logístico. La posibilidad de romper esquemas criptográficos tradicionales mediante algoritmos cuánticos, como el de Shor, o la de realizar búsquedas ultrarrápidas con el algoritmo de Grover, plantea una amenaza existencial para las comunicaciones seguras en defensa, inteligencia y diplomacia. Según Mosca (2018), incluso si la computación cuántica tarda décadas en materializarse plenamente, los datos interceptados hoy (bajo el principio de *"store now, decrypt later"*) podrían volverse vulnerables en el futuro cercano. En ese contexto, los Estados que primero logren desarrollar o acceder a capacidades cuánticas obtendrán ventajas estratégicas asimétricas sobre sus adversarios. Canadá, Estados Unidos, China, Rusia, la Unión Europea (UE) y, recientemente, la India y Australia han lanzado ambiciosos programas de investigación y despliegue de tecnologías cuánticas con aplicaciones duales (civiles y militares), lo que consolida un nuevo campo de competencia geopolítica. China, por ejemplo, ha desarrollado una red de comunicaciones cuánticas a escala nacional, e incluso lanzó un satélite de comunicaciones cuánticas (Micius), y con ello demuestra que la carrera por la supremacía cuántica es también una carrera por el poder internacional. Como advierte Bousquet (2021), el campo de batalla del futuro no será simplemente informatizado, sino cuánticamente modulado.

Para países como Colombia el advenimiento de esta revolución tecnológica presenta al menos tres tipos de desafíos estratégicos. El primero es el de la vulnerabilidad estructural. Como nación todavía en transición digital, Colombia no posee hoy las capacidades científicas, industriales o tecnológicas suficientes para generar desarrollos propios en computación cuántica, lo que la deja en una posición de alta dependencia frente a actores externos. Esta brecha tecnológica podría traducirse en una brecha de poder en escenarios de conflicto o disuasión, donde

proteger infraestructuras críticas (redes de mando y control, comunicaciones, sistemas de navegación satelital, vigilancia estratégica) dependa de su resistencia frente a adversarios con capacidades cuánticas ofensivas.

El segundo desafío es el de la obsolescencia doctrinal. La transformación profunda que implican las tecnologías cuánticas no puede ser enfrentada tan solo desde la adquisición tecnológica, sino que exige una revisión a fondo de los marcos doctrinales y estratégicos de la defensa nacional. Los conceptos tradicionales de ciberseguridad, inteligencia técnica, superioridad informacional y comando y control deben adaptarse a un entorno en el que la incertidumbre cuántica, la aleatoriedad programable y la superposición operativa reconfiguran las lógicas del enfrentamiento. Si la revolución digital exigió pasar del paradigma mecanicista al paradigma informacional, la revolución cuántica exigirá transitar hacia un paradigma probabilístico y emergente.

El tercer desafío es el de la gobernanza internacional. Colombia, como Estado comprometido con el derecho internacional y el uso responsable de las tecnologías emergentes, deberá posicionarse diplomáticamente en los foros multilaterales donde se discutan los usos legítimos de la computación cuántica, los marcos normativos para su control y la prevención de carreras armamentistas cuánticas. Como señala Kania (2019), aún no existe un régimen de gobernanza global claro para estas tecnologías, lo cual abre un margen de acción para que países medianos propongan reglas, estándares y mecanismos de confianza que garanticen la seguridad compartida. La inserción activa de Colombia en estas discusiones es crucial para evitar quedar marginada de los futuros regímenes internacionales de tecnología estratégica.

Frente a estos desafíos, se propone una serie de recomendaciones a la comunidad de defensa y seguridad de Colombia:

1. Anticipación estratégica e inversión en vigilancia tecnológica. Es imperativo crear un Observatorio Nacional de Tecnologías Cuánticas que actúe como centro de alerta temprana, análisis prospectivo y asesoramiento estratégico en ciencia disruptiva para la seguridad y la defensa. Dicho observatorio debería integrarse a la estructura de planeamiento del Ministerio de Defensa y contar con participación de las universidades, el sector privado y las Fuerzas Armadas.
2. Formación y educación avanzada en tecnologías cuánticas. La Fuerza Aeroespacial Colombiana, la Escuela Superior de Guerra (ESDEG) y las academias militares deben incorporar en sus programas de formación

contenidos sobre computación cuántica, criptografía poscuántica, algoritmos cuánticos e implicaciones estratégicas de dichas tecnologías. Se recomienda establecer convenios para capacitación del talento nacional y transferencia de conocimiento con universidades internacionales líderes (como MIT, Caltech, Tsinghua o ETH Zürich), centros latinoamericanos como el INPE (Brasil) y universidades colombianas que ya tienen computadores cuánticos y grupos de investigación con interés en tecnologías cuánticas (por ejemplo, la Universidad de los Andes).

3. Cooperación internacional para transferencia tecnológica y desarrollo conjunto. Colombia debe fortalecer sus alianzas tecnocientíficas con socios estratégicos (como Estados Unidos, la UE, Corea del Sur e Israel), para acceder a proyectos de investigación colaborativa en tecnologías cuánticas con fines duales. En particular, el Comando Sur de Estados Unidos y la Organización del Tratado del Atlántico Norte (OTAN) ofrecen esquemas de cooperación en innovación en defensa que podrían incluir dimensiones cuánticas si Colombia demuestra capacidades de absorción tecnológica.
4. Seguridad poscuántica y resiliencia criptográfica. A nivel de ciberdefensa, debe iniciarse de inmediato un proceso de evaluación de los sistemas criptográficos actualmente en uso en la infraestructura militar, de inteligencia y gubernamental. Esta evaluación debe identificar posibles vulnerabilidades frente a ataques cuánticos futuros e iniciar una transición progresiva hacia sistemas de criptografía poscuántica, como los propuestos por el National Institute of Standards and Technology (NIST).
5. Inclusión del tema cuántico en doctrina y planeamiento militar. Las capacidades cuánticas deben integrarse en el pensamiento doctrinal de la defensa nacional. El Comando Conjunto Cibernético, el Comando Espacial y el Estado Mayor Conjunto deberían contemplar escenarios de guerra cuántica dentro de sus ejercicios de planeamiento, simulación y guerra de *wargaming*, incluyendo dimensiones como la negación de comunicaciones seguras, la manipulación de sensores satelitales y la optimización logística cuántica.
6. Desarrollo nacional de capacidades en simulación cuántica para defensa. Aunque el *hardware* cuántico de altas capacidades aún está en fase experimental, Colombia podría comenzar a desarrollar capacidades en simulación cuántica aprovechando plataformas como IBM Q Experience o Google Quantum AI. Estas herramientas permiten modelar materiales,

moléculas y escenarios físicos complejos relevantes para la defensa, como nuevos materiales resistentes, algoritmos de optimización táctica o comportamientos emergentes en conflictos asimétricos.

En suma, la computación cuántica no es tan solo una tecnología del futuro, sino una dimensión emergente del poder estratégico global. Así como la Segunda Guerra Mundial afianzó el rol de la computación digital en los asuntos militares, el siglo XXI será testigo de una nueva reconfiguración del poder, basada en la aplicación de los conceptos de la mecánica cuántica en diferentes tecnologías y dominios de aplicación. En dicho escenario Colombia no puede limitarse a ser un consumidor pasivo de tecnología, sino que debe posicionarse como un actor estratégico inteligente, capaz de anticipar, adaptarse y participar de manera activa en la configuración de las reglas del nuevo orden tecnológico-militar. El desafío es inmenso, pero también lo es la oportunidad de construir una defensa nacional que no solo proteja el presente, sino que también se proyecte soberanamente hacia los campos de batalla del mañana.

Referencias

- Adams, P. y Warf, B. (1997). Introduction: Cyberspace and Geographical Space. *Geographical Review*, 87(2), 139-145.
- Adamson, D. (1994). *Blaise Pascal: Mathematician, Physicist and Thinker about God*. Palgrave Macmillan.
- Álvarez, C.; Santafé, G. y Urbano, O. (2017). 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.; Murillo, S.; Hernández, J. y Urbina, J. (2019a). El Poder Espacial y la Seguridad Multidimensional, en Álvarez, C. y Corredor, C. (Eds), *El Espacio Exterior: Una Oportunidad Infinita para Colombia, Volumen 1, Mirando Hacia las Estrellas: Una Constante Necesidad Humana* (pp. 21-85). Sello Editorial ESDEG.
- Álvarez, C., Benavides, E. y Ramírez, Y. (2019b). Geopolítica del Espacio Exterior: Dominio Estratégico del Siglo XXI para la Seguridad y Defensa, en Alvarez, C. y Corredor, C. (Eds), *El Espacio Exterior: Una Oportunidad Infinita para Colombia, Volumen 1, Mirando Hacia las Estrellas: Una Constante Necesidad Humana* (pp. 85-194). Sello Editorial ESDEG.
- Ampère, A. (1843). *Essai Sur La Philosophie Des Sciences*. Bachelier.
- Arquilla, J. (2021). *Bitskrieg: The New Challenge of Cyberwarfare*. Polity Press.
- Arquilla, J. y Ronfeldt, D. (1997). In *Athena's Camp: Preparing for Conflict in the Information Age*. RAND Corporation.
- Aumente, J. (1987). *New Electronic Pathways: Videotex, Teletext and Online Databases*. Sage Publications.
- Bamford, J. (2001). *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. Anchor Books.
- Bass, T. (1992). *The Eudaemonic Pie*. Vintage.
- Beer, S. (1995a). *Decision and Control: The Meaning of Operational Research and Management Cybernetics*. Wiley.
- Beer, S. (1995b). *Brain of the Firm*. Wiley.
- Berlinghoff, W. y Gouvea, F. (2019). *Math Through the Ages: A Gentle History for Teachers and Others*. Dover Publications.
- Bernhardt, C. (2016). *Turing's Vision: The Birth of Computer Science*. MIT Press.
- Bertalanffy, L. von. (1968). *General System Theory: Foundations, Development, Applications*. George Braziller.
- Bousquet, A. (2021). *The Eye of War: Military Perception from the Telescope to the Drone*. University of Minnesota Press.
- Bowker, G. (1993). How to be universal: Some cybernetic strategies, 1943-70. *Social Studies of Science*, 23(1), 107-127.

- Boyer, C. (1949). *The History of the Calculus and its Conceptual Development*. Dover Publications.
- Campbell-Kelly, M. (2003). *From Airline Reservations to Sonic the Hedgehog: A History of the Software Industry*. MIT Press.
- Campbell-Kelly, M.; Aspray, W.; Yost, J.; Tinn, H. y Díaz, G. (2023). *Computer: A History of the Information Machine (4th ed.)*. Routledge.
- Christianson, G. (2005). *Isaac Newton*. Oxford University Press.
- Cifuentes, C. (2021a). *Cybernetic Architectures: Informational Thinking and Digital Design*. Routledge.
- Cifuentes, L. (2021b). La cibernética como modelo epistemológico: Norbert Wiener y el pensamiento estratégico. *Revista Colombiana de Filosofía de la Ciencia*, 21(2), 45-67.
- Colton, K. y Kraemer, K. (1980). *Computers and Banking: Electronic Funds Transfer Systems and Public Policy*. Springer.
- Cooper, S. y van Leeuwen, J. (Eds.). (2013). *Alan Turing: His Work and Impact*. Elsevier.
- Copeland, J. (2006). *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*. Oxford University Press.
- Davis, M. (2018). *The Universal Computer: The Road from Leibniz to Turing*. CRC Press.
- Der Derian, J. (2001). *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*. Westview Press.
- Dooley, J. (2013). *A Brief History of Cryptology and Cryptographic Algorithms*. Springer.
- Dordick, H. (1985). The Search for the Electronic Publishing Business. En Greenberger, M. (Ed.), *Electronic Publishing Plus* (pp. 205-217). Knowledge Industries Publications.
- Dutton, W.; Blumer, J. y Kraemer, K. (1986). *Wired Cities: Shaping the Future of Communications*. G.K. Hall & Company.
- Edwards, P. (1996). *The Closed World: Computers and the Politics of Discourse in Cold War America*. MIT Press.
- Elton, M. y Carey, J. (2013). The Prehistory of the Internet and Its Traces in the Present: Implications for Defining the Field. En Dutton, W. (Ed.), *Oxford Handbook of Internet Studies* (pp. 123-187). Oxford University Press.
- Ensmenger, N. (2010). *The Computer Boys Take Over: Computers, Programmers, and the Politics of Technical Expertise*. MIT Press.
- Federal Networking Council (1995). *FNC Resolution: Definition of "Internet"*. Obtenido de: https://www.nitrd.gov/fnc/internet_res.pdf
- Feichtinger, M. (2022). Computing Counterinsurgency: The Hamlet Evaluation System (HES) in the American War in Vietnam. *IEEE Annals of the History of Computing*, 44(1), 1-16.
- Foerster, H. von. (2003). *Understanding Ensminger: Essays on Cybernetics and Cognition*. Springer.
- Gertner, J. (2012). *The Idea Factory: Bell Labs and the Great Age of American Innovation*. The Penguin Press.

- Gleick, J. (2011). *The Information: A history, a theory, a flood*. Pantheon Books.
- Gray, C. (2004). *Peace, War and Computers*. Routledge.
- Hafner, K. y Lyon, M. (1998). *Where Wizards Stay Up Late: The Origins of the Internet*. Simon & Schuster.
- Hafner, K. (2001). *The WELL: A Story of Love, Death and Real Life in the Seminal Online Community*. Carroll & Graf Publishers.
- Haigh, T.; Priestley, M. y Rope, C. (2016). *ENIAC in Action: Making and Remaking the Modern Computer*. MIT Press.
- Hiltz, S. y Turoff, M. (1993). *The Network Nation: Human Communication via Computer*. The MIT Press.
- Hodges, A. (2014). *Alan Turing: The Enigma*. Princeton University Press.
- Ifrah, G. (2000). *The Universal History of Numbers: from Prehistory to the Invention of the Computer*. John Wiley & Sons.
- Ifrah, G. (2001). *The Universal History of Computing: from the Abacus to the Quantum Computer*. John Wiley & Sons.
- Johansen, R. (1984). *Teleconferencing and Beyond: Communication in the Office of the Future*. McGraw-Hill.
- Kania, E. (2019). *Securing Our Future: The Role of National Security in Quantum Technology Development*. Center for a New American Security.
- Kott, A. y Alberts, D. (2021). Quantum Computing for Military Cyber Operations: Threats and Opportunities. *Journal of Cybersecurity and Information Systems*, 9(2), 13-22.
- Le Rond d'Alembert, J. (1967). *Traite de Dynamique*. Culture et Civilisation.
- Lyon, D. (2003). *Surveillance after September 11*. Polity Press.
- Martin, E. y Carey, J. (2013). The Prehistory of the Internet and its Traces in the Present: Implications for Defining the Field. En Dutton, W. (Ed.), *The Oxford Handbook of Internet Studies* (pp. 123-187). Oxford University Press.
- Medina, E. (2011). *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*. MIT Press.
- Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38-41.
- Mullaney, T. (2024). *The Chinese Computer: A Global History of the Information Age*. MIT Press.
- Munk, N. (2005). *Fools Rush In: Steve Case, Jerry Levin, and the Unmaking of AOL Time Warner*. Harper Paperbacks.
- Nahin, P. (2012). *The Logician and the Engineer: How George Boole and Claude Shannon Created the Information Age*. Princeton University Press.
- Ning, H. (2022). *A Brief History of Cyberspace*. CRC Press.
- O'Regan, G. (2012). *A Brief History of Computing (2nd ed.)*. Springer.

- O'Regan, G. (2016). *Introduction to the History of Computing: A Computing History Primer*. Springer.
- O'Reilly, O. (2008). *Intermediate Dynamics for Engineers: A Unified Treatment of Newton-Euler and Lagrangian Mechanics*. Cambridge University Press.
- Pérez-Montoro, M. (2018). *Interaction in Digital News Media: From Principles to Practice*. Springer International Publishing.
- Peters, B. (2016). *How Not to Network a Nation: The Uneasy History of the Soviet Internet*. MIT Press.
- Pickering, A. (2010). *The Cybernetic Brain: Sketches of Another Future*. University of Chicago Press.
- Prados, J. (2009). *Vietnam: The History of an Unwinnable War, 1945-1975*. University Press of Kansas.
- Richelson, J. (2008). *The U.S. Intelligence Community (6th ed.)*. Westview Press.
- Rid, T. (2016). *Rise of the Machines: A Cybernetic History*. WW Norton & Co.
- Robič, B. (2020). *The Foundations of Computability Theory*. Springer-Verlag.
- Rosenblueth, A.; Wiener, N. y Bigelow, J. (1943). Behavior, Purpose and Teleology. *Philosophy of Science*, 10(1), 18-24.
- Rossi, C. y Russo, F. (2017). *Ancient Engineers Inventions: Precursors of the Present*. Springer.
- Shannon, C. (1948). *A Mathematical Theory of Communication*. Bell System Technical Journal.
- Shannon, C. (1949). *Communication Theory of Secrecy Systems*. Bell System Technical Journal.
- Soni, J. y Goodman, R. (2017). *A Mind at Play: How Claude Shannon Invented the Information Age*. Simon & Schuster.
- Swedin, E. y Ferro, D. (2007). *Computers: The Life Story of a Technology*. Johns Hopkins University Press.
- Swedin, E. y Ferro, D. (2022). *The Computer: A Brief History of the Machine That Changed the World*. Greenwood Publishing Group.
- Turing, J. (2022). *The Enigma Story: The Truth Behind the 'Unbreakable' World War II Cipher*. Sirius Publishing.
- Valentine, D. (2000). *The Phoenix Program*. Open Road Media.
- Vallée, J. (1984). *Computer Message Systems*. McGraw Hill.
- Wiener, N. (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine*. MIT Press.
- Wiener, N. (1954). *The Human Use of Human Beings*. Houghton Mifflin.
- Wiener, N. (1963). *God and Golem Inc.* MIT Press.
- Williams, M. (1985). Electronic Databases. *Science*, 299(4), 450-455.

Capítulo 2

Mapeando el ciberespacio: cartografías de poder y soberanía digital en el siglo XXI*

DOI: <https://doi.org/10.25062/9786287818705.02>

Carlos Enrique Álvarez Calderón

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo analiza las estructuras físicas, geográficas y políticas que hacen posible el funcionamiento del ciberespacio, así como los vínculos entre infraestructura, gobernanza y poder en el entorno digital contemporáneo. A través de un enfoque interdisciplinario se estudian las arquitecturas técnicas de internet y la cartografía material de cables submarinos, satélites, centros de datos y espectros electromagnéticos, así como los marcos regulatorios e intereses geopolíticos que configuran la soberanía digital. El texto examina modelos internacionales (Estados Unidos, China y Europa) y plantea una reflexión crítica sobre los desafíos que enfrenta América Latina, y en particular Colombia, ante su creciente dependencia tecnológica. Se concluye que el ciberespacio no es un entorno neutro, sino un campo disputado de poder donde la infraestructura y las normas se convierten en instrumentos estratégicos. Finalmente, se ofrecen recomendaciones para fortalecer la resiliencia digital, la autonomía informacional y la seguridad cibernética en el contexto colombiano.

Palabras clave: ciberespacio; geopolítica; redes; soberanía digital; seguridad 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

Citación APA: Álvarez Calderón, C. E. (2026). Mapeando el ciberespacio: cartografías de poder y soberanía digital en el siglo XXI. 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. 79-176). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818705.02>

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

En los últimos treinta años el ciberespacio ha emergido como una dimensión estructural de la realidad contemporánea, imbricada en las dinámicas sociales, políticas, económicas y militares del siglo XXI. Lo que en sus orígenes fue concebido como un experimento de interconexión científica entre computadores ha devenido en una infraestructura crítica, global y omnipresente, cuyas ramificaciones se extienden desde el comercio internacional hasta la disuasión estratégica. En este contexto, resulta indispensable analizar al ciberespacio no como una simple red virtual o un espacio inmaterial de interacción digital, sino como una construcción geotécnica y geopolítica compuesta por capas físicas, lógicas y simbólicas que sostienen y configuran la vida digital moderna.

La pregunta orientadora que articula este capítulo es: ¿qué estructuras físicas, geográficas y políticas hacen posible el funcionamiento del ciberespacio, y cómo se configuran los vínculos entre infraestructura, gobernanza y poder en el entorno digital contemporáneo? A partir de esa interrogante se plantea una aproximación multiescalar e interdisciplinaria que integra análisis geográficos, tecnológicos y políticos, a fin de comprender las condiciones materiales y las lógicas de control que permiten la existencia y operación del ciberespacio.

Esta aproximación parte del reconocimiento de que el ciberespacio no flota en una “nube etérea”, sino, por el contrario, se sustenta en una arquitectura física densa y compleja. Desde cables submarinos y centros de datos hasta satélites de comunicaciones y espectros electromagnéticos, la infraestructura digital está anclada en lugares específicos, responde a decisiones políticas y es atravesada por conflictos geoestratégicos. El tránsito de paquetes de datos que posibilita el acceso a una página web, la transmisión de una videollamada o el funcionamiento de un dron militar dependen de la estabilidad y resiliencia de dicha infraestructura. Así,

se vuelve urgente mapear el ciberespacio como un territorio híbrido, donde se superponen lo digital y lo geográfico, lo material y lo simbólico, lo técnico y lo político.

En este punto, resulta necesario precisar el sentido en el que el presente capítulo utiliza el concepto de “cartografía”. En su acepción clásica, la cartografía ha sido entendida como una práctica descriptiva orientada a representar de manera objetiva un territorio preexistente delimitando espacios, fronteras y relaciones espaciales con pretensiones de neutralidad técnica. Desde esa perspectiva, el mapa aparece como un instrumento de conocimiento pasivo, cuya función principal es reflejar una realidad espacial dada. Sin embargo, desde los enfoques contemporáneos de la geopolítica crítica la cartografía no se limita a describir el espacio, sino que participa activamente en su producción política.

Por consiguiente, la cartografía “performativa” no solo representa territorios, sino que los construye, al definir qué cuenta como espacio relevante, dónde se trazan los límites, qué actores son visibles y qué relaciones de poder quedan naturalizadas. En este sentido, mapear es un acto político que configura imaginarios, habilita decisiones estratégicas y legitima formas específicas de control y soberanía. Aplicada al ciberespacio, esta distinción resulta decisiva. Lejos de ser un dominio puramente técnico o neutral, el ciberespacio es continuamente cartografiado mediante discursos, infraestructuras, marcos normativos y arquitecturas digitales que “performan” fronteras, jerarquías y zonas de control. Así, las cartografías del ciberespacio (ya sean estatales, corporativas o transnacionales) no solo describen redes y flujos de información, sino que producen espacialidades digitales alineadas con proyectos específicos de poder y seguridad.

El capítulo se estructura en cuatro secciones interdependientes que abordan distintos niveles de análisis. En primer lugar, se hace una genealogía conceptual de internet, la Web, las redes y el ciberespacio, distinguiendo sus componentes estructurales y su evolución histórica. A través del examen de metáforas fundacionales como la “autopista de la información” o el “ciberespacio” como frontera, se revela de qué modo las concepciones culturales han influido en la forma como se ha imaginado y construido el entorno digital. Asimismo, se expone cómo la estructura de protocolos (TCP/IP), el sistema de nombres de dominio (DNS), y la segmentación lógica de la red constituyen formas de arquitectura política y técnica que configuran el ejercicio del poder en línea.

La segunda sección se adentra en la dimensión geográfica y material del ciberespacio. A partir de una revisión crítica de la literatura sobre infraestructura digital se analiza el papel estratégico de los cables submarinos, los centros de datos, las estaciones de aterrizaje, los satélites de comunicación y el espectro electromagnético como componentes clave del ecosistema cibernético. El objetivo de esta

sección es demostrar que el acceso y la soberanía sobre dichas infraestructuras no es neutro ni universal, sino desigual, jerárquico y profundamente conflictivo. Se argumenta que estos nodos materiales forman una cartografía oculta, pero determinante, del poder digital global.

En la tercera sección se examinan los conflictos actuales en torno al control del ciberespacio, así como las tensiones emergentes entre actores estatales, corporativos y multilaterales. A partir del estudio de modelos de soberanía digital (como el chino, el europeo, el estadounidense y los incipientes intentos latinoamericanos) se problematiza la gobernanza de internet como un campo de disputa normativa, económica y militar. La lógica de "soberanía de datos" y las estrategias de localización de información, bloqueo territorial, control del tráfico y segmentación de infraestructura revelan la emergencia de una nueva gramática de poder en el ciberespacio, donde la defensa digital, la autonomía tecnológica y la resiliencia informática se vuelven factores centrales de la seguridad nacional.

Finalmente, en la cuarta sección se sintetizan los hallazgos más relevantes del capítulo y se hacen recomendaciones para la comunidad académica, gubernamental y militar en Colombia. Se subraya la necesidad de adoptar un enfoque integral sobre el ciberespacio que combine capacidades técnicas, criterios geopolíticos y marcos normativos actualizados. Asimismo, se hace un llamado a superar la dependencia tecnológica de proveedores extranjeros, fortalecer la infraestructura crítica nacional y articular políticas de ciberseguridad con estrategias de desarrollo científico, autonomía digital y soberanía informacional.

En conjunto, este capítulo propone una cartografía crítica del ciberespacio, entendida como una forma de pensamiento estratégico y analítico que permite comprender no solo cómo funciona el mundo digital, sino también quién lo controla, con qué fines y bajo qué lógicas de poder. Lejos de reducirse a un espacio de innovación o conectividad, el ciberespacio aparece como una nueva dimensión geopolítica, cuyas infraestructuras, normas y flujos constituyen el nuevo territorio sobre el cual se disputa la soberanía en el siglo XXI.

Arquitecturas del mundo digital: comprendiendo internet, la Web, las redes y el ciberespacio

En la era de digitalización ubicua es clave delimitar con precisión los conceptos que estructuran el ecosistema informacional contemporáneo. Si bien términos como "internet", "redes", "World Wide Web" y "ciberespacio" son frecuentemente

utilizados de manera indistinta tanto en el discurso público como en documentos técnicos y normativos, cada uno de ellos designa niveles distintos de infraestructura, funcionalidad y abstracción dentro del entorno digital global. Esta diferenciación no solo es relevante desde el punto de vista terminológico, sino que tiene implicaciones estratégicas para la seguridad cibernética, la gobernanza digital y la formulación de políticas públicas orientadas a la soberanía tecnológica.

Comprender las interrelaciones y distinciones entre estos conceptos permite identificar con mayor claridad los vectores de vulnerabilidad, los espacios de disputa y los nodos críticos dentro de la arquitectura informacional. Mientras “internet” constituye la base física y lógica de interconexión global, las “redes” describen estructuras funcionales que articulan dispositivos a diferentes escalas. La “Web” representa la interfaz hipermedial de acceso a la información digital. Y el “cibespacio”, en su acepción más amplia, designa el entorno estratégico, simbólico y político donde se configuran interacciones, se construyen narrativas y se ejercen formas emergentes de poder.

Taxonomía del mundo digital: internet, la Web, redes y ciberespacio

Internet no surgió como producto comercial ni como una invención aislada, sino como el resultado de una convergencia entre investigación científica, necesidades estratégicas de defensa y una visión sociotécnica de interconexión global. A comienzos de la década de 1960, en el contexto de la Guerra Fría, el Departamento de Defensa de los Estados Unidos creó la Advanced Research Projects Agency (ARPA), con el propósito de financiar investigación avanzada que garantizara superioridad tecnológica frente a la Unión Soviética (URSS). Dentro de ARPA se estableció una oficina dedicada a la investigación informática. Fue allí donde J. C. R. Licklider, psicólogo e informático del Massachusetts Institute of Technology (MIT), formuló en 1962 la idea de una “red galáctica”: es decir, un sistema global de computadores interconectados que permitiría a los usuarios acceder a datos y programas desde cualquier lugar (Leiner et al., 1997).

Para comprender la radicalidad de esta idea cabe recordar que en esa época los computadores eran máquinas aisladas, extremadamente costosas y utilizadas bajo esquemas de tiempo compartido. Licklider imaginó algo por completo distinto: una red distribuida de máquinas que permitiría colaboración remota, intercambio de información y acceso descentralizado al conocimiento. Esa intuición era no solo técnica: además, era estructural. Anticipaba un sistema de circulación de información que superaba el modelo jerárquico de control centralizado.

Sin embargo, una visión sin arquitectura no basta. La pregunta crítica era cómo conectar físicamente múltiples computadores dispersos geográficamente. En ese punto entró en escena la conmutación de paquetes. Hasta entonces las comunicaciones a distancia se basaban en la conmutación de circuitos, el modelo telefónico tradicional en el que cuando dos puntos se conectaban se establecía un canal dedicado y continuo entre ellos durante todo el proceso de la comunicación. Ese sistema era eficiente para voz, pero en extremo rígido y vulnerable.

De manera casi simultánea, otros tres equipos de investigación desarrollaron una alternativa. Leonard Kleinrock (MIT, y luego University of California, en Los Ángeles [UCLA]) formuló la base matemática de la teoría de colas aplicada a redes. Paul Baran (RAND Corporation) diseñó modelos de redes distribuidas resistentes a ataques. Y Donald Davies (National Physical Laboratory [NPL], del Reino Unido) acuñó el término "paquete". La innovación consistía en fragmentar la información en pequeñas unidades independientes (paquetes) que podían viajar por rutas distintas dentro de la red y recomponerse al llegar a destino. Si una parte de la red fallaba, los paquetes podían redirigirse por otro camino. En términos técnicos, eso implicaba mayor eficiencia en el uso del ancho de banda. En términos estratégicos, implicaba resiliencia estructural: una red no dependía de un único punto de control ni de un canal fijo (Leiner et al., 1997).

Sobre esta base conceptual, ARPA financió el desarrollo de ARPANET en 1967. En septiembre de 1969 se instaló el primer *Interface Message Processor* (IMP) en UCLA. Poco después se conectaron el Stanford Research Institute (SRI), la Universidad de California en Santa Bárbara (UCSB) y la Universidad de Utah. Estos cuatro nodos iniciales constituyeron la primera red operativa de conmutación de paquetes. Es importante subrayar que ARPANET no fue un simple experimento técnico de transmisión de datos. Desde su concepción integró dos dimensiones inseparables: por un lado, una infraestructura de transporte diseñada para interconectar computadores distribuidos; por otro, un conjunto de aplicaciones orientadas al uso humano que otorgaban sentido práctico a esa conectividad. La red no se pensó tan solo como un sistema de cables y nodos, sino como un entorno funcional donde la comunicación, el intercambio de información y la colaboración entre usuarios serían el verdadero propósito de la arquitectura técnica.

Durante los primeros años de funcionamiento de ARPANET se desarrolló el *Network Control Protocol* (NCP), el cual permitió establecer comunicación directa entre los llamados *hosts*, es decir, los computadores finales conectados a la red. Este protocolo constituyó el primer mecanismo operativo que hizo posible el

intercambio efectivo de datos entre instituciones académicas y centros de investigación. En 1972 emergió una aplicación que transformaría profundamente la lógica del sistema: el correo electrónico. Inicialmente concebido como una herramienta práctica de coordinación entre investigadores, el *e-mail* se convirtió con rapidez en la aplicación dominante. El volumen de tráfico “persona a persona” comenzó a superar al tráfico estrictamente computacional, hasta alterar el sentido mismo de la red. Este cambio no fue menor, ya que ARPANET dejó de ser un mecanismo destinado principalmente a compartir recursos informáticos costosos y se volvió, de forma progresiva, una infraestructura para compartir comunicación humana. La red empezó a organizar comunidades antes que máquinas. Con ello, la dimensión social de la conectividad empezó a adquirir un peso estructural.

Sin embargo, el salto verdaderamente decisivo fue conceptual. Pronto se comprendió que ARPANET no debía permanecer como una red aislada, sino que debía convertirse en el punto de partida de un sistema más amplio. La cuestión estratégica dejó de ser cómo interconectar computadores dentro de una misma red, y pasó a ser cómo interconectar múltiples redes entre sí, aun cuando estas fueran técnicamente distintas. Este cambio de enfoque implicaba abandonar la idea de una red única y centralizada para adoptar la visión de un entorno compuesto por redes autónomas, pero interoperables.

En ese contexto, Robert Kahn y Vinton Cerf diseñaron entre 1973 y 1974 el conjunto de protocolos conocido como TCP/IP. La innovación central consistió en separar dos funciones fundamentales del proceso de comunicación. El *Internet Protocol* (IP) se encargaría del direccionamiento y enrutamiento de los paquetes de datos, mientras que el *Transmission Control Protocol* (TCP) garantizaría que esos paquetes llegaran completos, en el orden correcto y sin errores. Esta división funcional introdujo una arquitectura modular que permitía que redes heterogéneas, ya fueran satelitales, radioeléctricas o cableadas, pudieran interconectarse sin necesidad de alterar su estructura interna. Si bien cada red conservaba su autonomía tecnológica, podía comunicarse mediante una capa común de interconexión. Este principio recibió el nombre de arquitectura abierta. Su relevancia fue extraordinaria, ya que estableció la base de una meta-arquitectura capaz de integrar sistemas diversos bajo reglas compartidas. Con la transición coordinada al protocolo TCP/IP el 1 de enero de 1983, ARPANET dejó de ser una red experimental y se configuró formalmente el Internet como una auténtica “red de redes” (Leiner et al., 1997).

A partir de ese momento la expansión fue acelerada. La creación del *Domain Name System* (DNS) permitió sustituir complejas direcciones numéricas por

nombres legibles, y así facilitó la escalabilidad y el uso masivo. La consolidación de NSFNET, durante la década de 1980, amplió significativamente el acceso académico y científico, mientras que la privatización de la infraestructura troncal, en 1995, marcó la transición hacia un sistema de alcance civil global (Abbate, 1999; Leiner et al., 2009).

Desde una perspectiva estratégica, el periodo comprendido entre 1962 y 1995 revela que el éxito de internet no puede atribuirse a una aplicación específica, sino a decisiones estructurales que moldearon su arquitectura y gobernanza (tabla 1). En primer lugar, un diseño descentralizado que evitó puntos únicos de fallo y concentración excesiva de control. En segundo lugar, la adopción de estándares abiertos formalizados mediante memorandos RFC (por las iniciales en inglés de *Request of Comments*), lo que permitió innovación acumulativa y compatibilidad progresiva. En tercer lugar, la consolidación de una comunidad técnica colaborativa que discutía, probaba y perfeccionaba los protocolos en un entorno de cooperación distribuida. Estos tres factores no solo hicieron posible la expansión técnica del sistema. Hicieron posible su expansión civilizatoria, al sentar las bases de una infraestructura global abierta, interoperable y socialmente apropiable que transformaría las dinámicas económicas, políticas y culturales del mundo contemporáneo.

Tabla 1. *Formación de internet (1962-1995)*

Periodo	Hito histórico-técnico	Actores clave	Innovación técnica	Problema que resuelve	Implicación estratégica estructural
1962	Concepto de "Red Galáctica"	J. C. R. Licklider (MIT/ARPA)	Visión de interconexión global distribuida	Aislamiento de sistemas de cómputo	Se Introduce el paradigma descentralizado de acceso universal al conocimiento
1961-1967	Teoría y desarrollo de conmutación de paquetes	Kleinrock (MIT/UCLA); Baran (RAND); Davies (NPL)	Fragmentación de datos en "paquetes"	Rigidez y vulnerabilidad de la conmutación de circuitos	Establece una arquitectura resiliente y adaptable a entornos inciertos
1967	Diseño formal de ARPANET	ARPA	Red experimental de conmutación de paquetes	Interconexión de centros de investigación financiados por Defensa	Nace la infraestructura científico-militar de interconexión
1969	Conexión de los primeros nodos (UCLA, SRI, UCSB, Utah)	ARPA; BBN; universidades	Primeros IMP (<i>Interface Message Processors</i>)	Comunicación remota entre hosts	Inicio operativo de la red distribuida

Continúa en la otra página

Periodo	Hito histórico-técnico	Actores clave	Innovación técnica	Problema que resuelve	Implicación estratégica estructural
1970-1972	Desarrollo NCP y aparición del correo electrónico	Network Working Group, Ray Tomlinson	Protocolo host-to-host y email	Coordinación entre investigadores	Transición de red técnica a red social ("persona a persona")
1973-1974	Diseño de TCP/IP	Vinton Cerf y Robert Kahn	Separación IP (enrutamiento) y TCP (control de transporte)	Interconexión entre redes heterogéneas	Nace la arquitectura abierta de "red de redes"
1983	Transición oficial a TCP/IP	Comunidad ARPANET	Unificación protocolaria global	Incompatibilidad entre sistemas	Formalización del internet moderno
1984	Creación del DNS	Paul Mockapetris	Sistema jerárquico de nombres de dominio	Escalabilidad de direcciones numéricas	Facilita expansión civil y comercial
1985-1995	NSFNET y expansión académica/comercial	NSF; universidades, sector privado	Infraestructura troncal de alta velocidad	Limitación de acceso restringido	Internacionalización y transición a infraestructura pública
1995	Privatización del backbone NSFNET	Sector privado	Infraestructura comercial	Dependencia de la financiación estatal	Consolidación de internet como infraestructura global civil

Fuente: elaboración propia, con base en Leiner et al. (1997; 2009).

Si internet constituyó la condición de posibilidad técnica de la conectividad global, la World Wide Web representó la condición de posibilidad cultural de su masificación. Hasta finales de los años ochenta, internet era utilizado principalmente por comunidades académicas, científicas y militares. Su operación exigía conocimientos técnicos específicos, manejo de interfaces basadas en comandos y comprensión de protocolos como FTP o Telnet. Se trataba de una red funcional y poderosa, pero aún distante de la experiencia intuitiva que caracterizaría su expansión posterior.

La transformación comenzó en 1989, cuando Tim Berners-Lee, físico e ingeniero británico del CERN (Conseil Européen pour la Recherche Nucléaire), propuso un sistema destinado a enlazar documentos científicos alojados en distintos servidores mediante hipervínculos. Su objetivo no era comercial ni político, sino resolver un problema concreto de coordinación y gestión de información entre investigadores que participaban en proyectos colaborativos internacionales. La propuesta respondía a una necesidad práctica, pero sus implicaciones trascenderían con amplitud el ámbito científico.

La solución fue conceptualmente simple y, al mismo tiempo, disruptiva. Berners-Lee diseñó un conjunto integrado de herramientas compuesto por el

protocolo HTTP, encargado de regular la comunicación entre cliente y servidor; el lenguaje HTML, orientado a estructurar documentos enlazables, y el sistema de identificación mediante Uniform Resource Locator (URL), que permitía localizar recursos específicos dentro de la red global. La combinación de estos elementos creó una capa de organización documental sobre la infraestructura existente de internet.

En 1991 la Web fue liberada públicamente, y este hecho marcó una inflexión histórica. Mientras internet operaba en múltiples capas técnicas invisibles para el usuario promedio, la Web introdujo una interfaz de navegación visual basada en documentos hipermediales accesibles mediante navegadores. Con el lanzamiento del navegador *Mosaic*, en 1993, la adopción civil del sistema se aceleró de manera exponencial. La navegación dejó de depender del dominio de comandos técnicos y empezó a organizarse en torno a enlaces, ventanas y entornos gráficos comprensibles para usuarios no especializados.

En este punto resulta imprescindible subrayar una distinción conceptual clave para la arquitectura analítica de este capítulo. La Web no es sinónimo de internet, sino un servicio construido sobre este. Internet abarca el conjunto de protocolos y servicios de comunicación digital, incluyendo correo electrónico, transferencia de archivos, telefonía IP y sistemas de enrutamiento. La Web, en cambio, se limita al acceso y visualización de documentos interconectados mediante el protocolo HTTP (Berners-Lee & Fischetti, 2000; Zittrain, 2008). Sin embargo, debido a su accesibilidad y a su carácter visual, la Web se convirtió en la interfaz dominante del ecosistema digital, hasta el punto de que en el lenguaje cotidiano ambos términos comenzaron a confundirse.

La transición hacia la Web no modificó únicamente la experiencia técnica del usuario, sino que alteró de manera profunda la estructura sociopolítica del entorno digital. La posibilidad de publicar y acceder a contenidos de manera relativamente sencilla permitió la proliferación de millones de sitios interconectados y favoreció la emergencia de lo que algunos autores denominaron una esfera pública digital (Sunstein, 2006). Al mismo tiempo, la expansión de esta arquitectura generó dinámicas de centralización en torno a grandes plataformas, economías basadas en la extracción de datos y modelos de negocio sustentados en la captura sistemática de la atención (Zuboff, 2019).

Desde una perspectiva estratégica, la Web desempeñó funciones históricas decisivas. Democratizó el acceso al contenido digital al reducir las barreras técnicas de entrada, amplió el espectro de actores capaces de producir y distribuir información y transformó una infraestructura técnica en un espacio cultural y

político. Si internet fue concebido bajo una lógica de resiliencia estructural orientada a garantizar la continuidad de la comunicación frente a fallos o interrupciones, la Web respondió a una lógica de accesibilidad cognitiva orientada a facilitar la circulación del conocimiento.

Esta capa experiencial preparó el terreno para una evolución ulterior, en la que la Web dejaría de ser un entorno predominantemente de lectura para convertirse en un espacio de participación, creación y validación distribuida. Esa transformación no fue accidental ni abrupta: fue el resultado lógico de la expansión técnica, social y económica de la arquitectura hipermedial creada a comienzos de los años noventa (tabla 2).

Tabla 2. *Evolución de la World Wide Web*

Dimensión analítica	Web 1.0 (lectura)	Web 2.0 (participación)	Web 3.0 (validación y descentralización)
Periodo dominante	1991-2004	2004-2018	2018-presente (en consolidación)
Modelo de interacción	Unidireccional	Bidireccional	Multidireccional y descentralizado
Rol del usuario	Consumidor de contenido	Creador y distribuidor de contenido	Cocreador, validador y propietario potencial de datos
Arquitectura tecnológica	Sitios estáticos; HTML básico	Plataformas dinámicas; <i>Application Programming Interface</i> (API); redes sociales	<i>Blockchain</i> ; contratos inteligentes; web semántica
Lógica económica	Publicación institucional	Economía de plataformas y publicidad basada en datos	Tokenización; economía descentralizada; activos digitales
Gobernanza	Centralizada (<i>webmasters</i> y servidores institucionales)	Centralizada en plataformas (<i>Big Tech</i>)	Tendencia a modelos distribuidos y <i>Decentralized Autonomous Organization</i> (DAO)
Infraestructura de confianza	Autoridad institucional	Reputación algorítmica y métricas de interacción	Validación criptográfica y consenso distribuido
Relación con el poder	Difusión de información	Amplificación algorítmica y concentración de plataformas	Redistribución potencial del control y soberanía digital
Implicación estratégica	Expansión informativa	Competencia narrativa y guerra de atención	Reconfiguración de la soberanía, identidad y control de datos

Fuente: elaboración propia, con base en Tesfaye (2023).

La primera etapa, retrospectivamente denominada Web 1.0, se caracterizó por la primacía del documento estático. Los sitios funcionaban como vitrinas digitales donde instituciones, empresas o medios publicaban información que los usuarios consumían de manera pasiva. La interacción era limitada, y el flujo comunicativo, predominantemente unidireccional. Desde el punto de vista estratégico, dicha fase amplió la difusión global de información, pero no alteró sustancialmente las estructuras tradicionales de producción del discurso.

La emergencia de la Web 2.0 supuso una ruptura cualitativa. A partir de mediados de la década de 2000 el desarrollo de tecnologías dinámicas, bases de datos interactivas y arquitecturas de programación abiertas permitió que los usuarios dejaran de ser meros receptores para convertirse en productores activos de contenido. Blogs, foros, redes sociales y plataformas colaborativas transformaron la Web en un espacio participativo. Como señala Tesfaye (2023), esta etapa puede entenderse como el tránsito del consumo pasivo hacia la creación activa. Sin embargo, la promesa democratizadora de la Web 2.0 vino acompañada de un fenómeno estructural de concentración, en el que la infraestructura participativa terminó articulándose alrededor de grandes plataformas que operan como intermediarios algorítmicos. La gobernanza dejó de estar distribuida entre múltiples sitios independientes y pasó a concentrarse en ecosistemas corporativos capaces de modular visibilidad, atención y monetización. Desde una perspectiva geopolítica, esta fase consolidó la economía de la atención y abrió el escenario para nuevas formas de competencia narrativa, manipulación informativa y guerra cognitiva.

En este contexto emerge la idea de Web 3.0, entendida como un intento de superar tanto la pasividad de la Web 1.0 como la centralización de la Web 2.0. Según Tesfaye (2023), esta fase se orienta hacia la validación distribuida, la descentralización de la infraestructura y la incorporación de tecnologías como *blockchain*, contratos inteligentes y sistemas de identidad digital soberana. La promesa central radica en reconfigurar la relación entre usuario y plataforma devolviendo al individuo cierto control sobre sus datos, activos digitales y procesos de verificación.

Desde una perspectiva estratégica, esta evolución no es tan solo técnica. Implica una transformación en la arquitectura del poder digital. Si la Web 1.0 amplificó la información y la Web 2.0 amplificó la interacción, la Web 3.0 aspira a redistribuir la confianza. Y en el ciberespacio contemporáneo la confianza es un recurso estratégico tan decisivo como la infraestructura física o la superioridad tecnológica. Así, la progresión de la Web no debe interpretarse como una simple secuencia de innovaciones, sino como una reconfiguración continua de las

relaciones entre infraestructura, usuario, plataforma y poder. Comprender esta evolución resulta indispensable para analizar cómo el ciberespacio se ha convertido no solo en un entorno de comunicación, sino en un dominio de competencia estratégica donde se disputan soberanía, identidad y legitimidad en tiempo real.

Ahora bien, si la evolución de internet explica la emergencia de una infraestructura global de interconexión, y la Web, su transformación en entorno cultural de masificación, el siguiente nivel de análisis exige ampliar la escala conceptual. Es aquí donde la noción de red adquiere centralidad teórica. El término “red” no se limita al ámbito digital: en sentido amplio, designa cualquier sistema compuesto por nodos interconectados que intercambian recursos, energía o información. Por ende, existen redes biológicas, financieras, sociales, organizacionales y tecnológicas. Lo distintivo de una red no es su soporte material, sino su estructura relacional. En el contexto digital esta lógica se materializa en múltiples configuraciones como redes locales, metropolitanas, extensas, privadas o inalámbricas. Cada una de dichas redes cumple funciones específicas, desde sostener una intranet corporativa hasta articular infraestructuras críticas como sensores industriales, sistemas de *Supervisory Control and Data Acquisition* (SCADA) o arquitecturas del Internet de las Cosas (IoT).

Sin embargo, reducir la red a su dimensión técnica sería insuficiente. Como advierte Castells (2009), vivimos en una sociedad en red, donde la lógica de la conectividad desplaza progresivamente a la lógica jerárquica tradicional. En este entorno el poder ya no depende exclusivamente del control territorial o institucional, sino de la capacidad para estructurar flujos de información, modular conexiones y gestionar nodos estratégicos. Las redes digitales no solo transmiten datos: también reorganizan las formas de producción, comunicación y autoridad. Esta transición conceptual permite comprender que internet no es la red en sí misma, sino una infraestructura específica dentro de una lógica reticular más amplia. Las redes pueden existir dentro o fuera de internet, pueden ser públicas o privadas, abiertas o cerradas, físicas o virtuales. Internet constituye una arquitectura particular de interconexión global basada en protocolos abiertos. Las redes, en cambio, son la forma estructural que adopta la interdependencia contemporánea.

Sobre esta arquitectura reticular emerge un nivel aún más complejo de abstracción: el ciberespacio. El ciberespacio no es tan solo el conjunto de cables, servidores y protocolos. Tampoco es reducible a la Web ni a una colección de plataformas. Constituye un entorno sociotécnico emergente que integra infraestructura física, sistemas lógicos, contenidos digitales e interacción humana. Como plantea

Nissenbaum (2005), el ciberespacio es una construcción normativa y social, tanto como tecnológica. Ning (2022) lo describe como una dimensión virtual creada por la interacción entre computadores, *software*, protocolos y actores humanos, donde se desarrollan dinámicas económicas, culturales, políticas y militares.

Por consiguiente, el ciberespacio no es un lugar, sino un entorno funcional donde se producen efectos reales, ya que allí ocurren operaciones de ciberguerra, campañas de desinformación, hacktivismo, espionaje digital y disputas narrativas. Desde una perspectiva estratégica, el ciberespacio se ha consolidado como un dominio de poder comparable a los dominios terrestre, marítimo, aéreo y espacial (Libicki, 2009). Sin embargo, a diferencia de estos, su naturaleza es híbrida. Combina materialidad física con dimensión simbólica; integra *hardware* con identidades colectivas y articula infraestructura con cognición. Kadlečová (2024) subraya, precisamente, esta ambigüedad estructural. En consecuencia, el ciberespacio no puede gobernarse únicamente con lógica técnica, porque su dinámica involucra derecho internacional, economía política, ingeniería, filosofía y teoría estratégica. La infraestructura puede ser descentralizada, pero las narrativas pueden concentrarse. La arquitectura puede ser abierta, pero el poder puede capturarse algorítmicamente.

En este punto se cierra el círculo histórico iniciado con la formación de internet. La cultura de estandarización abierta mediante memorandos RFC, la transición coordinada a TCP/IP, en 1983, y la implementación del DNS como sistema distribuido de nombres evidencian una lógica evolutiva constante. Internet resolvió sus propios cuellos de botella mediante arquitectura modular, protocolos interoperables y coordinación comunitaria (Leiner et al., 2009). Esa combinación de infraestructura, estándares abiertos y comunidad técnica permitió no solo la expansión técnica, sino la emergencia de un espacio sociopolítico global.

Por encima del soporte físico de internet y de la interfaz cultural de la Web, el ciberespacio se configura como un entorno sistémico donde se construye poder, se producen conflictos y se disputan narrativas. Una interrupción de internet puede afectar servicios específicos. Una operación en el ciberespacio puede alterar percepciones colectivas, procesos electorales o equilibrios estratégicos (Lonergan & Lonergan, 2023). La Web constituye apenas una fracción visible de este entorno, aunque ha sido escenario central de fenómenos como polarización algorítmica, concentración de plataformas y extracción masiva de datos (Zuboff, 2019). Diferenciar con precisión estos conceptos no es un ejercicio semántico, sino una exigencia analítica. Internet es infraestructura física y lógica. Las redes son arquitecturas relacionales que estructuran interdependencias. La Web es una capa

hipermedial construida sobre internet. El ciberespacio es el entorno estratégico donde convergen tecnología, identidad y poder (tabla 3).

Tabla 3. *Internet, web, redes y ciberespacio: distinción conceptual y estratégica*

Categoría	Internet	World Wide Web	Redes (network)	Ciberespacio
Naturaleza	Infraestructura físico-lógica global basada en TCP/IP	Servicio hipermedial construido sobre Internet	Estructura relacional de nodos interconectados	Entorno sociotécnico emergente
Nivel analítico	Técnico-arquitectónico	Interfaz cultural y comunicativa	Arquitectura estructural	Dominio estratégico y simbólico
Qué es	"Red de redes" interoperables	Sistema de documentos enlazados vía HTTP/HTML	Sistema de conexiones entre nodos	Espacio funcional donde interactúan tecnología, información y actores
Soporte material	Servidores; cables; routers; protocolos; DNS	Navegadores; servidores web; hipervínculos	Puede ser digital, social, biológica o institucional	Integra infraestructura, software, datos y actividad humana
Función principal	Permitir conectividad global	Facilitar navegación y acceso a contenidos	Organizar flujos de información o recursos	Articular poder, identidad, conflicto y gobernanza
Origen histórico clave	ARPANET (1969); TCP/IP (1983); DNS	CERN (1989-1991); HTTP; HTML	Concepto transversal previo a lo digital	Consolidación doctrinal en seguridad y estrategia (finales siglo XX- siglo XXI)
Ejemplos típicos	Correo electrónico; FTP; VoIP	Sitios web; blogs; portales; plataformas	LAN; WAN; redes sociales; IoT	Ciberguerra; desinformación; hacktivismo; vigilancia
Dimensión de poder	Control de infraestructura y protocolos	Control de plataformas y atención	Control de nodos y flujos	Control narrativo, cognitivo y estratégico
Vulnerabilidades críticas	Ataques a infraestructura; interrupciones físicas	Manipulación algorítmica; concentración de plataformas	Fragmentación; captura de nodos estratégicos	Operaciones híbridas; guerra cognitiva; erosión institucional
Pregunta estratégica central	¿Quién controla la conectividad?	¿Quién controla la visibilidad y la atención?	¿Quién estructura los flujos?	¿Quién define la percepción, la legitimidad y la narrativa?

Fuente: elaboración propia.

En una era de interdependencia digital, comprender con precisión esta taxonomía no es un ejercicio terminológico, sino una condición estructural para el pensamiento estratégico contemporáneo¹. Diseñar políticas de ciberdefensa, marcos de

¹ En términos doctrinales, esta distinción ha sido adoptada por algunas fuerzas militares y agencias de seguridad en el diseño de capacidades cibernéticas. La doctrina estadounidense distingue entre el *Cyber Domain*

gobernanza digital o estrategias de protección de la soberanía informacional exige distinguir con rigor entre infraestructura, arquitectura, interfaz y dominio. Sin esa claridad, el análisis corre el riesgo de confundir el soporte técnico con el espacio donde se disputa el poder, o de reducir el ciberespacio a su dimensión tecnológica ignorando su carácter político, simbólico y cognitivo.

Confundir internet con Web, redes con dominio estratégico, o conectividad con soberanía no es un error académico menor: es una vulnerabilidad conceptual que puede traducirse en decisiones institucionales equivocadas, asignaciones erróneas de recursos y respuestas inadecuadas frente a amenazas híbridas. En el campo de batalla digital, la imprecisión conceptual no produce únicamente debates teóricos defectuosos: también produce desventajas estratégicas reales. Allí donde el adversario comprende las capas del sistema y explota sus intersecciones, la confusión analítica se convierte en asimetría de poder.

La dimensión oculta de la Web: expansión masiva, centralización del tráfico y el nuevo orden digital global

Desde la creación del primer sitio web por Tim Berners-Lee en el CERN (6 de agosto de 1991) el crecimiento de la World Wide Web ha sido, sin duda, exponencial. Concebida originalmente como un sistema para facilitar la distribución e interconexión de documentos académicos, la Web ha venido evolucionado hasta convertirse en una infraestructura a escala planetaria que sustenta la comunicación global, el comercio, la política y la cultura contemporánea. Con base en Netcraft (2026), para febrero de 2026 se estima que existen 1.419.977.535 sitios web aproximadamente, distribuidos en 297.071.903 dominios registrados, de los cuales solo 193.890.945 (17,32 %), se mantienen activos; el resto conforma un vasto territorio digital inactivo, compuesto por dominios expirados, abandonados o aparcados, lo que refleja la naturaleza efímera y fluctuante de gran parte de la presencia web.

Empero, la creación de nuevos sitios web continúa a un ritmo extraordinario. En promedio, se generan entre 170.000 y 250.000 nuevos sitios por día, lo que equivale a entre 5 y 7,5 millones mensuales, entre 1,2 y 1,7 millones semanales y entre 120 y 175 sitios nuevos cada minuto (Netcraft, 2026). Estas cifras reflejan no solo la accesibilidad creciente a las plataformas digitales, sino la intensificación de la competencia por el espacio y la visibilidad en el ecosistema informacional

como espacio de operaciones militares, y las "redes", como activos críticos para defender o atacar. A nivel nacional, Estados como Estonia, Israel y Francia han incorporado la noción de "ciberespacio" como un entorno estratégico multidimensional, lo que ha derivado en políticas públicas específicas para garantizar su soberanía digital y proteger su infraestructura crítica.

global. Por consiguiente, la proliferación de sitios es síntoma de una transformación socio-tecnológica más profunda: estar en línea ha dejado de ser opcional para convertirse en una condición de existencia para individuos, empresas, instituciones y Estados.

La dinámica de registro de dominios refuerza esta tendencia de expansión global. Según Netcraft (2026), en los dos primeros meses de 2026 se registraron 5 millones de nuevos nombres de dominio. El dominio de nivel superior (DNS) más utilizado sigue siendo “.com”, con más de 157 millones de registros, seguido por “.net”, con 13 millones de registros. Los dominios “.com” representan el 44,4 % del total del mundo, por lo que se consolidan como el espacio web más codiciado y reconocible. La persistencia de estos DNS clásicos revela el valor comercial asociado a dichas extensiones tradicionales, a pesar de la creciente disponibilidad en el mercado de otros dominios alternativos, que son más especializados o geolocalizados. Sin embargo, no todos los sitios web contribuyen por igual al uso y la influencia de la red. De los más de mil millones de sitios existentes, aproximadamente 600 millones corresponden a blogs, lo que representa el 53,6 % de toda la web. Esta cifra evidencia la democratización de la producción de contenido digital. En contraste, los sitios de comercio electrónico, aunque apenas representan el 2,52 % del total (aproximadamente 28,2 millones), concentran una parte significativa del tráfico transaccional en línea. De manera similar, los sitios de contenido pornográfico constituyen el 2,23 % de la web (alrededor de 25 millones), pero generan cerca del 30 % del tráfico global (Netcraft, 2026), cifra que revela el poder de atracción de este tipo de contenidos dentro de la economía digital.

En 2026 el ecosistema digital a nivel global se caracteriza por una vasta, pero desigual, distribución de recursos, tráfico, infraestructura y contenidos, aunque dicha configuración no es neutral ni espontánea, pues responde a procesos históricos de acumulación, hegemonía y poder. Así, las dinámicas de distribución de la web determinan no solo quién tiene acceso a la información, sino también quién la controla, quién la produce, en qué lenguas circula y bajo qué condiciones se sostiene la soberanía tecnológica. Las implicaciones lingüísticas, geopolíticas y estratégicas derivadas de esta arquitectura informacional son decisivas para comprender los desafíos contemporáneos en torno al poder digital, la gobernanza de internet y la ciberseguridad internacional.

Desde el punto de vista lingüístico, la web reproduce y amplifica las jerarquías propias del orden geopolítico occidental. A pesar de que el inglés es la lengua materna de apenas el 4,9 % de la población mundial (Eberhard et al., 2023), más del

52 % de los sitios web están escritos en inglés, seguidos muy de lejos por los escritos en español (5,5 %), en alemán (4,8 %), en ruso (4,5 %) y en japonés (4,35 %) (Statista, 2024a). Esta sobrerrepresentación del idioma inglés no solo limita la participación significativa de comunidades lingüísticas no anglófonas, sino que genera un sesgo epistémico en los resultados de búsqueda, en los corpus de entrenamiento de inteligencia artificial y en las plataformas dominantes del conocimiento digital. Tal como señala Phillipson (2009), la expansión del inglés ha sido no solo una tendencia cultural, sino también una expresión de "imperialismo lingüístico", en el que la lengua funciona como instrumento de control simbólico y acceso desigual al capital cognitivo.

Asimismo, los lenguajes de programación constituyen no solo herramientas técnicas de construcción de *software*, sino también vectores fundamentales de gobernanza tecnológica, innovación y dominio epistemológico en el ecosistema digital contemporáneo. Entonces, comprender su distribución y uso es clave para trazar los contornos del poder computacional global. Según los datos más recientes recopilados por Statista (2024b), los lenguajes de programación más utilizados en el mundo reflejan patrones tanto de estandarización técnica como de herencias históricas, decisiones corporativas y estructuras educativas que configuran las capacidades y límites del desarrollo digital global. JavaScript ocupa el primer puesto en el *ranking*, al ser utilizado por el 63,61 % de los desarrolladores encuestados. Este dominio se debe a su centralidad en el desarrollo web moderno, tanto del lado cliente como del lado servidor, a través de entornos como Node.js. Su ubicuidad se ha visto potenciada por marcos de trabajo como React, Angular y Vue.js, los cuales permiten construir aplicaciones web interactivas y altamente escalables. En este orden de ideas, JavaScript no solo ha logrado extender su relevancia más allá del navegador, sino que también se ha convertido en una puerta de entrada para nuevos desarrolladores, debido a su accesible curva de aprendizaje y disponibilidad de recursos de formación.

En segundo lugar, se encuentra HTML/CSS, con el 52,97 % de uso (Statista, 2024b). Aunque técnicamente no son lenguajes de programación, sino de marcado y estilo, su inclusión en el *ranking* refleja su papel imprescindible en la creación de las interfaces gráficas, arquitectura de la información y diseño de experiencias de usuario: sin dichas herramientas, ninguna aplicación web moderna podría tomar forma de manera visual o funcional, y por tal motivo su presencia denota que el desarrollo de *software* contemporáneo es una cuestión no solo de lógica algorítmica, sino también de presentación, accesibilidad y usabilidad. Por su lado,

SQL, con el 51,52 % de adopción (Statista, 2024b), sigue siendo importante para la gestión de datos estructurados, y su vigencia revela que a pesar del auge de arquitecturas orientadas a eventos, microservicios y bases NoSQL, la mayoría de las aplicaciones empresariales, sistemas financieros y plataformas institucionales continúan dependiendo de bases de datos relacionales².

Por su parte, Python ocupa el cuarto lugar, con el 48,07 % (Statista, 2024b), por lo que se constituye en un caso paradigmático de expansión transversal. Si bien fue adoptado inicialmente por las comunidades académicas y científicas, Python ha demostrado una gran capacidad para adaptarse a múltiples dominios, desde análisis de datos y aprendizaje automático hasta desarrollo web y automatización. Su sintaxis simple, acompañada de una vasta cantidad de bibliotecas (como NumPy, Pandas, TensorFlow y Flask), ha impulsado su incorporación generalizada en proyectos educativos, *startups* tecnológicas y sistemas de inteligencia artificial (IA). Además, su uso extensivo en educación ha reforzado su presencia como uno de los lenguajes más amigables para principiantes, y así favorecer la inclusión digital en el ámbito técnico.

Ahora bien, de acuerdo con Statista (2024b), otros lenguajes con importantes niveles de adopción incluyen TypeScript (40,15 %), Java (33,27 %), C# (29,95 %) y Bash/Shell (28,38 %). En relación con el crecimiento de TypeScript (un superconjunto de JavaScript con tipado estático), este refleja una tendencia hacia una mayor robustez en entornos de desarrollo a gran escala, donde la previsibilidad del código se vuelve crítica. Java, por su parte, mantiene la relevancia gracias a su integración profunda en sistemas bancarios, plataformas empresariales y el desarrollo de aplicaciones Android. Con referencia a C#, el cual es impulsado por la plataforma .NET de Microsoft, es una opción popular en entornos corporativos y para videojuegos mediante el motor Unity. El uso de Bash/Shell remite a la necesidad de automatizar tareas administrativas y gestionar entornos de servidor en sistemas operativos basados en Unix. En un plano más técnico se ubican lenguajes como C++ (20,21 %) y Go (13,94 %), los cuales se utilizan mayoritariamente en el desarrollo de sistemas, programación embebida y *backend* de alto rendimiento. Rust, aunque con menor penetración (13,05 %), ha emergido como una opción preferente en entornos donde la seguridad de memoria, concurrencia y eficiencia son prioritarias, y debido a ello es adoptado por diversas empresas como Mozilla y Microsoft, especialmente en proyectos experimentales y de infraestructura crítica.

² Este lenguaje desempeña un rol central en la persistencia de información, el modelado de entidades y la integridad de los datos, lo que lo convierte en un pilar de la infraestructura digital.

Este panorama de lenguajes utilizados indica no solo preferencias técnicas, sino también un mapa de competencias profesionales, orientaciones estratégicas de grandes plataformas tecnológicas y paradigmas de enseñanza en instituciones educativas, ya que la popularidad de un lenguaje se correlaciona con su apoyo institucional, su comunidad activa, su presencia en entornos de trabajo reales y la disponibilidad de herramientas de desarrollo integradas. Y desde una perspectiva geopolítica y epistémica, esta distribución también refleja una forma de hegemonía cultural, pues la mayoría de los lenguajes dominantes han sido desarrollados y mantenidos en el Norte Global, lo que implica que las reglas gramaticales del código, los entornos de desarrollo, los foros de discusión y la documentación son modelados por valores culturales y prioridades económicas de las grandes potencias tecnológicas. Tal situación plantea interrogantes sobre la soberanía digital, la dependencia tecnológica y la posibilidad de desarrollar infraestructuras de *software* localizadas, resilientes y adaptadas a contextos lingüísticos y sociales diversos. Así pues, el análisis de los lenguajes de programación más utilizados entre 2024 y 2025 ofrece una ventana al estado actual del desarrollo tecnológico global, ya que más allá de cumplir una evidente función instrumental, estos lenguajes de programación constituyen un auténtico campo de disputas por la estandarización, la autonomía y la capacidad de innovación. Comprender su distribución es clave para diseñar estrategias educativas, políticas de innovación y arquitecturas digitales que respondan a los desafíos del siglo XXI.

La dimensión geopolítica de esta distribución también es crítica. Aunque existen más de 270 millones de dominios registrados a nivel global, cerca del 63 % de ellos están registrados de forma privada o en jurisdicciones opacas (Netcraft, 2025). Entre los dominios atribuibles, Estados Unidos controla el 18,6 %, seguido por países como Islandia (21,03 millones), China (19,94 millones) y Canadá (9,92 millones), aunque todos por debajo del volumen estadounidense. El predominio estadounidense se traduce en un control desproporcionado sobre los centros de datos, servidores raíz, intercambios de tráfico y proveedores de servicios de nombres de dominio (DNS), lo cual consolida una posición geoestratégica privilegiada en la gobernanza de la infraestructura crítica del ciberespacio (Mueller, 2017).

La desigualdad en la visibilidad y el tráfico de los sitios web también se refleja en la lista de los más visitados. Aunque existen más de 1.100 millones de sitios web, la mayoría del tráfico global se concentra en menos de 20 plataformas (Semrush, 2026), donde google.com encabeza el *ranking* global, con más de 88,46 mil millones de visitas mensuales (Semrush, 2026), seguido por YouTube

(45,68 mil millones), Facebook (8,22 mil millones), Instagram (5,32 mil millones), ChatGPT (5,19 mil millones), Reddit (4,45 mil millones) y Wikipedia (3,77 mil millones). Estas plataformas no solo concentran una proporción descomunal del tráfico, sino que también actúan como infraestructuras cognitivas que moldean el acceso a la información, las dinámicas culturales y la experiencia digital cotidiana de miles de millones de usuarios. Es especialmente notable la irrupción de plataformas como ChatGPT.com, que reflejan la integración cada vez mayor de la IA en el consumo masivo de contenidos y servicios. Esta concentración convierte las plataformas en actores de poder fáctico transnacional, capaces de condicionar el acceso a la información, manipular flujos de opinión pública y definir los términos del debate político y cultural. Como advierte Zuboff (2019), nos enfrentamos a una nueva forma de capitalismo de vigilancia, en la que el control sobre los datos y los comportamientos de los usuarios es más valioso que la infraestructura misma.

Para los Estados, especialmente los del Sur Global, como Colombia, la situación representa un doble desafío, ya que, por un lado, se ven expuestos a vulnerabilidades estructurales al depender de infraestructura alojada en el extranjero. Por otro, enfrentan barreras de entrada para desarrollar capacidades propias de producción de contenidos, tecnologías de lengua local y sistemas de seguridad digital autónomos. La ausencia de soberanía tecnológica se traduce en una forma de dependencia estratégica en el dominio informacional. Como plantea Kadlečová (2024), la soberanía cibernética no se limita al control técnico de redes, sino que incluye la capacidad para definir normativas, proteger infraestructuras críticas y garantizar que las decisiones sobre gobernanza digital respondan a intereses nacionales.

Por lo tanto, la distribución desigual de la web no solo refleja disparidades económicas o técnicas, sino que constituye un campo de disputa global por el control del conocimiento, la identidad y la seguridad. La hegemonía anglófona, la concentración de dominios y el control infraestructural convergen en un sistema asimétrico que limita la pluralidad lingüística, la equidad informacional y la autodeterminación tecnológica. En el contexto descrito, los Estados que aspiren a ejercer soberanía digital deberán invertir en infraestructura propia, fomentar ecosistemas de contenido multilingüe, establecer marcos regulatorios autónomos y promover una diplomacia tecnológica activa en los foros internacionales de gobernanza de internet. Por consiguiente, las implicaciones lingüísticas, geopolíticas y estratégicas de la distribución de la web no pueden analizarse por separado, ya que, en conjunto, configuran el nuevo orden informacional del siglo XXI, donde el poder ya no se ejerce únicamente por la posesión del territorio, sino por la capacidad para

controlar los circuitos invisibles que hacen posible la conectividad, la comunicación y la cognición en red. Comprender esta arquitectura de poder distribuido (y a la vez, centralizado), es clave para diseñar políticas públicas, estrategias de defensa y modelos de gobernanza que respondan a los desafíos de una humanidad crecientemente digitalizada.

En resumen, lo que emerge de ese panorama estadístico es un retrato de internet como espacio vasto, pero desigual. La web de 2025 es, al mismo tiempo, expansiva y centralizada; accesible, pero jerárquica; multilingüe en capacidad, pero anglocéntrica en su práctica. La distancia entre la cantidad de sitios existentes y la proporción de sitios realmente activos y relevantes dice mucho sobre las dinámicas de participación digital. Si bien las barreras técnicas de entrada han disminuido, la posibilidad de generar impacto y mantenerse visible se ha vuelto cada vez más difícil. Entender la arquitectura, la distribución y los patrones de comportamiento de la red en 2025 no es solo una tarea académica: es una necesidad para interpretar el futuro del conocimiento, el poder, la gobernanza y la identidad en la era digital.

Internet hoy: tráfico, comercio electrónico y conectividad

Por definición, internet es una infraestructura comunicacional que permite la interconexión de redes de todo el mundo. En otras palabras, es una red de redes; dicho esto, en las últimas tres décadas internet ha llegado a significar mucho más que solo la tecnología. Con más del 60 % de la población mundial en línea, internet es ahora una parte integral del tejido de muchas sociedades alrededor del mundo³. el número de usuarios de internet creció en casi el 900 %, de 400 millones a más de 4.540 millones de usuarios entre 2000 y 2020⁴ (Internet Society, 2020). En 2025 se estima que el número de usuarios de internet en todo el mundo ascendió a 5.560 millones, lo que representa el 68 % de la población mundial (Statista, 2025a). Por ende, pocas tecnologías habrían generado (en un período relativamente corto) un cambio social, económico, político, militar y cultural tan extendido en la historia de la humanidad como internet.

El impacto de internet en las sociedades contemporáneas y sus estructuras estatales ha trascendido con creces su concepción original como un entorno para el correo electrónico, las páginas web estáticas o los foros de discusión. Hoy en día internet se configura como un espacio dinámico y multifuncional, clave para

³ No obstante, aún el 40 % de la población total del mundo sigue sin estar conectada a internet (aproximadamente 4.800 millones de personas en el mundo). Más de mil millones de estas personas "fuera de línea" viven en el sur de Asia (31 %), y 870 millones, en África (27 %).

⁴ Entre enero de 2019 y enero de 2020 el aumento fue del 7 % (298 millones de nuevos usuarios en línea).

la colaboración, el comercio global, la creación artística, la educación, el activismo político y, cada vez más, los conflictos geopolíticos y cibernéticos. Su expansión ha transformado no solo hábitos individuales, sino también los modos de organización social, las economías de la atención y los mecanismos del poder en la era digital. Un indicador revelador de esta transformación es el predominio del contenido audiovisual: actualmente el video representa más de dos tercios del tráfico global en línea, impulsado por plataformas como YouTube, TikTok, Instagram y servicios de *streaming* (Cisco, 2023). Además, el uso de redes sociales continúa creciendo; en efecto, para diciembre de 2025 se registraron más de 5.240 millones de usuarios activos, lo que representa aproximadamente el 63,9 % de la población mundial, con un incremento interanual cercano al 3,2 % (Kemp, 2025).

Este ecosistema hiperconectado también redefine la gestión del tiempo y la cognición colectiva. Según los informes del Global Web Index (2024a), el usuario promedio pasa actualmente 6 horas y 37 minutos conectado a internet cada día, lo que equivale a más de 96 días al año navegando, comunicándose o consumiendo contenidos digitales. Si se toma en cuenta que una persona promedio duerme ocho horas diarias, esto implica que más del 41 % del tiempo consciente es dedicado a actividades mediadas por internet. A nivel agregado, los usuarios globales pasarán en 2025 un total estimado de 1.250 millones de años acumulados en línea, de los cuales más de un tercio se invertirá específicamente en plataformas de redes sociales (Global Web Index, 2024). Sin embargo, la cantidad de tiempo que las personas pasan en línea varía de un país a otro: por ejemplo, los internautas colombianos pasan un promedio de 9 horas y 10 minutos en línea por día, en comparación con las 4 horas y 22 minutos por día de los internautas japoneses. Estas cifras evidencian no solo la centralidad de internet en la vida cotidiana, sino también su poder para modelar emociones, percepciones, decisiones y estructuras de participación ciudadana. En ese contexto internet se ha vuelto una infraestructura crítica de la vida contemporánea, cuyo control, regulación y protección plantean desafíos estratégicos sin precedentes para los Estados, las democracias y la seguridad internacional.

Entre 2019 y 2025 el crecimiento sostenido en el número de usuarios de internet ha sido impulsado en gran medida por la mayor disponibilidad de teléfonos inteligentes y planes de datos móviles más asequibles. Sobre la base de datos de DataReportal (2025b), para abril de 2025 el número de usuarios únicos de teléfonos móviles alcanzó los 5.810 millones, lo que representa el 70,7 % de la población mundial; además, se estima que existen más de 7.400 millones de conexiones móviles asociadas a teléfonos inteligentes, por lo cual estos dispositivos constituyen

aproximadamente el 87 % de todos los teléfonos móviles en uso actualmente. En consecuencia, la conectividad móvil se ha consolidado como el principal medio de acceso a internet, debido a que el 96,3 % de los usuarios de internet a nivel mundial acceden a la red mediante un teléfono móvil, y el tráfico web desde dispositivos móviles representa el 63,15 % del total del tráfico global. No obstante, el uso de computadores portátiles y de escritorio sigue siendo relevante, si se toma en cuenta que más del 61 % de los usuarios de internet entre los 16 y los 64 años aún utilizan estos dispositivos, especialmente en contextos laborales y educativos⁵.

El ecosistema de aplicaciones móviles ha experimentado un crecimiento notable. En 2025 los usuarios descargaron aproximadamente 136.000 millones de aplicaciones a través de las plataformas iOS y Google Play. Aunque el número de descargas se ha estabilizado en los últimos años, el gasto de los consumidores en aplicaciones móviles alcanzó los 150.000 millones de dólares en 2025, lo que representa un aumento del 13 %, en comparación con el año anterior (Sensor Tower, 2025). Este crecimiento fue impulsado principalmente por las aplicaciones no relacionadas con juegos, que experimentaron un incremento del 23 % en ingresos, mientras que las aplicaciones de juegos también mostraron una recuperación, con un aumento del 4 % después de dos años de declive (Sensor Tower, 2025). En términos de uso, los usuarios de teléfonos inteligentes pasaron un total de 4,2 billones de horas en aplicaciones móviles en 2025, lo que equivale a un promedio de aproximadamente 3,5 horas por día por usuario (Sensor Tower, 2025). Aunque se observa una ligera desaceleración en el crecimiento del tiempo total dedicado a aplicaciones móviles, este sigue siendo un componente central en la vida digital de las personas.

El crecimiento sostenido del ecosistema digital en la región de América Latina ha consolidado a los teléfonos inteligentes como la principal puerta de acceso a internet y como plataforma dominante para la interacción cotidiana. En 2025 Colombia ejemplifica esta tendencia, dado que el 89,5 % de los internautas del país utilizan al menos una red social, lo que posiciona a estas plataformas como vehículos centrales de comunicación, entretenimiento e, incluso, participación política (Agencia Digital AMD, 2025). La preferencia de los colombianos por las aplicaciones móviles se manifiesta en que el promedio de uso semanal oscila entre seis y diez aplicaciones, con un claro predominio del acceso móvil frente a los navegadores web tradicionales (El Colombiano, 2025). Esta transformación no solo se encuentra vinculada al consumo de tecnología importada, sino que también se

⁵ Aproximadamente el 58 % de todas las solicitudes de páginas web provienen de teléfonos móviles, y el 42 %, de computadores portátiles y de escritorio.

expresa en el dinamismo del sector de desarrollo local. Colombia se ha consolidado como un referente regional en la creación de aplicaciones móviles, con empresas emergentes, estudios tecnológicos y desarrolladores independientes que ofrecen soluciones a medida para sectores tan diversos como el comercio electrónico, la salud, la educación, la movilidad urbana y la cultura digital (Alto Sentido Agencia, 2025). Esta capacidad innovadora permite a Colombia insertarse competitivamente en un mercado regional en expansión.

A nivel regional el crecimiento del mercado de desarrollo de aplicaciones móviles es aún más pronunciado. En 2024 este mercado alcanzó un valor de 18.900 millones de dólares, y se proyecta que para 2033 superará los 55.500 millones de dólares, con una tasa de crecimiento compuesta anual del 11,4 % entre 2025 y 2033 (IMARC Group, 2025). Este fenómeno refleja no solo una mayor demanda por parte de los consumidores, sino también una evolución de los modelos de negocio digitales, una mayor inversión pública y privada en infraestructura tecnológica, y un ecosistema de innovación cada vez más articulado. Un aspecto clave de esta expansión es la creciente penetración de teléfonos inteligentes. En América Latina la adopción de *smartphones* pasó del 81 % en 2024 al 86 % en 2025, y se proyecta que alcanzará el 93 % para 2030 (Frecuencia Online, 2025).

Esta disponibilidad de *hardware* ha facilitado la popularización de aplicaciones en casi todos los aspectos de la vida diaria: desde la educación hasta las relaciones afectivas, pasando por las finanzas, el transporte, la alimentación y la atención médica. Asimismo, destaca el auge de las aplicaciones *fintech*, especialmente en países como Brasil, México, Argentina y Colombia, debido a que estas aplicaciones democratizan el acceso a servicios financieros, especialmente en contextos de alta informalidad y baja bancarización, y eso permite a millones de personas gestionar pagos, enviar remesas, solicitar microcréditos o abrir cuentas digitales (IMARC Group, 2025). Por ende, la expansión del ecosistema móvil se ha consolidado como un motor de inclusión financiera y modernización económica. Y América Latina, en su conjunto, atraviesa una fase de maduración digital acelerada, en la que el uso intensivo de aplicaciones móviles evidencia no solo nuevas modalidades de consumo, sino también una transformación profunda de las prácticas sociales, las dinámicas económicas y las agendas de gobernanza tecnológica. En relación con el caso colombiano, este proceso se manifiesta en una ciudadanía digital cada vez más activa, una comunidad emprendedora en constante crecimiento y un entorno institucional progresivamente más abierto a la innovación y a la adopción de tecnologías disruptivas.

En la actualidad, el tiempo que las personas dedican a las pantallas constituye uno de los indicadores más reveladores de la transformación sociotécnica global; a medida que el mundo transita hacia formas de vida digitalizadas, la exposición diaria a dispositivos electrónicos conectados a internet se vuelve no solo una medida de consumo tecnológico, sino también un reflejo de nuevas formas de interacción social, laboral y cultural. Según los informes de Comparitech (2024), el promedio mundial de tiempo frente a pantallas conectadas asciende a 6 horas y 38 minutos por día, distribuidos entre actividades como redes sociales (2 horas 21 minutos), música en *streaming* (una hora 25 minutos) y *podcasts* (52 minutos). Los teléfonos móviles son el dispositivo predominante, con un uso promedio de 3 horas y 46 minutos diarios.

En el contexto descrito Colombia se ubica como uno de los países con mayor tiempo de exposición a pantallas, pues registra un total de 8 horas y 44 minutos diarios (Comparitech, 2024). Este indicador sitúa al país en el cuarto lugar global, superado únicamente por Sudáfrica (9 horas 37 minutos), Brasil (9 horas 9 minutos) y Filipinas (8 horas 52 minutos). Tal nivel de uso implica que los colombianos pasan más del 55 % de sus horas de vigilia interactuando con pantallas, ya sea en entornos laborales, recreativos, comunicativos o informativos. Asimismo, la distribución del tiempo de pantalla en Colombia revela una fuerte inclinación hacia la movilidad, ya que los dispositivos móviles concentran 4 horas y 47 minutos diarios, mientras que el uso de computadores asciende a 3 horas y 57 minutos (DataReportal, 2024). Esta cifra, claramente superior al promedio global (2 horas 52 minutos en computadores y 3 horas 46 minutos en móviles) sugiere una alta dependencia del ecosistema digital tanto en movilidad como en espacios fijos (Comparitech, 2024). Además, con velocidades de conexión relativamente bajas, en comparación con otras economías (20,67 Mbps en móviles y 162,59 Mbps en conexión fija), la alta exposición no parece estar relacionada con la lentitud de la red, sino con patrones culturales y estructurales de uso intensivo del entorno digital (DataReportal, 2024).

En 2025 el uso de redes sociales sigue consolidándose como una dimensión estructural de la vida digital global. Según el informe Digital 2025 Global Overview, de DataReportal (2025a), los usuarios de internet en el mundo dedican, en promedio, 2 horas y 31 minutos diarios a las redes sociales. Este patrón de uso intensivo del tiempo digital constituye un fenómeno global, con estimaciones que apuntan a que los usuarios de redes sociales podrían invertir en 2025 hasta 4 billones de horas al año en estas plataformas de redes sociales (Exploding Topics, 2025c).

En países como Nigeria, el consumo es de 3 horas 49 minutos al día, equivalente al 70 % más que el promedio mundial, mientras que en Japón apenas si se superan los 49 minutos. En Estados Unidos el tiempo dedicado se ubica en torno a 2 horas 09 minutos diarios⁶, un poco por debajo del promedio global, y en países como España, Francia, Italia y Canadá el tiempo dedicado a redes sociales está entre una hora 40 minutos y 2 horas, por lo cual se ubica apenas por encima o por debajo de la media global.

En Colombia, había 36,7 millones de usuarios activos en redes sociales a finales de 2024 (DataReportal, 2024), que representan aproximadamente el 70,3 % de la población total. Esta adopción coincide con el promedio global (alrededor del 62 %-63 % de la población). El tiempo promedio dedicado a redes sociales por parte de los colombianos es de 3 horas y 25 minutos por día, lo que representa más del 38 % del tiempo total de pantalla (Comparitech, 2024). Pues bien, este dato ubicaría a Colombia muy por encima del promedio global (2 horas 21 minutos), e incluso del estadounidense (2 horas 9 minutos), como reflejo de la centralidad que tienen en la actualidad las plataformas digitales como ejes de socialización, entretenimiento e, incluso, información noticiosa en Colombia. Pero este uso intensivo de pantallas en el país no puede interpretarse de forma unidimensional, ya que, si bien, por un lado, expone oportunidades vinculadas a la digitalización del trabajo, la educación en línea, la democratización del acceso a la información y la expansión de las industrias culturales, plantea, por otro, riesgos significativos, como fatiga digital, deterioro de la salud mental, aislamiento social, adicción tecnológica y vulnerabilidad ante la desinformación.

Desde una perspectiva estructural el fenómeno en mención también refleja desigualdades territoriales y socioeconómicas, pues el acceso a la conectividad y a dispositivos de calidad no es uniforme en todo el territorio nacional. En este contexto, se vuelve urgente el desarrollo de estrategias públicas de bienestar digital, alfabetización crítica y políticas de infraestructura resiliente que garanticen un uso saludable y productivo de las tecnologías. Además, la academia y los centros de pensamiento deben asumir un rol protagónico en la generación de conocimiento sobre los efectos del tiempo digital prolongado, proponiendo marcos éticos, normativos y pedagógicos que articulen innovación tecnológica con desarrollo humano. En suma, el caso colombiano constituye un ejemplo paradigmático de

⁶ Según Comparitech (2024), el usuario promedio en Estados Unidos consulta su dispositivo móvil unas 159 veces al día, lo que equivale a una frecuencia de uso cercana a nueve veces por hora a lo largo del periodo en que permanece despierto. Este patrón refleja una creciente dependencia de la conectividad digital en las rutinas cotidianas.

la intensificación de la vida digital en América Latina. Su alto tiempo de pantalla refleja tanto las oportunidades como las contradicciones del ecosistema hipermediatizado contemporáneo, y ofrece una base empírica valiosa para la reflexión estratégica sobre el futuro digital del país. Por lo tanto, el análisis estratégico del entorno digital contemporáneo no puede prescindir de la comprensión de dichos ecosistemas, donde se negocian no solo la atención y la identidad, sino, cada vez más, la soberanía informacional.

Facebook sigue siendo la red social más grande del mundo, con 3.070 millones de usuarios activos mensuales en 2025 (Statista, 2025b). A pesar del surgimiento de plataformas más recientes, como TikTok o BeReal, el ecosistema Meta (que incluye también WhatsApp e Instagram) mantiene una presencia dominante en términos de alcance global. Como destaca el informe en mención, Facebook permite a los anunciantes, potencialmente, llegar a más de un tercio de la población adulta del planeta, lo que reafirma su valor estratégico en los ámbitos político, comercial y cultural. TikTok, por su parte, ha experimentado un ascenso meteórico, al alcanzar en 2025 los 1.590 millones de usuarios activos mensuales, y consolidarse como la red preferida de los públicos más jóvenes. Este crecimiento ha sido especialmente pronunciado en mercados emergentes, donde la penetración móvil y el acceso a datos económicos han facilitado su expansión (DataReportal, 2025a). El ecosistema global, sin embargo, no es uniforme: plataformas como Reddit (1.100 millones de usuarios mensuales) y Pinterest (553 millones) han consolidado comunidades específicas en torno a intereses temáticos, mientras que redes sociales regionales como Sina Weibo mantienen una fuerte presencia en China, con 591 millones de usuarios activos mensuales (Statista, 2025b).

En 2025 el equilibrio de poder digital global ha comenzado a desplazarse claramente al Asia, evidencia de que el centro de gravedad de internet ya no reside exclusivamente en Silicon Valley o Europa Occidental. Con más del 45,7 % de los usuarios de internet a nivel mundial, Asia (especialmente, en sus regiones oriental y sudoriental) se ha consolidado como el epicentro del crecimiento digital (Go-Globe, 2025). En términos absolutos, eso representa una comunidad digital de más de 1.380 millones de personas activas en línea, que están redefiniendo los patrones globales de consumo, comunicación y entretenimiento. Sin embargo, el auge de plataformas y servicios asiáticos es no solo cuantitativo, sino cualitativo, ya que empresas asiáticas como Tencent, ByteDance, Alibaba y Baidu han emergido como referentes globales en servicios digitales, desde redes sociales y mensajería hasta comercio electrónico e IA. Baidu, el principal motor de búsqueda chino, figura entre los sitios web más visitados del mundo según el *ranking* de

SimilarWeb (2025), y este protagonismo también es cada vez más visible en la mensajería digital, donde WeChat y QQ, ambas de Tencent, han consolidado ecosistemas cerrados de comunicación, pagos y servicios gubernamentales.

En el ámbito de las aplicaciones móviles, el dominio asiático es cada vez más evidente. Según LinkedIn (2025), nueve desarrolladores chinos se ubicaron en el top 30 mundial por volumen publicitario de aplicaciones móviles no relacionadas con videojuegos. Este fenómeno revela no solo la sofisticación del ecosistema digital chino, sino también su estrategia de internacionalización, especialmente hacia mercados en desarrollo. Pero uno de los sectores más dinámicos ha sido el de los videojuegos. En 2024 la región de Asia-Pacífico concentró el 53 % de los jugadores a nivel mundial, con un crecimiento interanual del 4 %, que alcanza, según eso, los 1.800 millones de usuarios (Icon-Era, 2024). Este avance ha sido particularmente notorio en el sudeste asiático, donde Filipinas, Vietnam, Tailandia e Indonesia lideran el uso de videojuegos móviles, debido a la masificación de los teléfonos inteligentes y planes de datos asequibles⁷. Tal como señala Newzoo (2024), más del 69 % de los usuarios globales de internet juegan en teléfonos móviles, lo que equivale a una comunidad global de más de 3.500 millones de jugadores activos mensualmente.

En 2024 el gasto a nivel global en videojuegos continuó creciendo de manera sostenida. Según datos de Newzoo (2024), la industria alcanzó los 187,7 mil millones de dólares, lo que marca un incremento del 2,1 % respecto al año anterior. Este auge es impulsado principalmente por el mercado de los juegos móviles, que representa más de la mitad del total. De hecho, el gasto en juegos móviles superó los 111 mil millones de dólares en 2024, por lo que consolida su recuperación después de dos años de declive (Dean, 2024a). A este fenómeno económico se suma la intensificación del consumo audiovisual vinculado a videojuegos. Newzoo (2024) revela que aproximadamente uno de cada cinco usuarios de internet entre los 16 y los 64 años ha visto transmisiones en vivo de videojuegos, y uno de cada siete ha asistido virtualmente a torneos de *e-sports*. Este tipo de interacción, antes marginal, se ha convertido en una experiencia social masiva con audiencias globales que rivalizan con eventos deportivos tradicionales.

En paralelo, otros nichos de mercado del comercio electrónico también han mostrado una expansión acelerada. Global Web Index (2024b) estima que tres cuartas partes de los usuarios de internet en todo el mundo compraron productos o servicios en línea al menos una vez al mes. Esta cifra es particularmente alta en países del sudeste asiático como Indonesia y Tailandia, al igual que en

⁷ Colombia ocupa el puesto 22 entre los usuarios que en el mundo gastan más tiempo en juegos de consola.

naciones europeas emergentes como Polonia⁸, donde el acceso móvil y la localización de contenidos han sido clave para la adopción del *e-commerce*. En ese sentido, Global Web Index (2024b) sostiene que la satisfacción de las necesidades lingüísticas y culturales de los consumidores es más determinante que el nivel de desarrollo económico para explicar las tasas de adopción. Por otro lado, si bien el dispositivo móvil se consolida como la herramienta predominante para las compras en línea, con una clara ventaja en comodidad y disponibilidad, muchos usuarios siguen utilizando *laptops* y computadores de escritorio, dependiendo del tipo de producto, la necesidad de comparar precios o el contexto de compra (Tigren, 2024). Esta convivencia de plataformas confirma que el comportamiento del consumidor digital es situacional y multicanal⁹.

A nivel global, el gasto promedio por comprador en comercio electrónico varía significativamente según el contexto económico y la madurez digital de cada país. En 2024 el comprador promedio en línea en Estados Unidos gastó 3.991 dólares anuales, el valor más alto a nivel mundial, seguido por Corea del Sur, con 3.806 dólares, y el Reino Unido, con 2.045 dólares (Tigren, 2024). Por otro lado, en las economías emergentes como Colombia, el gasto promedio anual por usuario fue de 812 dólares, con un gasto promedio por transacción de 49 dólares, impulsado principalmente por el acceso desde los dispositivos móviles, que representaron el 87 % del volumen de ventas digitales (Payments CMI, 2024). Cabe destacar que en 2024 el volumen del comercio electrónico en Colombia alcanzó los 52 mil millones de dólares, con una tasa de crecimiento anual compuesta proyectada del 16 % hasta 2027.

En China, uno de los mercados más dinámicos del mundo, el gasto promedio por usuario fue de 1.353 dólares, cifra aún por debajo de países como Canadá y Alemania (ECDB, 2024). El crecimiento es incluso más notable en regiones del sur de Asia, como la India, donde el gasto promedio ha aumentado en el 43 % desde 2018, aunque sigue siendo inferior a los 50 dólares anuales por persona, reflejo del potencial expansivo del comercio electrónico en contextos de alta penetración móvil, pero bajo poder adquisitivo (ECDB, 2024). Si bien los motores de búsqueda siguen siendo el canal principal de descubrimiento de productos para el 53 % de los compradores en línea a nivel global, entre los usuarios de 16 a 24 años las redes sociales han superado a los buscadores como el método más común para

⁸ Por su parte, Colombia ocupa el puesto 40 en el escalafón mundial, por encima de Rusia, Sudáfrica y Egipto, pero por debajo de países como Brasil, México y Argentina.

⁹ Los viajes, la categoría más grande por gasto del consumidor en línea, registraron un aumento del 8 % en 2024, y llegaron a ventas por el orden de los 2.500 millones de dólares (Global Web Index, 2024b).

iniciar procesos de compra, lo que evidencia un cambio generacional en los hábitos digitales (Global Web Index, 2024b).

En este contexto, el comercio electrónico ha mostrado señales del liderazgo asiático. Si en 2019 ya era llamativo que cinco de los 20 principales sitios web globales según Alexa (2020) fueran plataformas chinas de comercio, en 2025 esta tendencia se ha consolidado, pues, según datos de DataReportal (2025a), plataformas chinas como Tmall, JD.com y Pinduoduo vienen compitiendo directamente con Amazon en volumen de visitas, usuarios activos y festivales de consumo como el *Singles Day*, que en China ha superado en ventas al *Black Friday* estadounidense. En suma, el liderazgo digital de Asia ya no es una promesa, sino una realidad estructural que moldea la evolución del ciberespacio global. Desde la infraestructura y los algoritmos hasta las plataformas dominantes y los modelos de negocio, el ascenso de Asia redefine no solo el mapa digital, sino también las reglas estratégicas del juego.

El video en línea se ha convertido en una de las actividades más ubicuas entre los usuarios de internet a nivel global. De acuerdo con datos recientes, el 52,3 % de los internautas utilizan la red para ver videos, programas de televisión y películas, lo que la posiciona como una de las principales fuentes de la conexión digital a nivel global (DataReportal, 2024). En este orden de ideas, YouTube sigue liderando como la plataforma de video más utilizada a nivel global, con más de 2,7 mil millones de usuarios activos mensuales en 2025 (DataReportal, 2025a). Y se estima que diariamente los usuarios de YouTube consumen colectivamente más de mil millones de horas de contenido en la plataforma, lo que ha llevado a que esta plataforma supere a la televisión tradicional en términos de tiempo de visualización en dispositivos de sala en Estados Unidos (MarketWatch, 2024). De manera paralela, el consumo de contenido televisivo a través de servicios de *streaming* ha experimentado un aumento sostenido. En 2024 el 76 % de los consumidores a nivel mundial ve a diario televisión en línea o contenidos en *streaming*, según lo cual dedican un promedio de una hora y 22 minutos al día a estas actividades (Global Web Index, 2024). Dicha evolución en los hábitos de consumo refleja una clara preferencia por plataformas de suscripción como Netflix, Prime Video y Hulu, los cuales lideran el sector global de servicios de video bajo demanda por suscripción, y consolidan así un modelo de distribución de contenidos cada vez más personalizado y bajo control del usuario (BB Media, 2024).

En el ámbito de las aplicaciones móviles, las plataformas de video mantienen su predominio. Solo en 2024 se registraron más de 110 mil millones de descargas de aplicaciones en todo el mundo, con una proporción significativa

correspondiente a *apps* de video y entretenimiento (TechJury, 2024). Esta tendencia subraya la creciente dependencia del contenido audiovisual accesible desde dispositivos móviles, impulsada por la portabilidad, la interfaz optimizada para el usuario y el ecosistema de datos móviles de alta velocidad. Por lo tanto, el panorama digital es claramente marcado por un incremento sostenido en el consumo de video en línea, tanto en términos de tráfico de datos móviles como en la adopción de plataformas de *streaming* y aplicaciones móviles. Esta tendencia revela una transformación estructural en los hábitos de consumo cultural, con una fuerte inclinación hacia formatos visuales, accesibles y personalizados, que configuran el presente y el futuro de la experiencia mediática global.

En 2024 el mercado global de correo electrónico¹⁰ empresarial basado en la nube continúa su expansión, impulsado por la creciente adopción de soluciones digitales y la necesidad de comunicaciones seguras y eficientes. Se estima que este mercado alcanzó un valor aproximado de 6.500 millones de dólares, con proyecciones que indican un crecimiento sostenido hasta alcanzar los 12.700 millones de dólares para 2033, lo que representa una tasa de crecimiento anual del 8,1 % (Consejo Business Intelligence, 2024). Ese crecimiento es atribuido a las ventajas que ofrecen los servicios de correo electrónico en la nube, tales como una alta protección contra amenazas, soporte para dispositivos móviles, acceso remoto eficiente y costos operativos competitivos. Además, la integración de tecnologías avanzadas como la IA y el aprendizaje automático ha mejorado la capacidad de estas plataformas para detectar y prevenir amenazas en tiempo real (Market Research Future, 2024).

Sin embargo, a pesar de estos avances, la privacidad y la seguridad de los datos siguen siendo preocupaciones significativas para los usuarios. Según el Digital News Report 2024, del Reuters Institute (2024), el 59 % de los encuestados a nivel mundial expresó preocupación por la dificultad propia de distinguir entre las noticias reales y las falsas en línea, un aumento de tres puntos porcentuales respecto al año anterior. Este escepticismo se extiende al ámbito de las comunicaciones digitales, donde los usuarios demandan mayor transparencia y control sobre el uso de su información personal. En respuesta a dichas inquietudes, las empresas proveedoras de servicios de correo electrónico en la nube están implementando

¹⁰ El servicio de correo electrónico Hotmail fue creado en 1996, por Sabeer Bhatia y Jack Smith, y adquirido por Microsoft en 1997, para integrarse posteriormente al ecosistema de servicios que hoy operan bajo la marca Outlook. Gmail, lanzado por Google en 2004, introdujo innovaciones significativas en almacenamiento masivo gratuito, búsqueda integrada y arquitectura basada en la nube, lo que transformó el modelo competitivo del correo electrónico. Para 2025 Gmail superaba los dos mil millones de usuarios activos, y consolidaba así una elevada concentración de infraestructura comunicacional en manos de grandes plataformas tecnológicas.

medidas más estrictas de protección de datos y cumpliendo con regulaciones internacionales como el Reglamento General de Protección de Datos. Estas acciones buscan fortalecer la confianza del usuario y garantizar la integridad de las comunicaciones empresariales en un entorno digital cada vez más complejo (Newman et al., 2019).

En 2024 el uso de bloqueadores de anuncios sigue siendo una práctica extendida entre los usuarios de internet, aunque ha mostrado una ligera disminución, comparado con años anteriores. Según datos recientes, el 31,5 % de los usuarios globales de internet entre los 16 y los 64 años emplean bloqueadores de anuncios, al menos ocasionalmente, lo que representa una baja respecto al 37 % reportado en 2021 (Dean, 2024b). Esta reducción sugiere una mayor tolerancia hacia la publicidad digital, posiblemente motivada por mejoras en su personalización y menor intrusividad. Las razones más frecuentes para bloquear anuncios siguen estando relacionadas con la experiencia de navegación y la privacidad. Un informe de Funnel (2024) revela que el 63,2 % de los usuarios bloquean anuncios por considerarlos excesivos; el 53,4 %, porque interrumpen la navegación, y el 40,3 %, debido a preocupaciones sobre el uso de sus datos personales. Estos datos confirman que la sobrecarga publicitaria sigue siendo una fuente de frustración para los internautas, incluso más que el temor a la vigilancia digital directa.

Al mismo tiempo, persiste la “paradoja de la privacidad digital”, que explica cómo, si bien los usuarios se muestran crecientemente preocupados por la seguridad de su propia información, tienden, paradójicamente, a adoptar tecnologías que, precisamente, amplifican el rastreo de datos personales. El caso de dispositivos inteligentes para el hogar es paradigmático. De acuerdo con Strategic Market Research (2024), en 2024 existen más de 422 millones de usuarios de hogares inteligentes en el mundo, y se proyecta que esa cifra alcance los 478 millones de usuarios a finales de 2025. Estos dispositivos, que incluyen asistentes de voz, cámaras de seguridad, termostatos inteligentes y electrodomésticos conectados, están diseñados para recolectar datos de uso, comportamiento, e incluso, voz en tiempo real, lo que plantea dilemas éticos sobre la privacidad doméstica.

Como explica Kemp (2025), muchas personas aceptan voluntariamente estas tecnologías por su funcionalidad, comodidad y capacidad de automatización, aun a costa de entregar grandes volúmenes de datos personales. Así la tecnología redefine no solamente los límites de lo privado, sino también la percepción cultural de la vigilancia cotidiana y del consentimiento digital (Zuboff, 2019). Entonces, mientras que las herramientas de bloqueo de anuncios siguen siendo utilizadas como un mecanismo de defensa frente a la saturación publicitaria y la opacidad en la gestión de datos, la creciente incorporación de dispositivos inteligentes en la

vida cotidiana revela una aceptación progresiva de nuevas formas de exposición digital; por ende, esta tensión entre control individual y funcionalidad tecnológica es una de las dinámicas más complejas de la era informacional contemporánea.

Cartografía del ciberespacio: terreno, nodos y flujos digitales

A pesar de su vertiginosa evolución durante las últimas dos décadas, internet sigue siendo una infraestructura en expansión constante¹¹. Si bien se denomina a internet una “red”, en sentido tanto técnico como geográfico, su naturaleza no deriva directamente de las redes tradicionales de la industria telefónica o televisiva, sino que debe entenderse como una creación profundamente arraigada en la lógica computacional. En este sentido, su evolución no depende del modelo de transmisión lineal propio de los medios del siglo XX, sino de los ritmos acelerados de innovación que caracterizan a la industria informática contemporánea. Para mantenerse relevante y operativa frente a las demandas crecientes de procesamiento, tráfico y almacenamiento, internet debe continuar su expansión a la velocidad del desarrollo digital global.

Determinar con exactitud el tamaño actual de internet es una tarea compleja, dado su carácter dinámico y descentralizado. Sin embargo, para mayo de 2025 se estimaba que la Web indexada albergaba aproximadamente 1.200 millones de páginas (Exploding Topics, 2025a), una cifra que varía constantemente a medida que nuevos sitios web emergen y otros desaparecen. Esta porción visible de internet, conocida como Surface Web, corresponde al conjunto de páginas indexadas por motores de búsqueda convencionales, como Google, Bing, Yahoo, Baidu o Yandex, y constituye la parte accesible para cualquier usuario sin necesidad de credenciales especiales ni herramientas específicas (Álvarez & Zambrano, 2017). Es, por tanto, la “fachada pública” del ciberespacio, que oculta tras de sí otras capas más profundas y menos visibles de la arquitectura digital global.

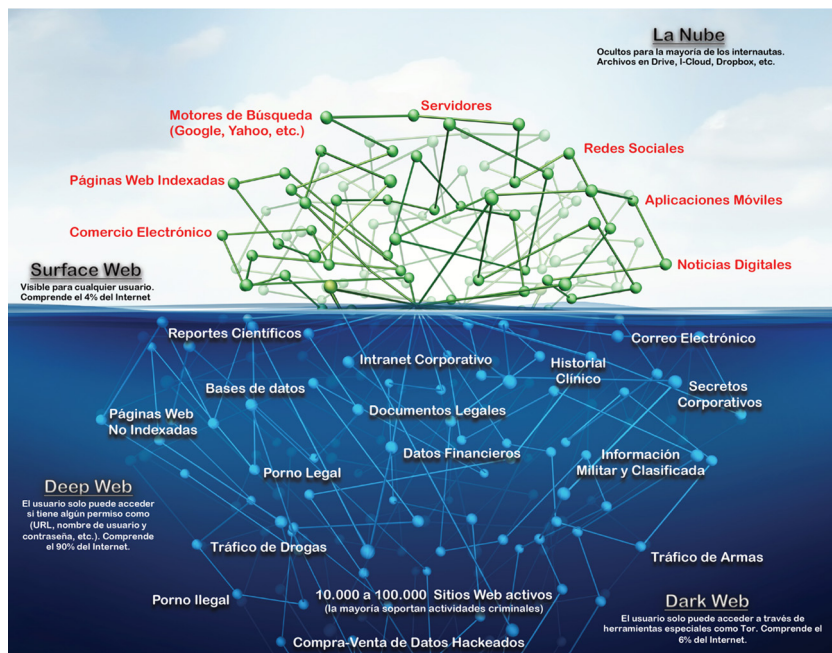
Se estima que más del 90 % del contenido de internet no es accesible mediante buscadores convencionales, dado que una gran proporción de sitios web se encuentra protegida por muros de pago (*paywalls*), o sistemas de seguridad que requieren credenciales de acceso, como nombres de usuario y contraseñas. Esta porción no indexada forma lo que se conoce como la Deep Web: es decir, el

¹¹ Internet se ha duplicado en tamaño cada año desde 2012.

conjunto de recursos digitales que, si bien legítimos y legales, no están disponibles para el rastreo automatizado de motores de búsqueda como Google o Bing. Sin embargo, dentro de tan vasta infraestructura invisible se encuentra un subconjunto más restringido y deliberadamente oculto: la Dark Web, cuya extensión estimada representa apenas el 6 % del total de internet, aunque su tamaño real sigue siendo incierto (Finklea, 2017).

La Dark Web se define como la parte del ciberespacio que ha sido intencionalmente excluida de los mecanismos convencionales de indexación, y que opera a través de protocolos de anonimato como Tor (The Onion Router), los cuales permiten el enmascaramiento de direcciones IP y dificultan la trazabilidad del tráfico web (Bartlett, 2014). Si bien este entorno es frecuentemente asociado con actividades ilícitas, como mercados negros, foros criminales o distribución de material prohibido, también cumple funciones legítimas, ya que permite a disidentes políticos, periodistas y organismos de seguridad mantener comunicaciones seguras y protegidas frente a los regímenes represivos o las amenazas cibernéticas. Incluso, algunos Estados lo utilizan con fines de inteligencia, rastreo de redes delictivas o infiltración de operaciones en la economía digital clandestina.

Figura 1. Niveles de internet



Fuente: elaboración propia.

Por ende, la combinación entre el carácter dinámico de la Web de superficie y la imposibilidad de cuantificar con exactitud la magnitud de la Web profunda y la Web oscura explica por qué resulta tan complejo estimar el tamaño real de internet. A esto se suma el hecho de que, si bien se contabilizan aproximadamente 1.200 millones de sitios web en la actualidad, cada uno de ellos puede contener múltiples páginas internas, lo que multiplica exponencialmente el volumen total de contenido disponible en línea. Es importante mencionar que esa estructura fragmentada, cambiante y parcialmente inaccesible convierte a internet en un sistema de información de escala casi indeterminada, cuya verdadera dimensión escapa de los métodos convencionales de medición. En ese sentido, tan solo Google (sin incluir a Dropbox), Amazon, Microsoft y Facebook almacenan colectivamente al menos 1.200 *petabytes* (PB)¹² (Exploding Topics, 2025b). Poniéndolo en perspectiva, una canción de 3 minutos usa aproximadamente 3 megabytes (MB) de almacenamiento, lo cual significaría que a 1.200 PB esas cuatro compañías tienen suficientes datos para 400 billones de canciones o 1,2 billones de minutos de música (más de 2.200 millones de años de audio)¹³.

Anatomía técnica de internet: tamaño, tráfico y arquitectura digital

Para dimensionar la magnitud de internet resulta útil analizar el volumen de datos que se transfieren globalmente a través de la Web. Se estima que para 2025 se habrán generado aproximadamente 181 *zettabytes* (ZB) de datos a nivel mundial (Exploding Topics, 2025b). Dado que 1 ZB equivale a 1.000 *exabytes* (EB) o un sextillón de *bytes*¹⁴, este volumen representa una escala casi inconcebible de información. Para ilustrarlo, un solo ZB contendría suficiente contenido en video de alta definición para reproducirse de forma continua durante 36.000 años¹⁵ (Live Science, 2016). Si la cantidad de datos transferidos globalmente a lo largo de 2025 será de 181 ZB, se transferirán aproximadamente 181.000 EB de datos a nivel global en 2025. Según algunas estimaciones técnicas (Live Science, 2016), la capacidad máxima teórica de la infraestructura global de internet rondaría el millón de

¹² Mil *gigabytes* (GB) equivalen a un *terabyte* (TB), lo que, a su vez, corresponde a un millón de megabytes (MB). En consecuencia, 1.200 *petabytes* (PB) representan 1,2 millones de *terabytes* o, lo que es lo mismo, 1,2 billones de *megabytes*.

¹³ Si se descargara toda la Web, tomaría aproximadamente 11 billones de años hacerlo.

¹⁴ Es decir, 21 ceros después del 1.

¹⁵ Si se asumiera que cada ladrillo en la Gran Muralla China es un *gigabyte*, se podrían construir 258 grandes murallas chinas con un solo *zettabyte*.

EB (o 1.000 ZB). Y 1 EB equivale a 1 billón de billones de bytes (18 ceros después del 1)¹⁶. Esta cifra sirve como un marco de referencia para comprender que, si bien el tráfico de datos crece de forma exponencial, el sistema todavía tiene margen operativo antes de alcanzar un umbral crítico de saturación.

En la era contemporánea, el volumen de datos que se genera, transmite y consume a diario ha alcanzado proporciones sin precedentes, lo cual consolida a la información digital como el insumo céntrico de la economía, la cultura y la geopolítica globales. Según Exploding Topics (2025b), cada día se crean alrededor de 402,74 millones de TB de datos, lo que equivale a 0,4 ZB diarios o más de 147 ZB al año; este crecimiento exponencial responde no solo a una mayor cantidad de usuarios y dispositivos conectados, sino a la intensificación de las interacciones digitales y al auge de las plataformas audiovisuales, redes sociales y servicios en la nube, así como al de tecnologías emergentes como el IoT y la IA.

Para contextualizar la magnitud, basta con señalar que en 2010 el volumen global de datos era de apenas 2 ZB, mientras que las proyecciones para 2025 estiman un total de 181 ZB generados, lo cual representa un incremento de más del 9.000 % en menos de dos décadas. Este ritmo acelerado implica que el 90 % de los datos del mundo se han creado en los últimos dos años, y pone en evidencia el carácter vertiginoso de la llamada “infoesfera global”. El tráfico de datos no se distribuye de manera uniforme, sino que se concentra sobre todo en ciertas categorías: el contenido en video representa el 53,7 % del total, seguido por redes sociales (12,7 %) y videojuegos (9,9 %), que en conjunto absorben más de tres cuartas partes del tráfico mundial (Sandvine, 2022). Plataformas como TikTok, YouTube y Netflix son responsables de una parte significativa de este fenómeno, donde el consumo de video en alta definición (o incluso en 4K) multiplica la demanda de ancho de banda y almacenamiento.

El impacto de esta sobrecarga informacional no es meramente cuantitativo; también plantea desafíos estructurales para la gobernanza digital, la sostenibilidad energética y la distribución del poder tecnológico. A nivel físico, este ecosistema se sustenta en una red global de infraestructura compuesta por cables submarinos, centros de datos, servidores distribuidos y nodos de interconexión. Estados Unidos lidera, con más de 5.426 centros de datos, diez veces más que

¹⁶ Una Biblia promedio contiene cerca de 3.116.480 caracteres, lo que equivale a aproximadamente 3,1 MB de información en formato de texto. Por tanto, un EB puede almacenar más de 320.000 millones de biblias. Para visualizar esta magnitud, basta considerar que se necesitan alrededor de 96 millones de biblias apiladas para alcanzar la distancia entre la Tierra y la Luna. En consecuencia, un EB permitiría formar más de 3.300 pilas completas de biblias que llegarían hasta la superficie lunar.

Alemania, el segundo país del *ranking* global, seguido por el Reino Unido, Francia, Australia, Holanda, Rusia, Italia, México, Polonia, España, China, Japón y Brasil (Statista, 2025c). Esta concentración territorial revela desigualdades en la capacidad de procesamiento, soberanía digital y resiliencia cibernética, al tiempo que consolida la hegemonía tecnológica de ciertos Estados y corporaciones.

La distribución regional del tráfico y la capacidad de almacenamiento también presenta desequilibrios notables. Mientras algunas economías emergentes como la India, Brasil y México aumentan su presencia digital, su infraestructura crítica aún está lejos de alcanzar niveles comparables con los de Europa o América del Norte. Este desbalance afecta no solo el acceso equitativo al conocimiento y al comercio digital, sino también la capacidad de estos países para proteger su propia soberanía informacional en un contexto de ciberguerras latentes y espionaje industrial. A ello se suma el hecho de que el crecimiento de datos no es neutral. En otras palabras, genera externalidades ambientales (por el consumo energético de los centros de datos), vulnerabilidades de seguridad (por la expansión de la superficie de ataque) y dilemas regulatorios en torno a la privacidad, la propiedad intelectual y el control algorítmico de la información.

Por otro lado, el análisis de las actividades digitales por minuto ofrece una radiografía más concreta del comportamiento cibernético global. Según PCMag (2024), los 60 segundos promedio de actividad en internet ofrecen una visión condensada del comportamiento digital a escala planetaria, lo cual revela no solo el volumen masivo de datos que circulan, sino también la creciente centralidad de ciertas plataformas y rutinas tecnológicas en la vida cotidiana, profesional y económica. A finales de 2024 y comienzos de 2025 se enviaban cada minuto más de 251 millones de correos electrónicos¹⁷ y se realizaban aproximadamente 5,9 millones de búsquedas en Google, lo que evidencia el papel decisivo del correo electrónico como herramienta de comunicación profesional y personal, al igual que la

¹⁷ En la era de la hiperconectividad el correo electrónico sigue siendo una de las herramientas fundamentales de comunicación en los entornos laborales, pero también una de las principales fuentes de sobrecarga informacional. Diversos estudios han evidenciado que el empleado de oficina promedio envía y recibe aproximadamente 120 correos electrónicos por día, lo que representa entre 30.000 y 43.800 correos electrónicos al año, dependiendo de si se calcula sobre días laborales efectivos o sobre el total del calendario anual (Radicati Group, 2023). Este volumen constante de mensajes contribuye no solo a la saturación de la atención y a la fragmentación del tiempo de trabajo, sino también a una cultura organizacional de inmediatez y respuesta continua que obstaculiza la concentración profunda, la toma estratégica de decisiones y el bienestar digital. En términos estructurales, la dependencia del correo electrónico como canal principal de comunicación asíncrona revela tanto la inercia de modelos comunicativos del siglo XX como la necesidad de repensar los flujos informativos en contextos altamente digitalizados. La gestión eficiente del correo electrónico (mediante filtros automatizados, IA y rediseño organizacional) se ha convertido en un reto estratégico para las organizaciones que buscan equilibrar conectividad, eficiencia y salud mental en el entorno laboral.

función hegemónica de Google como interfaz cognitiva global. Esta concentración de consultas convierte al motor de búsqueda no solo en un nodo clave de acceso a la información, sino también en un dispositivo de mediación del conocimiento y del pensamiento digitalizado.

En el contexto de la acelerada transformación digital, la IA ha dejado de ser una promesa tecnológica futura para convertirse en una infraestructura activa que moldea múltiples dimensiones de la vida contemporánea. El informe *Data Never Sleeps: AI Edition*, publicado por Domo (2024), proporciona una instantánea reveladora sobre lo que ocurre cada 60 segundos en el ecosistema algorítmico global, que evidencia no solo el volumen de interacciones, sino también las dinámicas estructurales de automatización, creación simbólica, dependencia tecnológica y consumo cognitivo que definen la nueva economía digital.

En ese orden de ideas, Google AI Gemini (la nueva plataforma de IA generativa del ecosistema Alphabet) recibió más de 8.500 visitantes cada minuto, por lo cual se consolida como uno de los puntos de entrada hacia la automatización de tareas cognitivas, consulta inteligente y generación de contenido algorítmico en tiempo real. Asimismo, ChatGPT procesa 6.944 instrucciones, o *prompts*, cada 60 segundos, lo que refleja su centralidad no solo como plataforma conversacional, sino también como herramienta de redacción, resolución de problemas y generación de código en tiempo real. En paralelo, DALL·E crea 1.389 imágenes por minuto, mientras que otras plataformas de generación visual producen 19.028 imágenes adicionales mediante algoritmos de texto a imagen (Domo, 2024), lo que subraya la consolidación de la IA generativa como fuerza productiva simbólica (Zuboff, 2019). Este fenómeno no se limita al contenido estático, pues cada minuto se generan 7.431 minutos de video mediante IA, cifra que refleja el auge del video sintético como nuevo formato de expresión, comunicación y comercialización visual (Farhadi et al., 2022).

El uso extendido de estas herramientas también tiene efectos mensurables en términos de productividad. De acuerdo con Domo (2024), los empleados que utilizan ChatGPT en tareas cotidianas logran ahorrar colectivamente alrededor de 467.000 horas de trabajo por minuto, lo que indica una delegación creciente de funciones cognitivas en modelos automatizados y el inicio de una reorganización estructural del trabajo intelectual. Esa externalización algorítmica de la agencia humana también se manifiesta en la interacción cotidiana con asistentes virtuales: por ejemplo, Siri respondió a más de 1.050.000 consultas cada minuto, lo que posiciona al asistente de Apple como uno de los principales intermediarios cognitivos en la vida cotidiana digital (PCMag, 2024).

Sin embargo, cabe señalar que no todo el impacto de esa infraestructura algorítmica es intangible. Cada minuto la operación de modelos como ChatGPT requiere 185 galones de agua para el enfriamiento de sus supercomputadores, lo que visibiliza una huella hídrica significativa y usualmente subestimada en análisis sobre sostenibilidad digital (Chesney et al., 2023). Desde el punto de vista financiero, el gasto estimado en servicios y tecnologías de IA asciende a 293.000 dólares por minuto, lo que proyecta un mercado altamente rentable, concentrado y en expansión exponencial (Domo, 2024). Pero el panorama también incluye elementos críticos relacionados con la veracidad, ética y seguridad informacional: por ejemplo, cada minuto se detectan 52 trabajos académicos potencialmente plagiados mediante IA, lo que plantea interrogantes profundos sobre la autoría, la originalidad y la integridad del conocimiento producido. Asimismo, se estima que se crea al menos una *deepfake* por minuto (Domo, 2024), lo cual representa un riesgo sistémico para la gobernanza informacional y para los procesos democráticos, al facilitar la manipulación audiovisual de sujetos, contextos y discursos (Kadlečová, 2024).

YouTube, por su parte, recibió más de 500 horas de contenido audiovisual cargado cada minuto, y registró aproximadamente 3,5 millones de visualizaciones de video por minuto (PCMag, 2024), lo que la convierte en una de las mayores plataformas de archivo y circulación audiovisual en la historia de la humanidad. Esta magnitud no solo refleja el volumen masivo de producción y consumo de contenidos, sino también el papel clave que desempeña YouTube como infraestructura cultural global en la era digital. TikTok, la red social con el crecimiento más acelerado en usuarios y volumen de tráfico global, reporta que sus usuarios suben más de 16.000 videos cada minuto (PCMag, 2024), mientras que en el mismo lapso se visualizaron más de 167 millones de clips. Estas cifras evidencian no solo una reconfiguración radical en los patrones de consumo de contenido, sino también una transformación en la arquitectura temporal de la atención digital. La lógica de TikTok se basa en la producción y circulación de microvideos diseñados para captar fragmentos breves de atención, operando en ciclos de reproducción algorítmica potencialmente infinitos. En ese entorno el contenido se vuelve efímero, adictivo y profundamente personalizado, y altera las nociones tradicionales de narrativa, tiempo y profundidad en la experiencia informacional contemporánea.

Simultáneamente, cada 60 segundos se comparten 97 millones de mensajes en WhatsApp, se envían 3,3 millones de *snaps* en Snapchat, se publican 347.222 historias y 65.972 fotografías en Instagram, y se generan cerca de 350.000 *tuits* en X (antes Twitter), según informa PCMag (2024). Como puede observarse, estos

flujos masivos de comunicación han configurado en los últimos años un ecosistema digital global caracterizado por la inmediatez, la imagen y la brevedad, donde las plataformas priorizan formatos efímeros y de bajo umbral atencional por encima de las estructuras tradicionales de comunicación secuencial. En otras palabras, más que simples indicadores de uso, estas cifras reflejan los rasgos de una sociedad hipertextual y emocionalmente acelerada, donde la velocidad de interacción y la lógica viral del contenido sustituyen los modelos lineales de expresión e intercambio informativo.

En ese mismo intervalo de un minuto, los suscriptores de Netflix transmitieron cerca de 362.962 horas de contenido cada 60 segundos, mientras que se publicaron más de 138,9 millones de *reels* combinados entre Facebook e Instagram (PCMag, 2024). Estos datos ponen de relieve no solo la omnipresencia de las plataformas digitales en la vida cotidiana, sino también su papel estructural en la configuración de una nueva economía de los datos, donde el valor no reside únicamente en el contenido generado, sino en su trazabilidad, analítica e instrumentación, ya sea con fines comerciales, conductuales o políticos. Por consiguiente, en este entorno y en cada interacción, cada segundo de visualización y cada clic representan no solo una experiencia mediática, sino una unidad cuantificable en la arquitectura del poder algorítmico contemporáneo.

En el ámbito profesional, alrededor de 9.000 usuarios postulan a ofertas laborales en LinkedIn cada minuto (PCMag, 2024), lo que refleja la creciente digitalización del mercado de trabajo y la intermediación algorítmica del talento a través de plataformas especializadas. En paralelo, las herramientas de colaboración digital han adquirido una centralidad estratégica en la organización empresarial. Microsoft Teams, por ejemplo, reportó en 2024 un volumen diario superior a los 229 millones de minutos de reuniones (PCMag, 2024), lo que equivale a un promedio de aproximadamente 159.000 minutos de interacción virtual cada 60 segundos. Esta cifra evidencia el grado de integración alcanzado por los servicios de videoconferencia y productividad en la rutina operativa contemporánea. En el mismo intervalo Zoom alojó cerca de 858 seminarios web por minuto, mientras que 288 personas descargaban la aplicación, y consolidaban así su presencia en un ecosistema laboral cada vez más remoto, flexible y distribuido (PCMag, 2024). Por consiguiente, tanto Teams como Zoom se han convertido en infraestructuras digitales esenciales para garantizar la continuidad de las operaciones, coordinación de equipos globales y adaptación temporal de los modelos de trabajo frente a la expansión del entorno virtualizado.

Es difícil proporcionar una cifra exacta sobre la cantidad total de horas de música transmitidas en Spotify cada 60 segundos, ya que la plataforma no publica oficialmente este dato de forma desagregada y en tiempo real. Sin embargo, es posible hacer estimaciones razonables a partir de información disponible públicamente. De acuerdo con la Federación Internacional de la Industria Fonográfica, un usuario activo promedio dedica aproximadamente 25 horas mensuales a escuchar música en Spotify. Considerando que la plataforma tiene una base global de al menos 100 millones de usuarios activos (una cifra conservadora frente a su número total de suscriptores), esto implicaría un consumo agregado cercano a 2.500 millones de horas de música por mes. Si se distribuye ese volumen total en el número promedio de minutos que tiene un mes (aproximadamente 44.640) se obtiene una estimación aproximada de 558.000 horas de música transmitidas por minuto en la plataforma.

No obstante, esta proyección debe interpretarse con cautela, pues presupone que todos los usuarios se mantienen activos y escuchan de forma constante, lo cual no necesariamente refleja la realidad del comportamiento de consumo, que es altamente variable según la región, el perfil demográfico y la plataforma utilizada (por ejemplo, móvil, escritorio o dispositivos conectados). En síntesis, aunque no es posible establecer con precisión el volumen de horas transmitidas por minuto en Spotify, se puede afirmar que, dada su extensión global y elevada tasa de uso, la plataforma genera un flujo continuo y masivo de consumo musical, que la convierte en una de las principales infraestructuras culturales de la era digital. Este fenómeno no solo transforma las prácticas de escucha, sino que también reconfigura las dinámicas económicas, algorítmicas y simbólicas de la industria musical contemporánea.

Asimismo, cada minuto se deslizan (*swipes*) más de un millón de perfiles en Tinder (PCMag, 2024), una cifra que evidencia no solo la digitalización acelerada del ocio y de las interacciones sociales, sino también la consolidación de una intimidad algorítmica, donde los vínculos afectivos y el deseo son cada vez más mediados por plataformas digitales. Este fenómeno representa una transformación profunda en las formas de relacionamiento humano, ahora reorganizadas por sistemas de recomendación automatizada, filtros de compatibilidad y patrones de consumo emocional, propios de una lógica *tecnomediada* que convierte la búsqueda de pareja en una experiencia fragmentada, cuantificable y *gamificada*.

Paralelamente, el mismo ecosistema digital que habilita esas nuevas formas de contacto también expone a sus usuarios a riesgos estructurales en materia de privacidad y seguridad informacional, ya que cada 60 segundos se comprometen

aproximadamente 4.080 registros personales como resultado de brechas de datos, lo que se traduce en más de 5,8 millones de registros vulnerados diariamente (PCMag, 2024). Esta cifra pone en evidencia la fragilidad de los sistemas digitales ante ciberataques y filtraciones masivas, los cuales se han convertido en eventos rutinarios en la vida digital contemporánea. Así, la expansión de la conectividad y personalización algorítmica también conllevan una exposición creciente de las personas donde su vida íntima, emocional y financiera circula permanentemente por infraestructuras que no siempre garantizan su protección.

En términos económicos, las cifras son también significativas. Durante el Cyber Week los compradores globales gastaron más de 43,6 millones de dólares por minuto, un indicador que subraya la potencia del comercio electrónico como motor económico a escala planetaria. En cada minuto de 2024 Amazon procesa compras por más de 443.000 dólares, mientras que Venmo transfiere más de 437.000 dólares en pagos entre usuarios (PCMag, 2024). Esto muestra cómo las plataformas de comercio electrónico y pagos digitales ya no son auxiliares del sistema económico, sino infraestructuras financieras de facto operando con una inmediatez que redefine los flujos monetarios y las relaciones de consumo.

Este panorama sobre lo que ocurre en internet cada 60 segundos no solo ilustra la magnitud y densidad del tráfico digital, sino que plantea interrogantes críticos sobre infraestructura, gobernanza, soberanía y sostenibilidad en la era de la hiperconectividad. En efecto, la cantidad de datos generados, procesados y transferidos por segundo exige que funcionen redes de almacenamiento, cómputo y transmisión de escala planetaria, lo cual incrementa de forma sostenida la demanda energética y ayuda a la concentración tecnológica en manos de un número limitado de actores corporativos y geopolíticos. A su vez, la distribución desigual del acceso, la conectividad y la infraestructura digital amplifica las brechas estructurales entre regiones, países e individuos, y así refuerza dinámicas de exclusión y dependencia que van más allá del simple acceso a internet.

Desde una perspectiva crítica, este minuto hiperdenso (donde cada interacción digital se multiplica exponencialmente) refleja la aceleración del capitalismo de datos (Zuboff, 2019), un sistema en el que cada comportamiento es rastreado, cada segundo de atención es monetizado y cada clic genera valor económico en arquitecturas algorítmicas opacas. En ese ecosistema las plataformas digitales operan como infraestructuras invisibles de mediación económica, cultural y subjetiva determinando qué contenidos se visibilizan, qué vínculos se fortalecen y qué decisiones se automatizan. Por tanto, comprender lo que ocurre en internet a cada

instante no es un simple ejercicio estadístico, sino una ventana hacia la reconfiguración profunda del poder, del tiempo y de la experiencia humana.

Este ecosistema algorítmico global opera de manera masiva, permanente y multisectorial, afecta dimensiones que van desde la producción cultural hasta el empleo y desde la privacidad hasta el medio ambiente, pasando por la seguridad, la ética y la política. Lo que sucede en un solo minuto en el universo digital —y particularmente, en el ámbito de la IA— ofrece no solo una visión cuantitativa del fenómeno, sino también una advertencia cualitativa sobre los riesgos de delegar procesos humanos esenciales en sistemas computacionales autónomos. Comprender esta realidad es clave para diseñar marcos regulatorios eficaces, arquitecturas institucionales adaptativas y horizontes éticos claros, que aseguren que la revolución algorítmica complemente y potencie los valores humanos fundamentales, en vez de subordinarlos.

Por ende, el crecimiento exponencial de los datos no debe interpretarse como un fenómeno aislado ni meramente técnico: constituye la manifestación visible de una transformación estructural en las formas contemporáneas de producción, comunicación y ejercicio del poder. El reto para los Estados, las organizaciones internacionales y la comunidad académica radica en desarrollar normativas robustas, infraestructuras resilientes y capacidades estratégicas soberanas, que permitan canalizar esta avalancha de datos hacia el bienestar colectivo, en vez de profundizar las asimetrías tecnológicas o consolidar nuevas formas de dependencia.

En definitiva, la era digital ha alcanzado, para 2025, un umbral de expansión sin precedentes. Según Ericsson (2024), el tráfico mensual global de datos móviles alcanzó un promedio de 157,16 EB para finales de 2024. Esto equivale a un total anual superior a 1.885 EB, o 1.885.920 PB. Es decir, más de 1,8 mil millones de TB de información transmitida en apenas un año. Para dimensionar esa cifra vale la pena traducirla en una imagen tangible: ¿qué sucedería si intentáramos almacenar ese volumen de información en una tecnología obsoleta como los disquetes? Pues bien, el clásico disquete de 3½ pulgadas, popular en las décadas de 1980 y 1990, tenía una capacidad máxima de 1,44 MB. Al convertir los 1.885 EB de tráfico móvil a MB¹⁸ obtenemos un total de 2.023.967.674.368.000 MB. Si cada disquete almacena 1,44 MB se necesitan más de 1,4 billones de disquetes para contener el tráfico anual móvil de datos de 2025.

Para mayor claridad, considérese el grosor de un disquete: aproximadamente 3 mm (0,003 metros). Por lo tanto, al apilar 1,4 billones de disquetes el resultado es

¹⁸ 1 exabyte = 1.073.741.824 megabytes.

una columna de 4.071.000 km de altura. Este dato es particularmente revelador si lo comparamos con escalas astronómicas; por ejemplo, la distancia promedio entre la Tierra y la Luna es de 384.400 km, por lo que la altura de la pila de disquetes (4.071.000 km) sería más de diez veces la distancia Tierra-Luna. Esa distancia representaría el 2,7 % de una *unidad astronómica* (UA): es decir, la distancia entre la Tierra y el Sol, que es de 149,6 millones de km (Álvarez et al., 2019b). Es también 70 veces mayor que la órbita geoestacionaria, que se encuentra a 35.786 km sobre el ecuador terrestre. Y aunque no alcanzaría ningún planeta del sistema solar, la misma pila virtual de datos penetraría profundamente el espacio interplanetario. Esto permite visualizar, no solo la magnitud del ecosistema digital móvil, sino también la intensidad con que los seres humanos producen, transmiten y consumen información en la vida cotidiana. Como afirma Ensmenger (2010), la infraestructura digital contemporánea “no puede separarse de la historia de su propia expansión material, ni de la lógica de crecimiento que la impulsa” (p. 93).

Por consiguiente, la metáfora de la pila de disquetes que se extiende más allá de la órbita lunar no es solo una curiosidad técnica: es un símbolo del carácter sistémico, ubicuo y omnipresente de la sociedad de la información, donde las telecomunicaciones móviles representan un componente vital tanto para las economías digitales como para la geopolítica del siglo XXI. En palabras de Haigh (2016), “la historia de la computación moderna es también la historia del tránsito de lo terrenal a lo planetario” (p. 172).

Finalmente, aunque internet pueda parecer inagotable, su funcionamiento depende de una base material crítica: los servidores, cables submarinos, *routers* y centros de datos que constituyen su soporte físico. La única manera como esta red global podría alcanzar un límite sería si dejara de expandirse la capacidad de su *hardware* e infraestructura física. En este contexto, cobra pleno sentido hablar de la geopolítica del ciberespacio y de la urgencia de proteger la infraestructura crítica cibernética (ICC), entendida no solo como soporte técnico, sino como pilar estratégico de la soberanía, la seguridad y la autonomía digital de los Estados en el siglo XXI.

El ciberespacio cómo metáfora geográfica

El ciberespacio ha sido abordado desde múltiples disciplinas, incluyendo la teoría de medios, la arquitectura, la sociología, la teoría literaria, la cultura popular y el derecho (Smith, 1985; Lanham, 1993; Rheingold, 1993; Cavazos & Morin, 1995; Mitchell, 1995; Rushkoff, 1995; Turkle, 1995; Shields, 1996; Smith, 1999; Lessig, 2006). Sin embargo, su exploración desde la geografía ha sido significativamente

más limitada. Aunque existe una literatura creciente en geografía y comunicación de masas, que ha examinado medios como el cine, la televisión, la telefonía, la fotografía o los sistemas de información geográfica (Abler, 1977; Gould, 1984; Brooker-Gross, 1985; Burgess, 1985, 1987; Gold, 1985; Monmonier, 1989; Adams, 1992; Aitken & Zonn, 1994; Pickles, 1995; Dodge & Kitchin, 2000, 2001; Everett, 2009), al igual que temas como los flujos comerciales (Hepworth, 1990; Sack, 1992; Warf, 1995), el crecimiento urbano vinculado a las redes de comunicación (Graham y Marvin, 1996) o la inserción de las tecnologías de la información en las dinámicas del capitalismo (Castells, 1998), la geografía como disciplina ha prestado escasa atención a las dimensiones políticas, económicas y culturales de las redes informáticas.

Una posible explicación de este desinterés radica en la crítica de algunos representantes de la academia a la conceptualización del ciberespacio como un "espacio" de carácter geográfico. Por ejemplo, Lemley (2003) argumenta que, si bien a menudo se describe internet mediante metáforas espaciales y los usuarios pueden experimentar aspectos del entorno digital como si fuera un lugar, la analogía entre el ciberespacio y un espacio físico resulta errónea. Según Lemley (2003), "como cuestión técnica, por supuesto, la idea de que Internet es literalmente un lugar en el que viaja la gente no solo es errónea, sino que es ridícula" (p. 523). Desde su perspectiva, nadie está "en" el ciberespacio, por cuanto este no es sino un conjunto de protocolos computacionales que permiten transmitir datos entre dispositivos mediante redes de comunicación existentes. Son los datos, y no las personas, quienes efectivamente "viajan" a través del ciberespacio. Dicha postura se refuerza cuando Lemley (2003) analiza la World Wide Web, usualmente vista como el principal vehículo de navegación digital. Según indica Lemley (2003), "si bien las personas podrán hablar de "visitar" sitios web, en realidad no hacen tal cosa. Envían una solicitud de información al proveedor del sitio Web, y el proveedor devuelve datos: la propia página web" (p. 524). Así, la metáfora espacial del ciberespacio como lugar físico se desmorona frente a una comprensión técnica del entorno digital como flujo de información, y no como territorio habitable.

A partir de lo anterior, y si bien el ciberespacio no constituye un lugar geográfico en el estricto sentido del término, diversas metáforas de tipo geográfico han sido frecuentemente empleadas para conceptualizar su naturaleza. Expresiones como "frontera electrónica", "autopista de la información" o "ciberespacio" ilustran de qué forma el lenguaje recurre a figuras espaciales para dar sentido a entornos digitales abstractos. De acuerdo con Adams (1997), estas metáforas no solo reflejan modos de entender el mundo, sino que lo configuran activamente al encarnar,

reproducir y naturalizar determinadas formas de pensamiento. Tradicionalmente, una metáfora se entiende como una herramienta cognitiva que otorga significado a algo nuevo al asociarlo a una imagen más familiar. Sin embargo, un enfoque más contemporáneo sugiere que las metáforas no solo representan, sino que producen significados inéditos mediante la asociación de dominios conceptuales dispares. Desde esta perspectiva pragmática, Barnes argumenta que el valor de una metáfora no reside en su veracidad representacional, sino en su capacidad performativa, pues “las metáforas, precisamente porque son evidentemente falsas y absurdas, nos hacen detenernos y pensar y, por lo tanto, posiblemente nos llevan a hacer cosas diferentes de lo que hemos hecho en el pasado” (Barnes, 1996, p. 154). La utilidad de la metáfora, entonces, radica en su capacidad para provocar una disrupción cognitiva que cuestiona supuestos previos y genera nuevos marcos de interpretación.

En esa misma línea Tuan (1978) señala que cuando las personas dicen que “la sociedad es como un organismo”, activan un proceso mental que los conduce a explorar, de manera explícita y crítica, en qué aspectos esa analogía es válida o no. La metáfora, por tanto, no porta un significado fijo, sino que funciona como un punto de partida para su construcción social. De ahí que, al establecer vínculos entre nociones previamente disociadas, las metáforas desestabilizan significados dados reconfigurando las relaciones entre el sujeto, el entorno y la estructura social. Marvin (1988) va aún más allá al sostener que ciertas metáforas pueden adquirir un carácter casi mítico, al punto de volverse elementos constitutivos de cosmovisiones compartidas. En dicho proceso la metáfora migra desde la percepción individual hacia el repertorio simbólico colectivo operando como mediadora entre la experiencia personal y las estructuras sociales. De este modo el uso de metáforas geográficas para referirse al “cibespacio” no es tan solo una acción estilística, sino una profundamente política y epistemológica, debido a que modela el modo como los seres humanos conciben la tecnología, se relacionan con ella y orientan sus prácticas en el entorno digital.

El significado de una metáfora no puede determinarse de forma unívoca o definitiva, dado que está sujeto a variaciones contextuales e interpretativas. Sin embargo, lo de verdad relevante no es la precisión semántica, sino el modo como las metáforas permiten a las personas pensar a través de sus experiencias y construir sentido en torno a fenómenos complejos. En esta línea, trabajos como el de Deetz (1984), al igual que los de Lakoff y Johnson (1980), han sido fundamentales para clasificar las metáforas en tres grandes categorías: 1) metáforas posicionales, que convierten condiciones no espaciales en orientaciones espaciales; 2) metáforas

ontológicas, que proyectan una dimensión ontológica al atribuir entidad o sustancialidad a conceptos abstractos, y 3) metáforas estructurales, que configuran el pensamiento al articular experiencias a partir de marcos familiares o conocidos.

Estas tres variantes se emplean de manera recurrente en el entorno digital, y de modo particular, en la configuración discursiva del "mundo virtual". Por ejemplo, la expresión "estar en línea" constituye una metáfora posicional que sugiere una ubicación relativa dentro de una red de conexiones. De igual manera, nociones como "sala de chat" o "autopistas de la información" son metáforas estructurales que remiten a espacios arquitectónicos, domésticos o de tránsito, al ofrecer un marco experiencial compartido para comprender la interacción digital. Por último, la idea de "ciberespacio" opera como una metáfora ontológica al conferirle a la red de comunicaciones una equivalencia funcional con un espacio físico. Es decir, como un campo de interacción, agencia y oportunidad.

Por consiguiente, el concepto de ciberespacio no es tan solo una descripción técnica, sino una metáfora geográfica profundamente arraigada en nuestra forma de imaginar lo digital¹⁹. Su uso no es neutral: implica una manera particular de entender la relación entre tecnología, espacio, subjetividad y poder. Al adoptar el lenguaje del espacio para referirse a lo virtual, se naturaliza la idea de que la interacción digital ocurre "en algún lugar", aunque este no sea físico, y se refuerzan así marcos cognitivos espaciales que permiten navegar y dotar de significado a la complejidad de la vida en red.

Como ya se ha señalado, internet constituye una red global que interconecta millones de computadores mediante un conjunto consensuado de protocolos, estándares técnicos, sistemas organizativos y dispositivos físicos. Su arquitectura incluye elementos fundamentales como el Sistema de Nombres de Dominio (DNS), los intermediarios de información, las infraestructuras de seguridad, los puntos de intercambio de tráfico, los sistemas autónomos, los proveedores de servicios de Internet (ISP), los registros, las bases de datos y los organismos de gobernanza y regulación, que abarcan tanto entidades públicas como empresas privadas y organizaciones sin ánimo de lucro (DeNardis, 2014). Esta complejidad técnica y organizacional excede las capacidades explicativas de la informática o de las ciencias sociales por separado, y requiere, por eso, un enfoque interdisciplinario para

¹⁹ Es importante señalar que incluso antes de la acuñación de la metáfora del "ciberespacio", los académicos especulaban que las tecnologías de comunicación sincrónica, como el telégrafo, unirían a la humanidad en algún tipo de espacio compartido (Graham, 2013).

comprender su funcionamiento estructural y su dimensión sociotécnica (O'Hara & Hall, 2013).

Desde el punto de vista físico, los componentes que integran la red (computadores, servidores, cables, centros de datos, dispositivos y operadores institucionales) tienen una localización específica en el espacio geográfico. En ese sentido, internet puede ser concebido como un "espacio" anclado materialmente a la faz de la Tierra. Por lo tanto, mapear el espacio de internet implica representar geográficamente las infraestructuras distribuidas a escala planetaria que hacen posible su existencia y funcionamiento: desde cables submarinos y centros de datos terrestres hasta satélites en órbita terrestre (Álvarez et al., 2019b).

En el marco de las tensiones geopolíticas contemporáneas internet aparece como una red altamente estratégica, comparable a una telaraña global en la que convergen intereses económicos, tecnológicos y de seguridad. En su núcleo se encuentra el sistema de identificación digital, cuyo funcionamiento exige que cada nodo conectado tenga una identidad única y reconocida universalmente. Este principio de unicidad se materializa en los números del Protocolo de Internet²⁰ (IP), que son traducidos (mediante el DNS), en nombres de dominio comprensibles para los usuarios. Así, el direccionamiento IP no solo garantiza la operatividad de internet como infraestructura técnica, sino que constituye también el fundamento de su organización simbólica y política como espacio global.

Toda dirección en internet está compuesta por un nombre de dominio (por ejemplo, www.esdegue.edu.co), cuya estructura se organiza jerárquicamente. La parte final del dominio, situada después del último punto, se denomina "dominio de nivel superior" (TLD), y cumple funciones tanto identificadoras como geográficas u organizacionales. Según Jiang y Ormeling (2000), existen dos tipos principales de dominios de nivel superior: los dominios organizativos clásicos (como: .com, .edu, .gov), que aluden a la naturaleza de la entidad registrada, y los dominios geográficos (como: .co, .uk, .au), que remiten a una localización nacional específica.

El vínculo entre las direcciones IP y los nombres de dominio es gestionado mediante una base de datos jerárquica y federada, conocida como el DNS. Dicho sistema opera como una infraestructura crítica de traducción que permite resolver nombres legibles por humanos en direcciones IP comprensibles por las máquinas, y viceversa. El DNS cumple múltiples funciones de forma simultánea y en tiempo real, lo que requiere mantener la unicidad, coherencia y disponibilidad del sistema a nivel global. La administración del DNS implica múltiples procesos altamente

²⁰ 32 bits de longitud en IP versión 4 [IPv4], 128 bits en IPv6.

especializados: la asignación y resolución de nombres de dominio, la edición y mantenimiento constante de la base de datos, la expansión de la jerarquía mediante la autorización de nuevos TLD (como ocurrió con .info o .tech), la adaptación del sistema a nuevos alfabetos y lenguajes no latinos y, lo que es crucial, la protección frente a amenazas cibernéticas.

Cada uno de estos procesos demanda no solo ingeniería avanzada, sino también una arquitectura institucional robusta. La gobernanza del sistema requiere la cooperación entre los actores estatales, organizaciones privadas, comunidades técnicas y entes multilaterales, mediante una coordinación compleja y transnacional que permita asegurar la estabilidad, la interoperabilidad y la seguridad de esta pieza clave del ecosistema digital contemporáneo, ya que el ciberespacio constituye una red global maleable, cuya accesibilidad puede o bien expandirse o restringirse mediante intervenciones técnicas, regulatorias o geopolíticas. Adicionalmente, su arquitectura no es monolítica, sino estratificada en múltiples capas, cada una de las cuales presenta vulnerabilidades, riesgos y dinámicas específicas. Por lo tanto, esta configuración multidimensional convierte el mapeo del ciberespacio (en términos de localización, distribución y volumen, según sus capas) en una tarea estratégica fundamental para su defensa y gobernanza²¹.

En esta línea, diversos autores, como Jiang y Ormeling (1997), Rattray (2001), Dodge y Kitchin (2001) y Russell (2017), coinciden en que el ciberespacio puede analizarse a partir de al menos cuatro capas estructurales: 1) la capa física, que comprende la infraestructura material y tangible; 2) la capa lógica, donde operan los protocolos, sistemas y redes virtuales; 3) la capa de información, donde circulan y se almacenan los contenidos digitales, y 4) la capa de los usuarios, que representa la dimensión humana e interactiva del entorno digital. En las siguientes páginas se examinará en detalle la capa física del ciberespacio, dado que las restantes (la lógica, la informacional y la relativa a los usuarios) serán abordadas con mayor profundidad en capítulos posteriores de esta obra.

²¹ En la arquitectura de redes un *host* designa cualquier dispositivo conectado a internet que posee una dirección IP y puede enviar o recibir datos. Aunque tradicionalmente se asociaba a una máquina física ubicada dentro de un dominio específico, en la actualidad puede tratarse de servidores virtualizados o distribuidos geográficamente. Por su parte, cada solicitud individual enviada a un servidor web (ya sea para cargar una página, una imagen o un archivo) genera un registro en los sistemas de monitoreo, comúnmente denominado *hit*. Sin embargo, desde el punto de vista analítico, el número de *hits* no necesariamente equivale al número de visitas, pues una sola interacción de un usuario puede producir múltiples solicitudes. Estos registros permiten construir métricas detalladas sobre patrones de tráfico, geolocalización y comportamiento digital, información que constituye un activo estratégico en la economía de datos contemporánea.

Capa física: la infraestructura material del ciberespacio

La capa física del ciberespacio está constituida por todos los componentes materiales que permiten la existencia, funcionamiento y expansión de las redes digitales. Dicha infraestructura incluye desde cables de telecomunicaciones de fibra óptica y torres de telefonía móvil hasta servidores, centros de datos y terminales de usuario, como computadores y dispositivos móviles. Uno de los elementos más críticos de esta capa son los cables submarinos de fibra óptica, que recorren el lecho oceánico conectando continentes y transmitiendo la inmensa mayoría de los paquetes de datos a escala planetaria. Junto a esos cables hay nodos estratégicos, denominados puntos de intercambio de internet (*Internet Exchange Points* [IXP]), en los que las redes se interconectan y redistribuyen el tráfico de datos. A estos se suman centros de datos, o “granjas de servidores”, donde se concentra el procesamiento de información, el almacenamiento y el enrutamiento de datos hacia sus destinos finales. Además, los sistemas satelitales en órbitas bajas, medias y geoestacionarias, como señalan Álvarez et al. (2019b), desempeñan un papel clave en las comunicaciones estratégicas gubernamentales, militares y comerciales, si bien transportan solo una fracción del volumen total de datos del ciberespacio.

Finalmente, el espectro electromagnético constituye un componente esencial de esta capa física²², ya que habilita las transmisiones inalámbricas que sustentan desde las redes móviles hasta los sistemas de comunicación por radiofrecuencia. En conjunto, estos elementos configuran la dimensión tangible del ciberespacio, sobre la cual se superponen las capas lógicas, informacionales y sociales, que serán desarrolladas en los siguientes apartados.

Cables submarinos y terrestres

El ciberespacio global, aunque intangible en su capa lógica, se sostiene en una compleja infraestructura física cuya columna vertebral son los cables submarinos de fibra óptica²³. A pesar de su relativa invisibilidad en las representaciones

²² El espectro electromagnético comprende el conjunto continuo de radiaciones electromagnéticas organizadas según su frecuencia y longitud de onda. Se extiende desde las radiaciones de alta energía y corta longitud de onda (como los rayos gamma y los rayos X) hasta las ondas de baja frecuencia y gran longitud de onda, como las ondas de radio. Entre estos extremos se encuentran el ultravioleta, la luz visible y la radiación infrarroja, cada uno con propiedades físicas y aplicaciones tecnológicas específicas.

²³ Físicamente, los cables submarinos consisten en fibras ópticas dispuestas en haces de vidrio y tendidas sobre el lecho marino, las cuales permiten la transmisión de datos entre dos o más puntos de amarre. Dichas fibras están recubiertas con gel de silicona y protegidas por múltiples capas de materiales como plástico, hilos de nailon, blindaje de acero, vaina de cobre y aislamiento de polietileno, lo que evita daños físicos y minimiza la degradación de la señal. A lo largo de su recorrido oceánico, los cables incorporan repetidores, o “amplificadores ópticos”, ubicados a intervalos regulares de aproximadamente cada 100 km, que regeneran la

populares de internet, estos cables transportan cerca del 99 % del tráfico mundial de datos²⁴, incluyendo comunicaciones financieras, diplomáticas, comerciales y militares. De hecho, en 2023 se estimaba que los cables submarinos soportaban transacciones diarias por un valor de aproximadamente de 10 billones de dólares (Capri, 2024a). Aunque las comunicaciones de datos también pueden transmitirse por satélites, el uso de cables de fibra óptica resulta considerablemente más económico y veloz. En este sentido, los cables submarinos constituyen las verdaderas fibras nerviosas que envuelven el planeta y sostienen el sistema de telecomunicaciones contemporáneo haciendo posible tanto la globalización como el funcionamiento del ciberespacio (Álvarez & Zambrano, 2017).

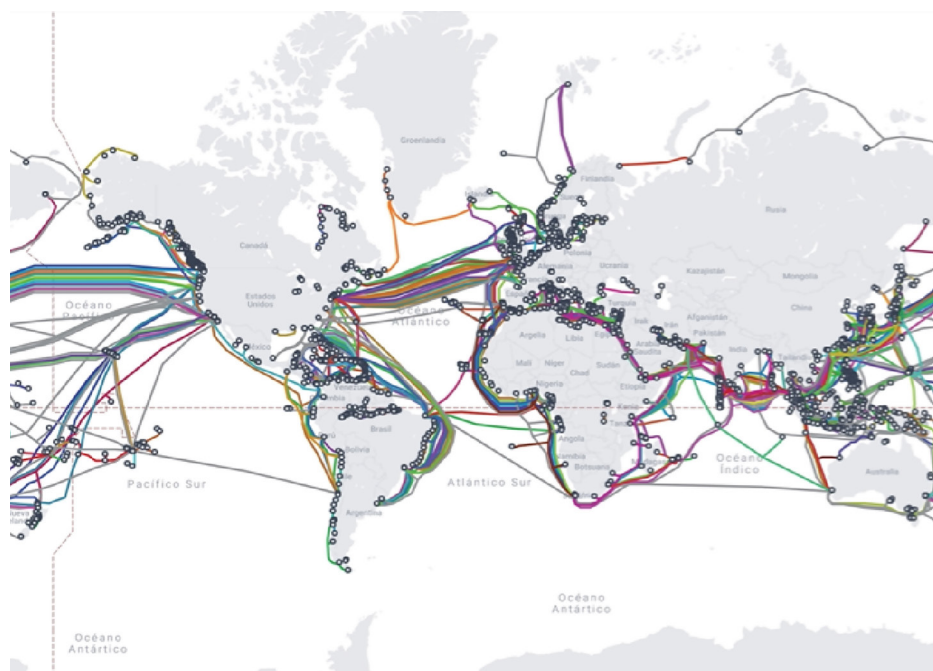
Dentro de la vasta infraestructura de telecomunicaciones global los enlaces más extensos corresponden a los que conectan los satélites espaciales con sus estaciones terrestres, y en especial, a los tramos intercontinentales de los cables submarinos de fibra óptica. Para 2025 se estimaba la existencia de más de 1,3 millones de km de cables submarinos en operación²⁵, integrados en más de 570 sistemas activos en todo el mundo (Telegeography, 2025). Los sistemas de mayor longitud establecen conexiones entre continentes, mientras que los más cortos bordean zonas costeras eludiendo las limitaciones de los enlaces terrestres y fortaleciendo la resiliencia de las redes (Carter et al., 2009). La concentración más densa de estos cables se halla entre la costa este de Estados Unidos y Europa. La ruta entre Nueva York y Londres es la de mayor capacidad de transmisión. La figura 2 ilustra la geografía de estos cables: tanto su distribución planetaria como sus trayectorias y sus nodos de conexión estratégicos.

señal para asegurar su integridad. En ambos extremos los cables llegan a “estaciones de aterrizaje”, o *Cable Landing Stations* (CLS), desde donde los datos se distribuyen mediante redes de fibra óptica terrestre hasta su destino final. Dichas estaciones funcionan como centros de datos alojando el equipamiento de energía y red necesario para gestionar las operaciones del cable y facilitar el flujo del tráfico digital.

²⁴ Las estimaciones muestran que si se envía un correo electrónico o se hace una llamada telefónica internacional, existe una probabilidad del 95 % de que se utilicen cables submarinos en el proceso (Van Logchem, 2014).

²⁵ El número total de cables cambia constantemente, a medida que los nuevos cables entran en servicio y los cables más antiguos se retiran del servicio.

Figura 2. Cables submarinos en 2024



Fuente: <https://www.submarinecablemap.com/#/>

La mayoría de los actuales cables submarinos de telecomunicaciones son de fibra óptica, y si bien su despliegue puede considerarse relativamente reciente, la infraestructura global de telecomunicaciones tiene raíces mucho más profundas. De hecho, aunque internet ha sido la innovación definitoria del siglo XXI, el proceso de "conectividad" planetaria empezó hace más de 160 años. Efectivamente, las rutas contemporáneas de los cables submarinos de fibra óptica (que constituyen el esqueleto físico de internet) replican en gran medida las trayectorias de los antiguos cables telegráficos transoceánicos. De hecho, el impacto de las telecomunicaciones modernas se remonta a 1844, con la invención del telégrafo, considerado el "primer mecanismo eficaz de telecomunicación" (Malecki & Wei, 2009, p. 360). Desde sus primeros años, dicho sistema fue aprovechado intensamente por bancos, agencias de noticias y otras organizaciones que buscaban operar en un incipiente "espacio electrónico global" permitiendo la circulación de información sin la necesidad del desplazamiento físico. Sin embargo, el telégrafo no reemplazó por completo otras formas de comunicación: sus altos costos lo reservaron sobre todo para mensajes urgentes, mientras que las comunicaciones menos críticas y

de menor valor siguieron utilizando medios más lentos, como el correo tradicional (Kaukiainen, 2001; McCusker, 2005).

El primer cable submarino, un cable telegráfico de cobre, fue instalado en 1850, a través del Canal de la Mancha, para conectar el Reino Unido con Francia (Mensah, 2000). Ocho años después, en 1858, se logró tender el primer cable transatlántico entre Estados Unidos y el Reino Unido²⁶, lo que marcó un hito en la historia de las telecomunicaciones globales²⁷. Para 1870, Gran Bretaña ya había establecido una conexión por cable con la India, y en 1872 Australia se incorporó a esta red incipiente (Thorat, 2019). En 1902, con el despliegue del cable que unía Manila y San Francisco a lo largo de 9.656 km, se completó por primera vez la conexión global por medio de esos cables submarinos. Por supuesto, el impacto subsiguiente de dicha infraestructura sería revolucionario, ya que la velocidad de transmisión de la información experimentó un salto cualitativo sin precedentes. Mientras que las noticias del asesinato de Abraham Lincoln, en 1865, tardaron trece días en llegar a Londres, las del terremoto de Nobi, en Japón (1891), arribaron en apenas unas horas (Clark, 2007). Aunque el financiamiento inicial del telégrafo fue predominantemente privado, los gobiernos también jugaron un papel relevante al subsidiar parte de la expansión. Para 1892, de los 246.871 km de cables instalados en el mundo, el 89,6 % pertenecía a empresas privadas, mientras que solo el 10,4 % correspondía a cables de propiedad gubernamental, en su mayoría destinados a conectar islas pertenecientes a un mismo territorio nacional (Malecki & Wei, 2009)²⁸.

No obstante, los gobiernos siempre desempeñaron un papel activo en el desarrollo de la infraestructura telegráfica y de cables submarinos, bien para promover dicha tecnología o, por el contrario, para obstaculizarla. En el caso de China, por

²⁶ Los avances tecnológicos se incorporaron a los cables que conectaban ubicaciones donde abundaban los clientes comerciales, como entre Nueva York y Londres.

²⁷ Si bien en su momento fue un gran avance tecnológico, la recepción fue terrible para los estándares modernos, ya que tomaba 2 minutos y 5 segundos transmitir un solo carácter, y más de 17 horas para transmitir el primer mensaje.

²⁸ Asimismo, si bien los cables telegráficos submarinos se extendieron a todos los continentes, el equipo y el conocimiento estaban en manos de una pequeña élite, principalmente británica, ya que los 257 cables privados de las empresas británicas representaban el 63,1 % del total mundial (Winde, 2006). Por su parte, los cables más modernos pertenecían tradicionalmente a operadores de telecomunicaciones que formaban un consorcio de todas las partes interesadas en usar el cable submarino. A fines de la década de 1990 una afluencia de empresas emprendedoras construyó muchos cables privados y vendió la capacidad a los usuarios. Tanto el consorcio como los modelos de cable privado todavía existen en la actualidad, pero uno de los mayores cambios en los últimos años es el tipo de compañías involucradas en la construcción de cables. Los proveedores de contenido, como *Google*, *Meta*, *Microsoft* y *Amazon*, son los principales inversores en nuevos cables, y han superado a los operadores de red troncal de internet en los últimos años. Frente a la perspectiva de un crecimiento continuo y masivo del ancho de banda, tener nuevos cables submarinos tiene sentido para estas compañías.

ejemplo, las autoridades imperiales inicialmente desconfiaron de la tecnología telegráfica, por considerarla una amenaza a su soberanía frente a las influencias extranjeras, por lo que negaron en múltiples ocasiones los permisos para conectar Shanghái a la red internacional, hasta que en 1875 permitieron finalmente el establecimiento de una red de propiedad nacional, al percibirla como una herramienta útil para la administración estatal (Headrick, 1991). De forma similar, la instalación del primer cable transpacífico por parte de Estados Unidos respondió a consideraciones estratégicas de seguridad. La Armada estadounidense descubrió, con alarma, que sus comunicaciones entre Washington y su nueva colonia en Filipinas eran transmitidas por cables británicos que cruzaban el océano Atlántico, el Mediterráneo y Asia, hasta llegar a Hong Kong y Manila. Esta vulnerabilidad geopolítica motivó una respuesta institucional que culminó en el desarrollo de una ruta propia (Headrick & Griset, 2001).

El predominio de los cables, sin embargo, fue temporal. Con la aparición de la radio de onda corta, en las décadas de 1920 y 1930, y más adelante, con los satélites, el uso de cables submarinos experimentó un notorio declive. En 1929, por ejemplo, un terremoto frente a la costa de Nueva Escocia rompió 12 de los 21 cables del Atlántico Norte, pero los usuarios apenas si notaron el impacto, gracias a la redundancia provista por las comunicaciones inalámbricas (Hugill, 1999). En efecto, para 1937 el número de circuitos internacionales por radio casi igualaba la red global de cables submarinos. Dicha tendencia fue reforzada por la Gran Depresión, que redujo drásticamente el comercio internacional (la principal razón de ser del telégrafo submarino). No sería sino hasta 1956, con la entrada en funcionamiento del primer cable telefónico transatlántico (TAT-1), cuando se reactivaría la expansión de la infraestructura submarina, lo que marcó el fin definitivo de los antiguos cables telegráficos (Headrick, 1991).

Durante un breve periodo posterior a la puesta en funcionamiento de los primeros satélites de telecomunicaciones, en la década de 1960, el futuro de las comunicaciones globales pareció estar firmemente ligado a la tecnología satelital espacial (Álvarez et al., 2019a). Los satélites eran en especial adecuados para la transmisión de señales televisivas, lo cual coincidió con la expansión masiva de los medios audiovisuales, y ofrecieron inicialmente una capacidad de transmisión telefónica superior a la de todos los cables submarinos combinados²⁹. Sin embargo, los cables de fibra óptica han desplazado, en las últimas décadas y de forma

²⁹ Según Malecki y Wei (2009), desde 1965 hasta 1988 los satélites proporcionaron casi diez veces la capacidad de los cables telefónicos submarinos por casi una décima parte del precio.

contundente, a los satélites espaciales como el medio dominante de transmisión de datos a escala planetaria³⁰. Esta preferencia obedece, entre otras razones, a que los cables pueden ser propiedad directa de operadores de telecomunicaciones, mientras que la capacidad satelital suele ser arrendada, lo cual limita el control estratégico y económico sobre la infraestructura (Álvarez et al., 2019c).

Por ende, el punto de inflexión tecnológico se produjo en 1988, con el despliegue del primer cable de fibra óptica transatlántico (TAT-8), que revalorizó la infraestructura submarina, previamente considerada obsoleta tras la irrupción de la radio en los años treinta y la hegemonía satelital en los setenta. Tan significativa ha sido la revitalización de esta tecnología que entre 2016 y 2020 se instalaron 107 nuevos sistemas de cable submarino de fibra óptica, que suman más de 400 mil km de longitud y una inversión total superior a los 13.800 millones de dólares (TeleGeography, 2020). El principio operativo de esta tecnología radica en el uso de emisores láser para enviar pulsos de luz a velocidades extremadamente altas a través de fibras de vidrio delgadas (del grosor aproximado de un cabello humano), hasta receptores en el extremo opuesto del cable. Para su protección, dichas fibras están encapsuladas en múltiples capas, que incluyen aislamiento plástico, y en zonas más expuestas, como aguas costeras, incluso blindaje con alambre de acero.

Ya sea por la manipulación no intencionada o por la destrucción deliberada, los cables submarinos son vulnerables tanto a daños accidentales como a actos de sabotaje, lo que representa una amenaza directa a la eficiencia, la confiabilidad y la seguridad estructural del ciberespacio. Cada año se registran entre 100 y 150 fallos en cables submarinos, definidos como incidentes que deterioran o interrumpen por completo su capacidad de transmisión de datos (Carter et al., 2009). A pesar de que la mayoría de estos daños son accidentales³¹ (ocasionados sobre todo por redes de pesca de arrastre o anclas de embarcaciones), también existen fallos provocados por fenómenos naturales, como ataques de tiburones o desastres geológicos³².

³⁰ Los circuitos satelitales fueron más numerosos que los circuitos de cable submarino a través del Océano Pacífico hasta 1989, y fueron más numerosos que los cables transatlánticos hasta 1994 (Bryson et al., 2004).

³¹ En los últimos 50 años los equipos de pesca y las anclas representaron aproximadamente el 70 % del daño causado a los cables submarinos. Estos cortes de cable submarino ocurren con frecuencia, pero la mayoría de ellos son menores y provocan solo una pequeña interrupción en el servicio.

³² Los cables submarinos también pueden verse afectados por desastres naturales, sobre todo por terremotos y erupciones volcánicas, los cuales representan aproximadamente el 12 % de los daños registrados en esta infraestructura crítica (Carter et al., 2009). Aunque dichos eventos son relativamente poco habituales, su impacto puede ser significativo para las telecomunicaciones internacionales. Un ejemplo notable ocurrió en 2003, cuando un terremoto en Argelia dañó tanto los cables submarinos como las estaciones terrestres satelitales, lo que interrumpió casi por completo los servicios internacionales de telecomunicaciones del país.

Empero, una fracción creciente de estos sucesos corresponde a actos deliberados de sabotaje perpetrados por actores hostiles³³. Tal fue el caso durante el 17 y el 18 de noviembre de 2024, cuando dos cables submarinos de fibra óptica en el Mar Báltico fueron dañados en lo que se presume fue un acto de sabotaje perpetrado por el carguero chino Yi Peng 3, que se hallaba en la zona al momento de la interrupción. De manera similar, un informe de la Oficina Nacional de Auditoría de Taiwán documentó que entre 2019 y 2024 buques extranjeros dañaron en 36 ocasiones los cables que conectan la isla principal con sus territorios insulares, y que 12 de esos incidentes se registraron tan solo en 2023³⁴.

En febrero de 2024 dos cables que enlazaban Taiwán con las islas Matsu fueron afectados, con pocos días de diferencia, por una embarcación pesquera y un carguero, ambos de la República Popular de China, lo cual generó interrupciones en el servicio de internet y llamadas telefónicas. Algunos analistas interpretaron estos hechos como un posible ensayo de bloqueo invisible a Taiwán por parte de la China continental. En otro episodio relevante los rebeldes hutíes de Yemen negaron en 2024 haber atacado cables submarinos en el mar Rojo, pese a que se reportaron daños en líneas pertenecientes a cuatro importantes redes de telecomunicaciones.

Pero más allá de la intencionalidad, las reparaciones de cables submarinos representan desafíos técnicos y financieros significativos. El costo promedio de un tramo de 1,5 km asciende a unos 55.000 dólares, mientras que la instalación de un nuevo cable transatlántico puede requerir inversiones entre de 270 y 340 millones de dólares, y su instalación, alcanzar profundidades de hasta 4.000 m bajo el nivel del mar. Como resultado, la ubicación actual de estos cables de

De forma similar, la erupción volcánica registrada frente a las costas de Tonga en 2022 provocó daños considerables a los cables submarinos en esa región, y así generó serias afectaciones en la conectividad del archipiélago.

³³ La acción estatal deliberada y otras actividades humanas representan aproximadamente el 8 % de los daños a los cables submarinos (Carter et al., 2009). Entre estas causas se incluyen el dragado del lecho marino, la construcción de tuberías, la extracción de petróleo y gas, el vertido de desechos y algunas prácticas de investigación científica. Si bien los cortes en cables cercanos a la costa suelen ser reparados con relativa rapidez, debido a su mayor accesibilidad, los daños ocurridos mar adentro (especialmente, a profundidades superiores a los 4.000 m) requieren operaciones de mayor complejidad técnica, tiempos prolongados y el uso de equipos altamente especializados.

³⁴ Los actos de sabotaje contra cables submarinos no son una amenaza reciente, sino una táctica utilizada a lo largo de la historia en contextos de guerra. Durante la Guerra Hispanoamericana de 1898 fuerzas estadounidenses cortaron cables telegráficos submarinos para aislar a sus adversarios de las comunicaciones internacionales. De forma similar, en la Guerra Fría, Estados Unidos intervino cables soviéticos con fines de inteligencia. Estos precedentes muestran que los cables submarinos, más allá de su función técnica, han sido considerados activos y objetivos estratégicos clave en las operaciones militares.

telecomunicaciones y sus más de 1.400 “estaciones de aterrizaje” (donde los cables se unen para tocar tierra), están marcados a menudo en cartas náuticas y mapas costeros, para que los operadores de barcos y otros puedan evitarlos.

No hay un organismo supranacional que esté encargado específicamente de la protección de los cables submarinos. En consecuencia, la responsabilidad de evitar su daño recae sobre todo en los navegantes, quienes deben consultar las cartas náuticas actualizadas y cumplir con las normativas locales para salvaguardar esa infraestructura crítica (Van Logchem, 2014). En ciertas regiones, las guardias costeras y las armadas con funciones litorales pueden asumir un rol más activo en su protección, especialmente en los tramos donde los cables emergen en tierra firme. Estos puntos de aterrizaje requieren una mayor vigilancia, al ser allí donde los cables son canalizados, a través de tuberías subterráneas, hasta su conexión con las redes terrestres, las cuales están compuestas por líneas físicas, amplificadores de transmisión y equipos de protección y supervisión, así como por terminaciones ópticas.

La privilegiada posición geográfica de Colombia, con costas sobre el Caribe y el Pacífico, le otorga al país un valor geoestratégico excepcional como punto de interconexión digital para toda América Latina. Hasta 2024 Colombia tenía al menos nueve cables submarinos activos: Arcos-1, Pan-Am, CFX-1, Maya-1, SAM-1, AMX-1, Globenet, PCCS y SAC-LAN. Tal infraestructura comprende más de 42.000 km de fibra óptica en el lecho marino, complementada por cerca de 24.000 km de fibra terrestre, lo cual asegura la capilaridad de la conectividad nacional. Las estaciones de aterrizaje de dichos cables se hallan estratégicamente distribuidas. Cartagena aloja tres de ellas (CFX, PCCS y ARCOS), mientras que Tolú alberga la estación del cable MAYA, y Riohacha, la del ARCOS. Otros puntos de aterrizaje se encuentran en Santa Marta, San Andrés, Barranquilla, Puerto Colombia, Parque Isla Salamanca y Buenaventura (Portafolio, 2023). A nivel terrestre, la conectividad hacia el interior del país se garantiza mediante cuatro rutas independientes de fibra óptica, que enlazan a las principales ciudades: Bogotá, Medellín, Cali, Barranquilla y Bucaramanga, además de una conexión extendida hasta Pasto, y de allí, hacia Ecuador.

Una de las actualizaciones más significativas ha sido la del sistema Colombia-Florida Express (CFX-1), el cual conecta a Colombia con Estados Unidos y Jamaica. Este cable fue optimizado para alcanzar una velocidad de transmisión cercana a los 32 Tbps, con servicios que permiten flujos de datos de 100 Gbps y 400 Gbps (Liberty Networks, 2023). Asimismo, entre 2010 y 2015 se incorporó el cable AMX-1, promovido por el Ministerio TIC de Colombia y operado por Claro. El sistema,

de 17.800 km de longitud, conecta a Colombia con Brasil, República Dominicana, Puerto Rico, Guatemala, México y Estados Unidos mediante once puntos de contacto costero. Su instalación permitió multiplicar por 50 la capacidad de conexiones internacionales del país. En el horizonte inmediato, Colombia seguirá fortaleciendo su rol regional como *hub* digital. Un ejemplo reciente es el proyecto Carnival Submarine Networks-1 (CSN-1), liderado por la compañía ecuatoriana Telconet, en colaboración con Alcatel Submarine Networks. Este cable se extenderá desde Florida hasta Ecuador, pasando por México, Panamá y Colombia (DCD, 2025). La estación de aterrizaje colombiana se ubicará en Playa Salgar, cerca de Barranquilla, y será construida por la empresa Vertiv. Su entrada en funcionamiento está prevista para 2026.

En conjunto, esa red de cables submarinos y estaciones de aterrizaje posiciona a Colombia como un nodo estratégico en la arquitectura del ciberespacio latinoamericano, al tiempo que fortalece la resiliencia de sus redes, la soberanía digital y la competitividad digital en el marco de la economía global del conocimiento. Pero este papel de Colombia como nodo digital regional depende no solo de la cantidad de cables o su capacidad técnica, sino también de las condiciones físicas y operativas que aseguran su funcionamiento. En efecto, la ubicación, diseño y resguardo de las estaciones de aterrizaje resultan decisivos para garantizar la continuidad de los servicios digitales que fluyen por esta infraestructura crítica.

En las estaciones de aterrizaje los cables de fibra óptica son encapsulados en tubos protectores, dispuestos en zanjas especialmente acondicionadas o integrados en infraestructuras existentes, como derechos de vía ferroviarios y puentes. Dichas medidas buscan garantizar su resguardo físico, especialmente en los tramos más expuestos cercanos a la costa. En ese contexto, la Armada Nacional de Colombia debe desempeñar un papel protagónico en la vigilancia y protección de dicha infraestructura crítica, esencial para el funcionamiento seguro, resiliente y estable del ciberespacio.

Una vez en tierra, estos cables siguen brindando conectividad mediante redes terrestres encapsuladas, pero permanecen particularmente vulnerables en las estaciones de aterrizaje, donde pueden ser objeto tanto de daños accidentales como de actos deliberados. Entre las amenazas comunes a estos sistemas se incluyen ataques dirigidos específicamente a la fibra óptica, al equipamiento de conmutación o red al que están conectados, o al sistema de alimentación eléctrica que garantiza su funcionamiento. Los segmentos más susceptibles son los cables expuestos sobre el terreno (por ejemplo, desde la playa hasta el edificio de

la estación) y los tramos subterráneos de fácil acceso, como los ubicados bajo tapas de alcantarilla³⁵.

La seguridad de los cables submarinos radica en la resiliencia y flexibilidad de la red global que los sostiene. En primer lugar, esta red posee capacidades de "autocuración": o sea, puede redirigir automáticamente el tráfico de datos hacia rutas o nodos alternativos cuando se presenta una interrupción. Por eso, un daño concreto a un cable o a una estación de aterrizaje rara vez genera consecuencias visibles en el funcionamiento cotidiano del sistema (Crain, 2012). En segundo lugar, tanto los cables como las estaciones de aterrizaje no están fijados de forma inmutable a ubicaciones específicas, y pueden ser reubicados estratégicamente en lugares más seguros si las condiciones lo requieren. Esta maleabilidad geográfica se explica por la propia naturaleza del ciberespacio: es decir, una red artificial cuya configuración espacial puede ser modificada por decisión humana.

El daño a las estaciones de aterrizaje puede producirse por medio de ataques físicos directos (como atentados explosivos o incursiones armadas), por vías indirectas (como sabotajes a los sistemas de energía que las abastecen) o mediante acciones internas encubiertas (tales como virus informáticos, incendios provocados o destrucción deliberada). Aunque muchas de esas estaciones tienen sistemas de respaldo eléctrico (como generadores autónomos y baterías), que las protegen de cortes de energía, su vulnerabilidad persiste ante incidentes mayores que afecten a toda una región. El tema es que, por lo general, las medidas de protección física de dichas instalaciones son mínimas: efectivamente, muchas de las estaciones de aterrizaje no cuentan con barreras defensivas robustas, y operan desde pequeños edificios situados cerca de la playa. En los pocos casos en que existe algún tipo de seguridad, esta suele limitarse a cercas básicas y sistemas elementales de videovigilancia. Tal situación hace que, al menos en términos operativos, resulte relativamente fácil ejecutar acciones de sabotaje físico contra esta infraestructura crítica.

En definitiva, el ciberespacio global, aunque intangible en su capa lógica, se sostiene en una compleja infraestructura física cuya columna vertebral son los cables submarinos de fibra óptica. Desde una perspectiva geoestratégica, el control sobre la fabricación, instalación, operación y mantenimiento de esa infraestructura

³⁵ Cabe señalar que, si bien las estaciones de aterrizaje suelen ser edificaciones equipadas con sistemas de telecomunicaciones especializados, el daño localizado en sus cables y equipos suele ser más fácil de identificar y reparar, en comparación con los cortes que se producen en tramos marinos profundos. No obstante, la seguridad física de dichas estaciones representa un componente fundamental dentro del esquema de protección de la infraestructura digital nacional.

otorga una ventaja crítica en términos tanto económicos como de recopilación de inteligencia. Según Capri (2024a), quien domine estos sistemas no solo controla la economía digital global, sino que también posee capacidades estratégicas para ejercer vigilancia, interceptación e, incluso, sabotaje sobre las comunicaciones transnacionales. Con base en lo anterior, el panorama actual revela una creciente bifurcación entre esferas de influencia dominadas por Estados Unidos y China. Mientras que empresas como SubCom (Estados Unidos), NEC (Japón) y Alcatel Submarine Networks (Francia) habían liderado tradicionalmente el mercado, el ascenso de la empresa HMN Technologies (filial china derivada de Huawei Marine) ha provocado una intensificación de la competencia tecnológica (Capri, 2024a).

En consecuencia, Washington ha desplegado una campaña de “tecno-diplomacia” presionando a gobiernos aliados para excluir a proveedores chinos de consorcios de cables, como ocurrió con el proyecto Coral Sea Cable, entre Australia y Papúa-Nueva Guinea. La lucha se extiende a tres arenas interrelacionadas: 1) la confrontación directa entre Estados Unidos y China por la hegemonía tecnológica³⁶; 2) la participación de gigantes tecnológicos como Google, Amazon, Meta y Microsoft en la expansión y control de redes de cable propias, con independencia relativa de los Estados, y 3) la amenaza creciente de sabotaje, como evidencian los recientes ataques o incidentes sospechosos en el Báltico, el estrecho de Taiwán y el golfo de Finlandia (Capri, 2024a). En particular, las estaciones de aterrizaje han pasado a ser nodos geoestratégicos de alto valor y vulnerabilidad, ya que, con más de 1.400 estaciones en operación o construcción a nivel global, su control se asemeja al de un “cuello de botella” digital que concentra capacidades críticas de interconexión.

Además, el papel de las empresas tecnológicas estadounidenses se ha vuelto ambivalente. Por un lado, son consideradas activos estratégicos por su capacidad para financiar y construir infraestructura global. Por otro, pueden ser percibidas como riesgos de seguridad nacional cuando cooperan con actores geopolíticamente sensibles. En 2023 Google era propietaria de 26 cables submarinos, lo que le otorgaba un control significativo sobre el tráfico de datos, frecuentemente alquilado a operadores tradicionales (Capri, 2024a). Sin embargo, este liderazgo también genera preocupaciones en materia de soberanía digital y seguridad nacional, ya que cuando estas plataformas interactúan con jurisdicciones sensibles, como

³⁶ El caso del cable SEA-ME-WE 6 (Southeast Asia–Middle East–Western Europe 6) ilustra esta tensión; aunque la empresa china HMN ofreció una propuesta más económica, el contrato fue adjudicado a SubCom, debido a la amenaza de sanciones estadounidenses, evidencia de que el factor político pesa más que el financiero en decisiones de infraestructura crítica.

China o Rusia, su papel puede percibirse como una amenaza latente o un vector de vulnerabilidad estratégica.

Este dilema no es ajeno a Colombia, que, si bien no posee cables propios, sí constituye un nodo clave en la arquitectura digital de la región. El país alberga múltiples estaciones de aterrizaje y participa en las redes de interconexión que lo vinculan con América del Norte, América Central y América del Sur. En ese contexto, la creciente dependencia de infraestructura de propiedad privada y extranjera (particularmente, de empresas con matriz en Estados Unidos) plantea interrogantes sobre el grado de autonomía tecnológica y ciberestratégica de Colombia. Tal como advierte Capri (2024a), la "privatización de la soberanía digital" puede consolidar una nueva forma de dependencia estructural, donde los intereses empresariales se imponen a la planificación estatal y a la defensa del interés público. Para Colombia ello implica la urgencia de diseñar políticas de resiliencia digital, diversificación de proveedores y vigilancia estratégica de su infraestructura crítica, especialmente en un entorno internacional cada vez más conflictivo y multipolar.

Satélites espaciales

En la configuración contemporánea del ciberespacio las comunicaciones satelitales son un componente indispensable de su infraestructura física. Si bien los cables submarinos de fibra óptica transportan la mayoría del tráfico global de internet, en ciertos contextos, los satélites de comunicaciones cumplen funciones críticas estratégicas, militares y geográficas que complementan (e incluso, sustituyen) la infraestructura terrestre. La capa satelital del ciberespacio permite la conectividad en regiones remotas, garantiza la resiliencia en zonas de conflicto y proporciona cobertura para plataformas móviles y aerotransportadas, lo que la convierte en un vector esencial para la interconexión digital global.

Si bien los satélites espaciales solo transmiten actualmente cerca del 5 % de las telecomunicaciones de voz y datos globales, y resultan entre cinco y 50 veces más lentos y costosos por *megabit* por segundo que las redes de fibra óptica, su relevancia estratégica no se deriva de la eficiencia, sino de su arquitectura funcional. En efecto, los cables requieren enlaces físicos punto a punto, que implican concentraciones geográficas de infraestructura, mientras que los satélites, al irradiar cobertura sobre vastas áreas desde órbita, permiten una distribución punto a multipunto sin precedentes, lo que otorga mayor equidad territorial en el acceso digital (Malecki & Wei, 2009). A pesar de su menor capacidad y vida útil limitada (de diez a quince años, frente a los 25 de los cables submarinos), los satélites siguen

desempeñando un papel insustituible, no solo en telecomunicaciones de respaldo y emergencia, sino también en la recolección remota de datos, la vigilancia geoespacial y la arquitectura estratégica del ciberespacio global.

La historia de las comunicaciones satelitales va intrínsecamente ligada al periodo de la Guerra Fría y el desarrollo de telecomunicaciones tanto militares como civiles. Desde el lanzamiento del primer satélite artificial, el Sputnik I, en 1957, el potencial de utilizar el espacio como medio para las comunicaciones globales catalizó una serie de iniciativas tecnológicas, políticas y comerciales. El despliegue del primer satélite de comunicaciones, el Telstar, en 1962, marcó el inicio de una era en la que la información podía transmitirse de forma transcontinental sin depender de cables submarinos ni de repetidores terrestres (Elbert, 2008). Durante las décadas de 1960 y 1970 los satélites geoestacionarios se convirtieron en la columna vertebral de la radiodifusión internacional, los servicios telefónicos y, posteriormente, los protocolos de internet.

En 1970 la Universidad de Hawái desarrolló ALOHAnet, la primera red de radio por paquetes, la cual demostró la viabilidad de la conectividad distribuida a través de enlaces inalámbricos satelitales. Este modelo fue pionero en integrar nodos remotos, y sentó las bases para futuras redes de conmutación por paquetes. En 1975 se logró la primera conexión TCP/IP vía satélite entre Estados Unidos y el Reino Unido a través del océano Atlántico, una proeza liderada por la Universidad de Stanford, BBN y University College London. Este hito precedió el establecimiento de SATNET, la red satelital de paquetes del Atlántico, que se constituyó en un puente digital entre Europa y América del Norte utilizando los satélites de INTELSAT. Empero, la demostración conjunta de ARPANET, SATNET y PRNET, en 1977, representó un avance decisivo en la interoperabilidad de redes heterogéneas. Durante este experimento se transmitió un mensaje desde una furgoneta en la bahía de San Francisco, en California, que cruzó varios sistemas de red (incluyendo enlaces satelitales), antes de llegar a Londres, y luego, regresar a Virginia, Estados Unidos. El ejercicio mostró por primera vez la viabilidad de una arquitectura verdaderamente interconectada, lo que prefiguraba la estructura global del Internet actual.

En 1982 la estandarización del protocolo TCP/IP para ARPANET marcó otro punto de inflexión, al establecer las bases de internet como un conjunto interconectado de redes usando protocolos comunes. A partir de entonces el papel de los satélites se fue diversificando: en Japón el establecimiento de redes como JUNET, en 1984, y su evolución hacia el proyecto WIDE, en 1987, mostraron la expansión de modelos de interconectividad respaldados por enlaces satelitales. También

durante los años ochenta surgieron redes como NSFNET y UUNET, que democratizaron el acceso a internet en el ámbito universitario y comercial, aunque ya en esta etapa el uso de enlaces terrestres empezaba a predominar en zonas urbanas.

Sin embargo, el uso de satélites no desapareció con el auge de la fibra óptica, sino que se adaptó a nichos específicos. En particular, las regiones rurales o en desarrollo continuaron dependiendo de enlaces satelitales para su acceso a internet. Además, el uso de enlaces satelitales asimétricos (donde la recepción de datos ocurre vía satélite, y el envío, por medios terrestres), se consolidó como una solución viable para equilibrar costos y capacidades. En este orden de ideas, el panorama de las comunicaciones satelitales comenzó a transformarse en los años noventa y principios del siglo XXI, con la aparición de nuevas constelaciones en órbita terrestre baja (LEO), las mejoras en el segmento terrestre y la liberalización de la actividad espacial comercial (Minoli, 2015). Estos desarrollos impulsaron lo que Kota et al. (2004) denominan la “banda ancha satelital”, que permitió la comunicación bidireccional basada en IP, la integración con redes terrestres y la provisión de servicios de internet a poblaciones no atendidas. En la actualidad constelaciones como Starlink, OneWeb y Kuiper representan no solo un salto tecnológico, sino, a su vez, una reconfiguración geopolítica del control de la información y de la gobernanza espacial.

Cabe señalar que una de las principales ventajas de los sistemas de comunicaciones satelitales radica en su capacidad para superar las limitaciones geográficas inherentes a las redes terrestres. De acuerdo con Elbert (2003), los satélites espaciales pueden proporcionar conectividad de línea de visión a grandes distancias³⁷, con patrones de cobertura determinados por la altitud orbital, el diseño de la huella de cobertura y el espectro de frecuencias. Asimismo, satélites en órbita geoestacionaria (GEO), ubicados a 35.786 km sobre el ecuador, ofrecen cobertura persistente de una región fija, lo que los hace ideales para la radiodifusión y los servicios satelitales fijos (Álvarez et al., 2019b). En contraste, los satélites LEO, situados entre los 500 km y 1.200 km de altitud, tienen periodos orbitales más cortos y menor latencia³⁸, lo que los hace adecuados para el internet de banda ancha,

³⁷ La conectividad de línea de visión (en inglés, *Line-of-Sight* [LOS]) se refiere a la transmisión de señales inalámbricas donde el transmisor y el receptor deben estar dentro de la vista directa uno del otro, sin obstáculos físicos que bloqueen la señal.

³⁸ Como lo argumenta Elbert (2008), los satélites LEO, al tener órbitas más cercanas a la Tierra, permiten mejorar los tiempos de respuesta en las comunicaciones y reducir significativamente los efectos de retardo en servicios de misión crítica, lo cual resulta vital en contextos de conflicto o en despliegues tácticos. Además, al estar en movimiento constante respecto a la superficie terrestre, requieren sofisticados mecanismos de entrega continua de señal, como el traspaso automático entre satélites, enlaces intersatelitales (ISL) y estaciones terrenas con capacidades de seguimiento en tiempo real.

aplicaciones en tiempo real y comunicaciones en entornos móviles o de alto riesgo (Elbert, 2014).

Estas características orbitarias, junto a las propiedades del espectro utilizado, configuran las bases técnicas que determinan el alcance, la latencia y la estabilidad de las comunicaciones por satélite. No obstante, para comprender a plenitud el funcionamiento y las capacidades de estas redes, es indispensable examinar su arquitectura, la cual se articula a través de componentes espaciales, terrestres y de control que interactúan de manera coordinada para garantizar la prestación eficiente del servicio. En ese sentido, las redes satelitales se componen de tres segmentos principales: el segmento espacial (satélites), el segmento terrestre (estaciones terrenas, antenas, módems) y el segmento de control (telemetría, seguimiento y comando). Las innovaciones en cada uno de estos ámbitos han contribuido al aumento del ancho de banda, la reducción de la latencia, la mejora en la eficiencia espectral y la habilitación de una gestión dinámica de red. Por ejemplo, el uso de antenas de haces dirigidos, así como la reutilización de frecuencias, y la modulación y codificación adaptativa (ACM) han permitido que los enlaces satelitales compitan con redes de banda ancha terrestre en términos de velocidad y calidad de servicio (Kota et al., 2004). Asimismo, los recientes avances en cargas útiles definidas por *software* y enlaces láser entre satélites aumentan la flexibilidad y la redundancia de la red³⁹.

A pesar de estos avances, las comunicaciones satelitales siguen enfrentando varios desafíos relacionados con la asignación de espectro, la congestión orbital, la atenuación atmosférica y la latencia, especialmente en sistemas de gran altitud. Minoli (2015) enfatiza la importancia de la optimización de protocolos, la gestión eficiente del ancho de banda y la integración híbrida con la infraestructura terrestre para lograr una experiencia de usuario fluida. Además, desde una perspectiva geopolítica, el control de las órbitas y las bandas de frecuencia (regulado por la Unión Internacional de Telecomunicaciones [UIT]) se ha convertido en una cuestión de interés nacional y de negociación diplomática, particularmente ante la expansión de las mega constelaciones de satélites por parte de actores privados respaldados por Estados poderosos.

³⁹ La introducción de antenas electrónicamente direccionables y de enlaces ópticos intersatelitales ha incrementado no solo el ancho de banda disponible, sino también la seguridad del canal frente a interferencias y la posibilidad de constituir mallas resilientes ante la caída de nodos individuales. Minoli (2015) destaca cómo los satélites de alto rendimiento (HTS) han incrementado la capacidad por haz en órdenes de magnitud, y facilitado así el soporte de aplicaciones de transmisión de video en 4K, servicios M2M, y conectividad en plataformas móviles como buques, aviones o vehículos de comando en campo de batalla.

En el contexto latinoamericano, y en el colombiano, las comunicaciones satelitales funcionan como un complemento de los despliegues de fibra óptica, especialmente en áreas remotas como la Amazonía, la costa Pacífica y la región del Orinoco. Las estrategias nacionales de conectividad, respuesta ante desastres y vigilancia de fronteras dependen cada vez más de servicios basados en satélites. Además, la posición geográfica estratégica de Colombia, cerca del ecuador, la convierte en un posible nodo para estaciones terrestres de satélites GEO y en un actor relevante dentro de la cooperación espacial regional. La Fuerza Aeroespacial Colombiana y la Comisión Colombiana del Espacio han reconocido la importancia de desarrollar capacidades soberanas en comunicaciones satelitales para garantizar autonomía estratégica y soberanía informacional (Álvarez et al., 2019d)⁴⁰.

En lo relativo a defensa y seguridad, los sistemas satelitales desempeñan funciones críticas que incluyen el mando y control (C2), la inteligencia, la vigilancia y el reconocimiento (ISR), la navegación y sincronización temporal (PNT), y las operaciones conjuntas de redes (C4ISR). Según Álvarez et al. (2019a), la arquitectura de comunicaciones satelitales constituye una columna vertebral para las funciones bélicas modernas, al facilitar el enlace entre fuerzas desplegadas, centros de comando y sistemas de armas inteligentes. La interrupción deliberada de estas redes, mediante ataques cibernéticos o cinéticos, puede generar una ventaja táctica sustancial degradando la capacidad de un adversario para coordinar sus movimientos, detectar amenazas o ejecutar maniobras sincronizadas.

Sin embargo, la resiliencia de estos sistemas depende de capacidades redundantes (redes terrestres, enlaces alternos por radio, enlaces cifrados), y de la velocidad con que una fuerza puede adaptarse a la degradación del sistema principal. La doctrina militar estadounidense, por ejemplo, reconoce que la superioridad en C4ISR (apoyada por plataformas satelitales) puede ser un factor decisivo en conflictos de alta intensidad, pero también admite que estas capacidades son vulnerables ante ataques sofisticados en el dominio cibernético.

Desde una perspectiva geopolítica, el control y operación de constelaciones satelitales se ha convertido en un instrumento de soberanía digital y proyección de poder. Estados con capacidades espaciales avanzadas (como Estados Unidos, China y Rusia) están utilizando redes LEO y GEO para consolidar su autonomía tecnológica, garantizar el dominio informacional y disputar el control de los flujos

⁴⁰ El desarrollo de los programas FACSAT-1 y FACSAT-2 marcó un hito en la capacidad nacional para desplegar satélites de propósito específico y participar activamente en la gobernanza del espacio cercano. De acuerdo con Minoli (2015), la capacidad de un Estado para desarrollar y operar sistemas satelitales es no solo un indicador de autonomía tecnológica, sino también un prerrequisito para consolidar la soberanía en el dominio digital.

globales de datos. Como indican Álvarez et al. (2019c), la soberanía cibernética implica no solo el control legal del tráfico de datos, sino también el dominio físico de la infraestructura, lo que incluye los satélites, estaciones de control y nodos de interconexión terrestre. En este sentido, el despliegue de redes como Starlink o el sistema chino BeiDou va más allá de su funcionalidad técnica, ya que representan dispositivos estratégicos para asegurar el control territorial en el espacio digital y reducir la dependencia de infraestructuras controladas por potencias rivales.

En el caso del Estado colombiano, la dependencia de capacidades satelitales extranjeras (tanto para defensa como para conectividad civil) representa un desafío estructural. Si bien el país avanzó con el programa FACSAT, particularmente con el desarrollo y operación de satélites de observación como el FACSAT-1 y el FACSAT-2 (los cuales ya alcanzaron el final de su vida operativa), la cobertura y autonomía satelital nacional continúan siendo limitadas, especialmente en el ámbito de las comunicaciones. En este contexto, el desarrollo del programa FACSAT-3, que contempla el despliegue de nuevos activos espaciales, constituye un paso relevante hacia la consolidación de capacidades propias, aunque aún insuficiente frente a las demandas estratégicas del entorno contemporáneo.

Fortalecer la arquitectura nacional en órbita baja y media, en cooperación con socios estratégicos y mediante políticas industriales de largo plazo, es una prioridad para garantizar la soberanía digital, la cobertura nacional en zonas remotas y la capacidad de respuesta frente a amenazas ciberespaciales. Como lo demuestra la experiencia internacional, el ciberespacio no es un dominio puramente virtual, sino un entramado material con profundas implicaciones geoestratégicas.

Espectro electromagnético

Si bien los satélites constituyen un componente visible y emblemático de la infraestructura física del ciberespacio, operan gracias a un sustrato invisible, pero absolutamente esencial, conocido como el espectro electromagnético (EM), el cual se establece como una dimensión física natural que sostiene buena parte de las infraestructuras de comunicación modernas. El EM comprende todo el rango de frecuencias de radiación electromagnética presentes en el medio ambiente, desde las ondas de radio de baja frecuencia hasta los rayos gamma, de altísima energía. Aunque la mayor parte de este espectro es imperceptible al ojo humano (salvo una estrecha franja, que corresponde a la luz visible), constituye el medio a través del cual se propaga la información digital en redes inalámbricas, móviles y satelitales.

En particular, las frecuencias más relevantes para el funcionamiento del ciberespacio se concentran en los rangos de radiofrecuencia y microondas, que

abarcan aproximadamente desde los 600 kHz hasta los 100 GHz. Esta porción del EM permite la transmisión de datos en redes Wi-Fi, comunicaciones móviles, enlaces satelitales, radares, televisión abierta y señales de radio AM y FM. Sin este medio físico, las comunicaciones digitales sin cables, como las que sustentan a las constelaciones de satélites de órbita baja o los sistemas GNSS, serían técnicamente inviables. Así, el ciberespacio no existe como una entidad aislada o puramente virtual, sino que se sostiene sobre fundamentos físicos (entre ellos, el EM), que le permiten operar, expandirse y conectar dispositivos a escala planetaria.

Aunque el EM y el ciberespacio son esferas conceptuales distintas, mantienen una relación de dependencia funcional. El ciberespacio, entendido como una construcción sociotécnica, se asienta sobre la infraestructura física habilitada por el uso del espectro. Sin embargo, este último excede con mucho los límites del ciberespacio, ya que abarca fenómenos naturales y aplicaciones físicas no digitales. Aun así, esta superposición ha generado una interdependencia estratégica que se traduce en capacidades, vulnerabilidades y desafíos compartidos.

Este vínculo cobra especial importancia en el dominio militar, donde el control del EM ha sido históricamente una prioridad. Desde hace décadas, las fuerzas armadas han desarrollado capacidades de guerra electrónica (GE), con el fin de obtener ventajas tácticas y estratégicas. Estas operaciones buscan asegurar el acceso propio y negar el del adversario al espectro, particularmente en las frecuencias críticas para el comando, control, comunicaciones e inteligencia. La GE incluye acciones de detección, interferencia, engaño, bloqueo, degradación, protección o destrucción de sistemas que dependen del espectro. Así, el espectro se convierte en un campo de batalla invisible, donde los flujos de datos y señales pueden ser interrumpidos, distorsionados o neutralizados como parte de una campaña militar.

De hecho, la integración entre el ciberespacio y el EM ha propiciado nuevas formas de confrontación. Según Cole (2014), la GE contemporánea incluye no solo técnicas convencionales como el *jamming* de radares, sino también tecnologías emergentes, como las armas de energía dirigida. La Marina de los Estados Unidos, por ejemplo, ya ha desplegado sistemas láser para neutralizar amenazas en tiempo real, mientras que la Fuerza Aérea explora dispositivos como el misil CHAMP (*Counter-Electronics High Power Microwave Advanced Missile Project*), capaz de emitir un pulso electromagnético (PEM) que inutiliza la electrónica enemiga sin causar daños colaterales físicos⁴¹. Un ataque por PEM ocurre cuando un artefacto

⁴¹ Un PEM es una emisión de energía electromagnética de alta intensidad proveniente de una gran explosión (sobre todo, una explosión nuclear) o de un campo magnético que fluctúa intensamente causado por la fuer-

explosivo, ya sea convencional o nuclear, detona a gran altitud y genera una onda de choque electromagnética capaz de interferir drásticamente con los campos electromagnéticos naturales de la Tierra.

Si bien las explosiones convencionales pueden producir efectos limitados, una detonación nuclear a gran altitud produce una perturbación significativamente más poderosa y extendida. La intensidad, duración y extensión geográfica del daño provocado por un PEM dependen en gran medida de la altitud de la explosión: a mayor altitud, mayor será el radio de afectación en la superficie terrestre. Por ejemplo, una explosión nuclear a 80 km de altitud podría generar un área de impacto en tierra con un radio de aproximadamente 965 km. Si la detonación ocurriera a 160 km, este radio se ampliaría hasta los 1.448 km. A 321 km de altitud, un PEM detonado sobre el centro de Colombia podría afectar a casi la totalidad del territorio nacional, así como extensas zonas de Ecuador y Venezuela. A diferencia de una explosión a nivel del suelo, el daño térmico o incendiario en estos escenarios sería mínimo o inexistente, mientras que los efectos electromagnéticos serían devastadores.

El PEM representa una amenaza crítica para la infraestructura digital y eléctrica moderna, dado que sus principales víctimas son los sistemas basados en componentes electrónicos de estado sólido. La red eléctrica, los computadores y los dispositivos de comunicaciones son extremadamente sensibles a este tipo de perturbación. Dado el alto grado de interconexión entre los sistemas eléctricos, digitales y logísticos, así como la dependencia generalizada de estos para el funcionamiento de la sociedad, las consecuencias de un PEM podrían ser catastróficas. Los daños podrían oscilar entre la degradación funcional temporal (con la pérdida de capacidad operativa por días o semanas) y la destrucción permanente de sistemas críticos, lo cual afectaría no solo las comunicaciones, sino también sectores vitales como la salud, el abastecimiento de agua, la cadena alimentaria, el transporte y los sistemas financieros. Paradójicamente, los sistemas más avanzados tecnológicamente serían también los más vulnerables, mientras que tecnologías más antiguas o menos sofisticadas, con componentes analógicos o blindaje natural, podrían resistir mejor sus efectos⁴². Esta asimetría subraya la fra-

za de empuje del "efecto Compton" (aumento de la longitud de onda de un fotón cuando choca con un electrón libre y pierde parte de su energía). Los campos eléctricos y magnéticos resultantes pueden interferir en los sistemas eléctricos y electrónicos de un adversario provocando picos de tensión que pueden dañar dichos sistemas. En el caso de una explosión con pulso electromagnético en altitud, es posible inutilizar todos los sistemas electrónicos de un país.

⁴² Es posible proteger el equipo electrónico de los ataques de PEM mediante el blindaje o el endurecimiento del equipo. Un escudo compuesto de un metal continuo, como acero, cobre o hierro blando, si rodea por completo el sistema, puede protegerlo de los ataques de PEM.

gilidad estructural de las sociedades digitalizadas frente a fenómenos de disrupción extrema como los PEM.

Por consiguiente, los atributos físicos del entorno ciberespacial pueden ser manipulados intencionalmente como vector de guerra o sabotaje para negar el acceso de un adversario a las redes digitales. Aunque los cables de fibra óptica, en especial los submarinos, constituyen la columna vertebral de la infraestructura del ciberespacio, su redundancia y distribución geográfica hacen que su destrucción total exija una acción coordinada y masiva. Los satélites, por su parte, ofrecen resiliencia adicional y son esenciales para la conectividad en entornos remotos o desplegados, aunque tienen limitaciones de capacidad y son susceptibles de interferencia o destrucción física. Frente a esta arquitectura diversa, el PEM destaca como la amenaza más global y destructiva, capaz de aniquilar simultáneamente la infraestructura electrónica, digital y de comunicaciones en vastas regiones. Sin embargo, debido a sus efectos indiscriminados y potencialmente catastróficos (que podrían traducirse en crisis humanitarias, colapsos sistémicos y pérdida de vidas), el uso deliberado de armas PEM de origen nuclear está prohibido por tratados internacionales como el Tratado de Prohibición Completa de los Ensayos Nucleares (en inglés, CTBT, por las iniciales de Comprehensive Nuclear-Test-Ban Treaty) y normativas asociadas al Derecho Internacional Humanitario (DIH).

En suma, el ciberespacio no debe concebirse como un reino inmaterial separado del mundo físico, sino como una extensión funcional de la infraestructura terrestre, orbital y espectral. El EM, aunque imperceptible a la vista, es una dimensión tangible y disputada, donde confluyen intereses civiles, comerciales y estratégicos. Comprender su dinámica es esencial para evaluar la seguridad, la resiliencia y la soberanía en la era digital, así como para anticipar los escenarios futuros en los que la GE, las operaciones cibernéticas y las plataformas espaciales convergen en una misma arquitectura de poder.

Los centros de datos

Finalmente, los centros de datos (*Data Centers*) son nodos esenciales de la infraestructura física del ciberespacio. Actúan como almacenes de información, procesadores de datos y plataformas de IA, por lo que constituyen el corazón digital de la economía, la política y la vida cotidiana del siglo XXI, y su relevancia se ha intensificado con la expansión de la computación en la nube, el IoT, el 5G y, sobre todo, la IA generativa, cuyos modelos demandan enormes volúmenes de procesamiento y almacenamiento de datos. En ese contexto, los centros de datos no son

solo espacios técnicos: son infraestructuras estratégicas cuya localización, abastecimiento energético, seguridad física y control administrativo se han convertido en objetos de disputa geopolítica.

En términos técnicos, un centro de datos es una instalación que alberga sistemas informáticos y componentes asociados, como servidores, dispositivos de almacenamiento, infraestructura de red y sistemas de refrigeración. Su diseño es condicionado por múltiples factores, como: requisitos de latencia, densidad de energía, seguridad ambiental, resiliencia ante fallas y acceso a conectividad de alta velocidad. El crecimiento exponencial de los datos, sumado a la sofisticación de las aplicaciones digitales contemporáneas, ha impulsado una transformación profunda en la arquitectura de estos centros de datos, que ahora adoptan configuraciones modulares, escalables y automatizadas, con una eficiencia energética optimizada a través de inteligencia ambiental, algoritmos de aprendizaje automático y sistemas de refrigeración líquida (Stacciarini & Gonçalves, 2025).

Empero, detrás de esta aparente neutralidad técnica subyacen relaciones de poder global. Como señala Capri (2024b), los centros de datos no solo gestionan la información, sino que controlan flujos digitales estratégicos que afectan desde el comercio hasta la soberanía digital de los Estados. El "nuevo realismo geodigital" se articula, en este sentido, a partir de la infraestructura crítica que representan los data centers. Estados Unidos, por ejemplo, ha promovido marcos regulatorios como el CHIPS Act y la Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, para garantizar el control de sus redes digitales, limitar la dependencia de actores adversarios como la República Popular de China y proteger el abastecimiento energético y de minerales críticos que sustentan sus instalaciones de procesamiento de datos.

A escala global, estos centros se agrupan en regiones con disponibilidad energética, estabilidad política, marcos legales robustos y conectividad redundante. Zonas como el norte de Europa, el noreste de los Estados Unidos y el sudeste asiático (Singapur, Malasia y Vietnam) se han consolidado en los últimos años como *hubs* de infraestructura digital. Esta geografía de la computación refleja no solo las capacidades técnicas, sino también las alianzas estratégicas y los intereses de seguridad nacional. El caso del Ártico y los países nórdicos es particularmente ilustrativo, ya que su clima frío permite reducir el gasto energético en refrigeración, mientras que su matriz energética renovable y su integración al mercado europeo les confiere ventajas competitivas en la economía del dato (Capri, 2024b).

En efecto, la sostenibilidad energética es un factor crucial, debido a que los centros de datos son instalaciones intensivas en electricidad, y su proliferación

plantea desafíos significativos para las matrices energéticas nacionales. Algunos informes estiman que para 2030 dichos centros podrían consumir hasta el 13 % de la demanda eléctrica mundial. Esta presión energética se traduce en una competencia global por el acceso a fuentes renovables, la eficiencia energética de las instalaciones y la adopción de tecnologías como el enfriamiento líquido directo, los sistemas de recuperación de calor y la arquitectura *Edge Computing*. Stacciarini y Gonçalves (2025) destacan que los centros de datos están entrelazados con los minerales críticos que hacen posible su funcionamiento: cobre, aluminio, neodimio, litio y cobalto, entre otros. La extracción, refinamiento y comercialización de esos minerales plantea una cadena de valor global en la que los países latinoamericanos, africanos, e incluso algunos del sudeste asiático, ocupan posiciones subordinadas, en tanto proveedores de materias primas.

Desde una perspectiva latinoamericana, y con relación a la geopolítica digital, la región enfrenta una doble condición. Por un lado, se ve afectada por asimetrías estructurales en la economía de los datos, como limitada infraestructura de data centers de clase mundial, dependencia tecnológica de actores externos y baja inversión en capacidades soberanas de almacenamiento, procesamiento y ciberseguridad. Y por el otro lado, América Latina posee ventajas comparativas estratégicas, gracias a la abundancia de recursos minerales, reservas energéticas significativas (particularmente, en energías limpias) y una población joven altamente conectada. De hecho, países como Brasil, México y Chile han comenzado a atraer inversiones de *hyperscalers*⁴³ como Amazon Web Services, Microsoft y Google instalando centros de datos de última generación en sus territorios, usualmente concentrados en zonas metropolitanas con acceso a infraestructura energética y conectividad internacional.

Por su parte, la ubicación estratégica de Colombia entre dos océanos y su acceso a múltiples cables submarinos la posicionan como un actor emergente en el ecosistema regional de infraestructura digital, al concentrar aproximadamente el 9 % del mercado de data centers en América Latina. Esta participación refleja una creciente relevancia del país en la arquitectura física del ciberespacio continental, impulsada tanto por su localización geográfica estratégica como por la expansión de su economía digital. Actualmente, el territorio colombiano alberga más

⁴³ En el contexto de la computación en la nube, un hyperscaler (o hiperescalar) es una empresa que ofrece servicios de computación a gran escala utilizando centros de datos masivos y una infraestructura informática distribuida para satisfacer las demandas de grandes organizaciones. Estos proveedores son capaces de escalar sus recursos de manera flexible para adaptarse a las necesidades cambiantes de sus clientes, en términos tanto de potencia de cálculo como de almacenamiento.

de 20 *Data Centers* instalados⁴⁴, los cuales suman una capacidad superior a los 14.000 m² destinados a albergar servidores, sistemas de almacenamiento, redes y demás componentes esenciales para el procesamiento y la gestión de datos (La República, 2024).

Según datos abiertos consolidados hasta 2022, los ingresos generados por el sector de *Data Centers* en Colombia superaban los 37 millones de dólares, lo que evidencia un crecimiento sostenido de este segmento económico. En el horizonte regional se proyecta que la inversión acumulada en estos centros en América Latina alcanzará los 10.000 millones de dólares para 2029 (La República, 2024), en un contexto de transformación digital acelerada. Colombia, junto con Brasil, México y Chile, figura entre los principales países tanto en la oferta como en el consumo de servicios asociados a centros de datos, lo cual refuerza su posición dentro de las cadenas de valor digital del hemisferio. Además, la proyección de crecimiento anual compuesto del sector se estima en el 7,95 % entre 2024 y 2029, lo cual sugiere una expansión no solo en el volumen de infraestructura, sino también en una creciente sofisticación tecnológica y demanda más intensiva en capacidad computacional. Este dinamismo convierte al ecosistema de *Data Centers* en una dimensión crítica para la soberanía digital, la competitividad económica y la seguridad informacional de Colombia en el contexto de la economía del conocimiento.

En este marco, se vuelve imperativo adoptar una perspectiva de seguridad nacional en torno a los *Data Centers*. Como infraestructuras críticas, su integridad física y lógica debe ser protegida frente a amenazas naturales, cibernéticas y geopolíticas. Capri (2024b) advierte sobre la creciente *proxy war* digital, en la que Estados compiten indirectamente mediante restricciones regulatorias, espionaje económico, imposición de estándares técnicos y alianzas estratégicas. En ese contexto, los centros de datos operan como campos de disputa silenciosa entre las potencias digitales, y su control puede acabar determinando el acceso a tecnologías emergentes como la IA, el *blockchain*, la biotecnología computacional y la guerra algorítmica.

La geopolítica de los *Data Centers* se entrelaza, además, con la arquitectura institucional global. Las decisiones sobre localización, inversión, regulación y

⁴⁴ El ecosistema colombiano de *data centers* ha mostrado un crecimiento notable, aunque desigual, ya que Bogotá concentra la mayor parte de los centros de datos comerciales, aprovechando su conectividad terrestre, su rol como nodo económico nacional y la relativa estabilidad institucional. Sin embargo, regiones como Antioquia, el Eje Cafetero y la costa del Caribe empiezan a emerger como potenciales nodos de descentralización digital, particularmente en ciudades como Medellín, que ha impulsado políticas de innovación y transformación digital.

gobernanza de los centros de datos no son neutras. Empresas tecnológicas como Amazon, Google o Huawei tienen la capacidad para condicionar políticas públicas, exigir exenciones fiscales o rediseñar normas sobre privacidad, competencia y ciberseguridad. Esto plantea un dilema estructural: ¿cómo garantizar la soberanía digital de los países cuando los datos, las infraestructuras y los algoritmos son controlados por corporaciones transnacionales cuyo poder excede al de muchos Estados? En América Latina diversos países han empezado a reconocer que los datos constituyen activos estratégicos cuyo resguardo es clave para el ejercicio de la soberanía digital. En respuesta, se han adoptado marcos regulatorios que busquen limitar el uso indebido de la información personal y garantizar la protección de los ciudadanos frente a los riesgos de un entorno digital cada vez más complejo.

Un caso destacado es el de Brasil, cuya Ley General de Protección de Datos (LGPD) establece principios claros sobre el tratamiento de datos personales y crea una autoridad nacional encargada de su regulación y supervisión. No obstante, a pesar de dichos avances, aún no se ha conformado una estrategia regional coherente que integre de manera sistémica los pilares de soberanía tecnológica, protección de datos, ciberseguridad e infraestructura crítica.

En el caso colombiano, existe la Ley 1581 de 2012, también conocida como Ley de Habeas Data, la cual consagra el derecho fundamental de los ciudadanos a conocer, actualizar y rectificar la información que reposa en bases de datos públicas y privadas. Dicha legislación establece principios, deberes y procedimientos para el tratamiento adecuado de los datos personales, y ha sido complementada por otras disposiciones normativas que fortalecen el ecosistema jurídico en materia de protección de la información. No obstante, estos esfuerzos normativos aún no se han articulado con una política nacional de infraestructura de datos que incorpore componentes estratégicos como la planificación energética sostenible para centros de datos, la formación de capital humano especializado y el establecimiento de alianzas tecnológicas que aseguren autonomía e innovación local. Así, Colombia avanza en materia de gobierno digital, conectividad y ciberseguridad, pero persiste el reto de desarrollar una visión integral que sitúe la infraestructura de datos como pilar de su desarrollo soberano en la era digital.

Por lo tanto, el debate sobre los centros de datos debe ir más allá de la eficiencia técnica o la rentabilidad económica. Se trata de entenderlos como infraestructuras materiales de la soberanía informacional y como eslabones clave en las nuevas configuraciones del poder global. En un contexto de creciente rivalidad entre Estados Unidos y la República Popular de China, reconfiguración del orden digital

y emergencia de amenazas híbridas, garantizar el control soberano, seguro y sostenible de los centros de datos es una tarea urgente para todos los países, especialmente aquellos del Sur Global que buscan superar su dependencia estructural y participar activamente en la economía digital del siglo XXI.

Geopolítica y soberanía digital

Desde una perspectiva geopolítica, el ciberespacio puede ser concebido como un “territorio” no físico, pero funcional, construido a partir de infraestructuras técnicas (como cables submarinos, satélites, *Data Centers*, EM y servidores), y sostenido por normas, protocolos, códigos y sistemas lógicos que median las interacciones humanas, comerciales y gubernamentales. Esta dimensión inmaterial, pero políticamente densa, redefine la noción clásica de territorio y proyecta nuevas formas de poder, control y conflicto (Kadlecová, 2024; Jelinek, 2023).

La geografía del ciberespacio no responde a la lógica de los Estados nación en términos de fronteras físicas, sino a configuraciones reticulares que se estructuran en torno a *hubs* tecnológicos, nodos de interconexión, jurisdicciones fiscales favorables y regímenes normativos de carácter transnacional. Tal como advierte Kadlecová (2024), la emergencia del concepto de “soberanía cibernética” implica una reformulación de la autoridad estatal ante infraestructuras digitales distribuidas globalmente y operadas por actores privados. Las funciones soberanas tradicionales (como la protección del territorio, la gestión de recursos estratégicos y la regulación de las comunicaciones) deben ahora ejercerse sobre infraestructuras intangibles, ubicuas y altamente dependientes de empresas transnacionales que actúan como nuevos poderes geopolíticos.

Este nuevo escenario territorial digital tiene implicaciones para la seguridad nacional, la autonomía estratégica y la resiliencia estatal. La infraestructura crítica del ciberespacio (como los puntos de intercambio de internet [IXP], los sistemas autónomos [AS], los servidores raíz del DNS o los cables de fibra óptica) constituye un espacio geotécnico cuya localización física, nivel de control y capacidad de intervención directa por parte de los Estados varía considerablemente entre países (Jelinek, 2023; Chander & Sun, 2023). Como subraya Kokas (2022), la mayoría de dichas infraestructuras se hallan radicadas en territorios o bajo el control normativo de Estados como Estados Unidos y China, lo que genera relaciones de dependencia digital que reproducen desequilibrios históricos del orden internacional.

Además, el ciberespacio representa un campo de disputa no solo territorial, sino también simbólica y narrativa. La batalla por los estándares tecnológicos, las plataformas dominantes y los modelos de gobernanza digital se manifiesta también como una pugna por definir los marcos normativos que rigen la conducta en este nuevo territorio. Así, el control sobre los flujos de datos, los algoritmos que rigen la visibilidad informativa, y las infraestructuras de IA y computación en la nube constituyen nuevas formas de “territorialización” digital (Bellanova et al., 2021). En ese sentido, hablar de geopolítica del ciberespacio implica comprender cómo los espacios digitales están siendo cartografiados, controlados y defendidos como si se tratase de espacios físicos estratégicos.

En la región latinoamericana esta territorialización digital se manifiesta en una arquitectura fragmentada, dependiente de infraestructuras externas y con limitada capacidad de gobernanza sobre sus nodos estratégicos. Colombia, por ejemplo, depende de cables submarinos internacionales, servidores radicados en el extranjero y servicios de almacenamiento en la nube gestionados por corporaciones extranjeras, lo que limita sus márgenes de soberanía y autonomía digital. Si bien se han realizado avances en conectividad y ciberseguridad, el país aún carece de una estrategia nacional que articule infraestructura, datos, normas y capacidades soberanas en el entorno digital. Esta situación hace evidente la necesidad de pensar el ciberespacio no solo como un ámbito técnico, sino como un espacio geopolítico que debe ser defendido, gobernado y disputado con visión estratégica.

Actores, intereses y conflictos en la gobernanza de la red

En el entramado contemporáneo de la geopolítica digital la gobernanza de internet se ha vuelto un campo de competencia estratégica entre actores estatales, corporativos y supranacionales. Lejos de ser una estructura neutra y descentralizada, la red global de datos se configura como un espacio de poder disputado, donde la influencia sobre las normas técnicas, los protocolos de enrutamiento y el control del flujo de información se ha vuelto tan relevante como el dominio de territorios físicos en épocas anteriores (Jelinek, 2023).

Entre los principales actores se encuentran los Estados nacionales, que buscan ejercer soberanía sobre los datos generados por sus ciudadanos y empresas dentro de sus fronteras. Esta tendencia ha derivado en una diversidad de iniciativas, desde la promoción de modelos de internet soberana (como el *Runet* ruso) hasta la exigencia de localización de datos, como lo establece China con su estrategia del “Gran Cortafuegos”, y diversas leyes de ciberseguridad y protección de

información personal (Chander & Sun, 2023). Esos Estados articulan sus intereses en torno a una lógica de seguridad nacional, control político y defensa de la soberanía territorial reconfigurada para el ciberespacio (Kokas, 2022).

En ese marco los casos de Rusia y China ilustran dos modelos diferenciados, pero convergentes, de cartografiar el ciberespacio como espacio estratégico sujeto a soberanía estatal. En ambos internet deja de concebirse como un dominio global abierto y pasa a ser tratado como una infraestructura crítica cuya gobernanza resulta inseparable de la seguridad nacional, el control político y la proyección de poder. Sin embargo, las trayectorias históricas y doctrinales de cada país revelan lógicas distintas en la forma de ejercer dicho control.

En el caso ruso, el desarrollo del *Runet* debe entenderse como el resultado de una evolución histórica específica del sistema mediático y comunicacional nacional. Como señala Vartanova (2020), internet se integró tempranamente en una estructura mediática caracterizada por la centralidad del Estado, al igual que por una concepción securitaria de la información. En este contexto, el *Runet* emerge no solo como un espacio técnico de conectividad, sino como una extensión del ecosistema mediático nacional, donde la soberanía informativa precede y condiciona la expansión digital. Konradova (2020) muestra que esta evolución atravesó distintas etapas, desde una fase inicial relativamente abierta en los años noventa hasta un proceso progresivo de institucionalización, recentralización regulatoria y control infraestructural a partir de la década de 2010.

Este tránsito refleja un cambio doctrinal clave: internet pasa de ser percibido como un espacio global desregulado a ser concebido como una infraestructura estratégica cuya continuidad debe garantizarse incluso en escenarios de crisis, sanciones o conflicto híbrido. La capacidad técnica de aislar el *Runet* del resto de la red global, junto con el control de puntos de intercambio y marcos legales de soberanía digital, responde a una lógica de resiliencia estatal y control narrativo en contextos de guerra informacional. En este sentido, la soberanía digital rusa se orienta menos a la ingeniería social cotidiana, y más, a la defensa del orden interno y la estabilidad del Estado frente a amenazas externas, particularmente en el plano cognitivo y mediático.

El modelo chino, en contraste, representa una concepción más integral y proactiva de la soberanía digital. El denominado Gran Cortafuegos no constituye simplemente un sistema de censura, sino una arquitectura compleja de gobernanza del ciberespacio destinada a construir y controlar una versión alternativa de internet coherente con los objetivos políticos del Partido-Estado. Como explica

Griffiths (2021), el proyecto chino busca no solo bloquear contenidos externos, sino rediseñar el ecosistema digital completo (es decir, infraestructuras, plataformas, flujos de datos y comportamientos de los usuarios), bajo una lógica de control, estabilidad y legitimidad política.

Desde esta perspectiva, el Gran Cortafuegos de China funciona como una cartografía deliberada del ciberespacio, en la que las fronteras digitales adquieren un estatus comparable al de las fronteras territoriales. A diferencia del enfoque ruso, China combina el control infraestructural con una estrategia de sustitución tecnológica y promoción de plataformas nacionales reduciendo la dependencia de actores occidentales y reforzando su autonomía estratégica. Además, como subraya Griffiths (2021), este modelo incorpora una dimensión avanzada de gobernanza algorítmica, donde la vigilancia masiva, el análisis de datos y la IA permiten no solo censurar información, sino anticipar comportamientos sociales y modelar dinámicas colectivas.

En términos estratégicos, ambos modelos revelan que la soberanía digital no es una noción homogénea, sino un conjunto de prácticas diferenciadas de control del ciberespacio. Mientras Rusia prioriza la resiliencia, la continuidad del Estado y el control narrativo en los escenarios de confrontación informacional, la República Popular de China concibe el ciberespacio como una extensión estructural del orden político interno y un instrumento de proyección de poder externo. No obstante, en ambos casos, la cartografía del ciberespacio aparece profundamente politizada: los datos, las plataformas y las infraestructuras digitales se transforman en vectores de poder estratégico, por lo que redefinen los límites entre seguridad, gobernanza y soberanía en el siglo XXI.

Junto a los Estados, las corporaciones tecnológicas globales (en particular, las grandes plataformas de origen estadounidense, como Google, Meta y Amazon), desempeñan un papel central en la infraestructura técnica y el gobierno efectivo de la red. Estas compañías controlan servidores, servicios en la nube, estándares de autenticación y hasta la economía de la atención, lo que les otorga un poder fáctico que desafía las estructuras regulatorias tradicionales. Ese fenómeno ha sido conceptualizado como una "privatización de la soberanía digital" o, en términos más críticos, como la emergencia de un "feudalismo digital", donde las plataformas sustituyen funciones del Estado (Glasze et al., 2023). La gobernanza multilateral y *multi-stakeholder*, tradicionalmente canalizada a través de organismos como Internet Corporation for Assigned Names and Numbers (ICANN) o el Foro de Gobernanza de Internet (en inglés, IGF, por las iniciales de Internet Governance

Forum), también ha sido objeto de disputas. China y Rusia han criticado la hegemonía occidental sobre los recursos centrales de internet, como el sistema de nombres de dominio (DNS), y fomentado propuestas alternativas en la Unión Internacional de Telecomunicaciones (UIT) para redefinir los principios de gobernanza global de la red (Kadlečová, 2024).

Estos conflictos geopolíticos también se manifiestan en dimensiones jurídicas y comerciales. La exportación de modelos regulatorios, como el Reglamento General de Protección de Datos (en inglés, GDPR, por las iniciales de General Data Protection Regulation), de la UE, representa una estrategia para proyectar “soberanía normativa” más allá de sus fronteras influyendo en la forma como se trata la privacidad y la protección de datos en contextos no europeos (Chander & Sun, 2023). En este sentido, la “soberanía digital” es un instrumento de *soft power*, aunque también un campo de fricción cuando choca con los modelos más permisivos o autoritarios de otros Estados (Jelinek, 2023).

En América Latina la región se posiciona como espacio de competencia entre diferentes visiones de gobernanza digital. Mientras algunos países adoptan marcos normativos alineados con estándares europeos (como Brasil, con su Ley General de Protección de Datos), otros han sido receptores de infraestructura tecnológica impulsada por China, lo que genera una creciente dependencia de proveedores asiáticos para servicios de conectividad, centros de datos y plataformas de vigilancia. Colombia, por ejemplo, ha firmado acuerdos con proveedores globales de servicios en la nube, pero aún carece de una política integral sobre soberanía tecnológica, lo que la expone a riesgos de subordinación digital (Glasze et al., 2023).

Este entramado de intereses y conflictos ha llevado a algunos autores a proponer una tipología de actores y sus agendas: por un lado, los Estados democráticos que promueven un “internet abierto y libre”, aunque con tensiones internas sobre vigilancia y control. Por otro, los regímenes autoritarios que ven la red como una amenaza al control político y la utilizan para censura y represión. Y finalmente, las empresas transnacionales que buscan mantener un entorno desregulado que favorezca sus intereses económicos y capacidad de acumulación de datos (Kokas, 2022). La noción de “soberanía digital”, entonces, se convierte en un campo de batalla discursivo y normativo, donde cada actor intenta imponer su visión del orden digital. La gobernanza de internet se trata ya no solo de aspectos técnicos o regulatorios, sino, además, de una profunda disputa sobre valores, modelos de sociedad y configuraciones de poder en el siglo XXI (Kadlečová, 2024).

La soberanía digital no puede comprenderse de forma aislada del control material sobre las infraestructuras que hacen posible el funcionamiento del

ciberespacio. Las lógicas de dependencia tecnológica y los riesgos asociados a la tercerización de servicios esenciales convierten a la infraestructura crítica digital en un campo estratégico para los Estados nacionales. Desde los cables submarinos que transportan la mayor parte del tráfico mundial de datos hasta los *Data Centers* que concentran el almacenamiento y procesamiento de información, pasando por los satélites de comunicaciones y las redes 5G, la soberanía digital se juega también en el dominio de la infraestructura física (Capri, 2024b).

El control de esa infraestructura no se distribuye equitativamente. La mayor parte de los centros de datos en la nube están concentrados en Estados Unidos y Europa, y las principales empresas que los operan pertenecen a un puñado de corporaciones tecnológicas, como Amazon Web Services, Microsoft Azure y Google Cloud (Jelinek, 2023). Este dominio les permite procesar, almacenar y analizar enormes volúmenes de datos generados incluso en otras partes del mundo, lo cual constituye un mecanismo de poder que escapa de los marcos normativos tradicionales. Tal como advierte Kadlečová (2024), esa centralización de recursos digitales en manos de actores no estatales impone una asimetría estructural que erosiona la capacidad soberana de los Estados periféricos.

La dependencia tecnológica no se limita al almacenamiento de datos, sino que también abarca el uso de *software* propietario, la gestión de algoritmos opacos y la vulnerabilidad ante interrupciones del servicio. La interrupción de acceso a servicios digitales clave, como plataformas de comunicación, motores de búsqueda o servicios en la nube, puede tener efectos sistémicos sobre economías, gobiernos y sociedades, y ello muestra la condición de dependencia en la que se encuentran muchos países frente a un reducido núcleo de proveedores globales (Chander & Sun, 2023). Asimismo, los conflictos geopolíticos contemporáneos han demostrado que la infraestructura digital puede ser utilizada como instrumento de presión o exclusión. El caso del bloqueo de servicios digitales a Rusia por parte de varias compañías occidentales tras la invasión de Ucrania, en 2022, ilustró la capacidad de las plataformas para ejercer soberanía de facto, imponiendo sanciones digitales más allá de las instancias estatales (Jelinek, 2023). Esta situación ha reactivado en muchos países el interés en fortalecer capacidades tecnológicas propias y reducir la dependencia crítica.

En América Latina la problemática se manifiesta de forma aguda. Muchos países de la región carecen de centros de datos soberanos, redes propias de fibra óptica o satélites de comunicaciones, lo que los obliga a depender de infraestructura ubicada en otros continentes y administrada por actores extranjeros. Colombia, por ejemplo, posee una infraestructura de telecomunicaciones en expansión, pero

gran parte de sus servicios digitales dependen de centros de datos localizados en Estados Unidos y de *software* desarrollado por empresas extranjeras (Glasze et al., 2023). Esa dependencia plantea interrogantes sobre la capacidad efectiva del Estado colombiano para garantizar la confidencialidad, integridad y disponibilidad de la información estratégica.

Desde una perspectiva más amplia, la infraestructura crítica digital constituye el corazón de la soberanía en la era del capitalismo de datos. La posibilidad de ejercer autonomía sobre los flujos de información, proteger los datos personales de la ciudadanía y garantizar la continuidad operativa de los servicios esenciales depende, y de manera creciente, del control de esa infraestructura. Por ello, diversos autores (Kadlečová, 2024; Jelinek, 2023), han planteado la necesidad de avanzar hacia modelos de soberanía tecnológica que articulen capacidades estatales, alianzas público-privadas y cooperación regional, para reducir la vulnerabilidad estructural y consolidar un ciberespacio más equitativo.

Modelos de soberanía digital: comparativo internacional

El debate en torno a la soberanía digital ha llevado a la consolidación de al menos tres modelos internacionales diferenciados, que reflejan no solo intereses geopolíticos divergentes, sino también distintas concepciones sobre el rol del Estado, la privacidad y los derechos digitales. Dichos modelos pueden agruparse en los enfoques de la UE, de China y de Estados Unidos, que configuran las principales rutas regulatorias y normativas en la disputa por la gobernanza del ciberespacio global.

El modelo europeo, encabezado por el GDPR, se centra en una visión de la soberanía digital como protección de los derechos fundamentales, especialmente la privacidad y la autodeterminación informativa. Esa postura se traduce en una agenda normativa extraterritorial que busca exportar estándares de protección de datos mediante acuerdos comerciales, cláusulas espejo y decisiones de adecuación, con lo cual la soberanía digital se vuelve una herramienta de poder normativo global (Jelinek, 2023). La UE considera el ciberespacio un nuevo campo de acción política, en el cual deben garantizarse los valores democráticos, los derechos de los usuarios y el control soberano sobre los datos estratégicos, sin renunciar a la integración de los mercados digitales. En ese sentido, los paquetes regulatorios, como el Digital Services Act (DSA) y el Digital Markets Act (DMA), complementan la agenda de soberanía digital europea limitando el poder de las plataformas y fortaleciendo la transparencia algorítmica.

En contraposición, el modelo chino se articula en torno a la noción de *ciber-soberanía* (*wǎngluò zhǔquán*), que se basa en el principio de control estatal del

ciberespacio dentro de las fronteras nacionales. Dicho enfoque, arraigado en la tradición de seguridad del Estado chino, promueve el almacenamiento local de datos, el bloqueo de contenidos, la censura y el uso extensivo de tecnologías de vigilancia como herramientas legítimas para preservar el orden político y social (Kokas, 2022). La Ley de Ciberseguridad (2017), la Ley de Protección de Información Personal (2021) y la Ley de Seguridad de Datos (2021) forman parte de un complejo entramado regulatorio que consagra esta visión. La soberanía digital, para el Gobierno chino, es no solo un mecanismo de protección económica, sino una pieza clave para el control ideológico y la estabilidad política interna, en concordancia con la estrategia Made in China 2025 y el plan China Standards 2035.

Por su parte, el modelo de Estados Unidos se caracteriza por un enfoque marcadamente liberal, centrado en la autorregulación del mercado, la innovación y la supremacía de las plataformas tecnológicas como motores de desarrollo económico. A pesar de algunos intentos legislativos, como el California Consumer Privacy Act (CCPA), Estados Unidos carece de un marco federal integral sobre privacidad de datos. Ello ha generado tensiones con la UE, en especial tras la invalidez del acuerdo Privacy Shield por parte del Tribunal de Justicia de la Unión Europea, debido a los programas de vigilancia masiva como PRISM. Desde una perspectiva geopolítica, el discurso estadounidense sobre el "internet libre y abierto" busca contrarrestar tanto el autoritarismo digital chino como las restricciones normativas europeas, bajo el argumento de preservar un ecosistema digital global interoperable y competitivo (Chander & Sun, 2023).

Kadlečová (2024) propone una tipología útil para comprender estas tensiones, basada en tres arquetipos: la soberanía como autonomía estatal (modelo chino), la soberanía como protección de derechos (modelo europeo) y la soberanía como competitividad estratégica (modelo estadounidense). Esa clasificación permite entender cómo las disputas sobre la gobernanza digital se articulan en torno a diferentes valores fundacionales: el orden, la libertad y el poder. Para Kadlečová (2024), estas concepciones no necesariamente son incompatibles, pero su coexistencia crea fricciones regulatorias, fragmentaciones técnicas y desacuerdos diplomáticos sobre la gobernanza global de internet.

Además de las mencionadas potencias, han emergido posiciones intermedias o híbridas en otras regiones. América Latina, por ejemplo, muestra una geografía normativa desigual: mientras países como Brasil y México han adoptado marcos inspirados en el GDPR, otros dependen en gran medida de proveedores tecnológicos chinos o estadounidenses, sin una estrategia nacional de soberanía digital

articulada. La región enfrenta así el desafío de construir capacidades regulatorias y tecnológicas propias que le permitan negociar en mejores condiciones su inserción en la geopolítica digital (Chander & Sun, 2023). Por último, como advierte Jelinek (2023), el riesgo de la “trampa de la soberanía digital” reside en que la proliferación de modelos excluyentes puede desembocar en un *splinternet*: un ecosistema fragmentado donde cada bloque impone sus normas técnicas y políticas y socava la interoperabilidad global y la cooperación multilateral. La paradoja, según el autor, es que en nombre de la soberanía se corre el riesgo de erosionar los beneficios de una red digital abierta e interconectada.

Este panorama evidencia que la soberanía digital no es una categoría unívoca, sino un concepto en disputa que sintetiza tensiones históricas entre control estatal, libertad individual y poder corporativo. Su evolución futura dependerá de la capacidad de los Estados y organismos internacionales para negociar acuerdos comunes que reconozcan la diversidad de enfoques sin renunciar a principios compartidos de transparencia, seguridad, equidad y desarrollo humano en el entorno digital.

Desafíos y perspectivas para Colombia

En el contexto de la transformación digital global Colombia enfrenta desafíos estructurales significativos para consolidar una estrategia nacional de soberanía digital. Aunque el país ha mostrado avances importantes en conectividad, gobierno digital y legislación sobre protección de datos, aún carece de un enfoque integral que articule infraestructura crítica, capacidades tecnológicas, normativas y autonomía estratégica. La creciente centralidad del ciberespacio como nuevo territorio geopolítico (donde se entrecruzan intereses estatales, corporativos y ciudadanos) exige de Colombia una mirada más sistémica e intersectorial, para garantizar la seguridad, el desarrollo y la democracia en la era digital.

Uno de los principales desafíos radica en la dependencia tecnológica de actores extranjeros, especialmente en lo que respecta a infraestructura crítica como centros de datos, servicios en la nube, *hardware* de red y plataformas digitales. Como advierten Chander y Sun (2023), esta dependencia puede traducirse en una pérdida de control sobre los flujos de datos, la exposición a regímenes regulatorios externos o, incluso, vulnerabilidad frente a interferencias geopolíticas. En el caso colombiano, si bien existen inversiones en infraestructura local, buena parte de los servicios digitales utilizados por el Gobierno, las empresas y los ciudadanos colombianos está alojada en diversas plataformas operadas por corporaciones

globales (principalmente, estadounidenses y chinas), cuyas decisiones responden a lógicas extraterritoriales de mercado y seguridad nacional.

El país también enfrenta rezagos en el desarrollo de capacidades nacionales de almacenamiento, procesamiento y protección de datos. Aunque Colombia cuenta con más de 20 *Data Centers* y participa con aproximadamente el 9 % del mercado regional de centros de datos en América Latina, aún está lejos de consolidar una red robusta y soberana que le permita gestionar de manera autónoma sus activos digitales estratégicos. En cuanto al marco regulatorio, Colombia ha adoptado la Ley 1581 de 2012, o Ley de Habeas Data, que establece principios para la protección de los datos personales y crea la figura del titular como sujeto de derechos. No obstante, la evolución de los modelos internacionales de soberanía digital (como el GDPR europeo o la Ley de Protección de Información Personal en China) plantea nuevos estándares que demandan una actualización normativa permanente. De acuerdo con Kadlečová (2024), los países que no alinean sus marcos legales con los estándares internacionales corren el riesgo de quedar excluidos de cadenas de valor digitales y de enfrentar restricciones al flujo transfronterizo de datos.

A ello se suma el reto de la ciberseguridad, un pilar ineludible de la soberanía digital. Colombia ha registrado un incremento sostenido en los ciberataques a infraestructuras públicas y privadas, evidencia tanto de brechas técnicas como de limitaciones en la coordinación institucional. La existencia de una Política Nacional de Ciberseguridad es un paso importante, pero su efectividad depende de la implementación transversal en todos los niveles del Estado y de su articulación con el sector privado y la sociedad civil. En palabras de Jelinek (2023), sin un ecosistema de confianza digital que combine gobernanza, tecnología y cooperación multiactor la soberanía se diluye en un entramado de vulnerabilidades estructurales. Además, el país debe enfrentar los dilemas asociados al poder de las plataformas digitales y la concentración de datos. Empresas como Google, Meta, Amazon o TikTok operan con escasa supervisión sobre sus algoritmos, sus prácticas de recolección de datos o su impacto en el discurso público. Tal como señala Kokas (2022), esta situación configura un escenario de "extracción asimétrica de datos", donde los ciudadanos y gobiernos del Sur Global entregan información estratégica sin reciprocidad en términos de transparencia o participación en la gobernanza digital. En este sentido, la ausencia de una legislación colombiana sobre plataformas y servicios digitales (como el Digital Services Act europeo) limita la capacidad regulatoria del Estado para garantizar derechos fundamentales en el entorno digital.

Frente a todos los desafíos que se mencionan, el Estado colombiano tiene la oportunidad de articular una perspectiva propia de soberanía digital, construida sobre tres pilares interdependientes. El primero es el fortalecimiento de capacidades tecnológicas nacionales, incluyendo el desarrollo de infraestructura crítica (*Data Centers*, redes 5G, computación en la nube), el apoyo a industrias digitales locales y la promoción de estándares abiertos. El segundo es la consolidación de un marco normativo integral que proteja los derechos digitales, garantice la portabilidad y soberanía de los datos y permita al Estado ejercer su autoridad sin aislarse del entorno internacional. El tercero es la diplomacia digital, mediante la que Colombia pueda insertarse activamente en los foros multilaterales y regionales que definen la gobernanza del ciberespacio, desde la UIT hasta las negociaciones sobre flujos de datos en la Organización Mundial del Comercio.

Desde una perspectiva comparada, el país puede aprender de experiencias híbridas, como la de Brasil, que ha logrado combinar normas inspiradas en el GDPR con desarrollos propios como la Autoridad Nacional de Protección de Datos y el Marco Civil de Internet. También puede observar el enfoque de la India, que ha promovido una arquitectura de identidad digital soberana (*Aadhaar*) y ha establecido requisitos para el almacenamiento local de datos (*data localization*), aunque no exenta de críticas por su vigilancia estatal. En ambos casos, el elemento común es el intento de articular desarrollo económico, inclusión digital y autonomía estratégica frente a los grandes polos de poder tecnológico.

Finalmente, Colombia debe abordar los desafíos de la soberanía digital desde una lógica de ecosistema. Ello implica alinear esfuerzos del Estado, el sector privado, la academia y la sociedad civil en torno a una visión común, con objetivos claros, métricas de evaluación y mecanismos de gobernanza participativa. Como señala Kadlečová (2024), la soberanía digital no puede ser entendida únicamente como control estatal, sino como la capacidad colectiva de una sociedad para decidir sobre el diseño, el acceso y el uso de las tecnologías que estructuran su presente y su futuro. Para Colombia, el camino hacia dicha soberanía digital es también una apuesta por la democracia, el desarrollo y la dignidad en la era del dato.

Conclusiones

En el contexto contemporáneo el ciberespacio se presenta como un nuevo escenario de competencia geopolítica, donde la soberanía ya no se ejerce únicamente sobre territorios físicos, sino también sobre infraestructuras digitales, flujos

de datos y plataformas tecnológicas. A lo largo del capítulo se ha abordado con profundidad esta transformación, partiendo de una pregunta fundamental: ¿cómo se configura el ciberespacio como una arquitectura estratégica de poder, y qué implicaciones tiene para la soberanía digital, particularmente en Colombia y América Latina? La respuesta, elaborada mediante un análisis multinivel, permite concluir que el ciberespacio constituye un entorno híbrido (físico, lógico y simbólico), que habilita, media y condiciona el ejercicio de funciones esenciales del Estado, desde la defensa hasta la regulación económica y la gestión de la información. En ese marco, la noción de soberanía digital se convierte en un principio rector para formular políticas públicas y doctrinas de seguridad nacional, en tanto implica la capacidad de un Estado para controlar, proteger y gobernar de manera autónoma y estratégica su propio ecosistema digital (Kadlecová, 2024).

Uno de los hallazgos centrales del presente documento es que la infraestructura física del ciberespacio (integrada por cables submarinos, estaciones de aterrizaje, satélites, centros de datos y nodos de interconexión) constituye no solo una red técnica, sino un espacio geopolítico altamente disputado. Como han señalado Chander y Sun (2023), el control sobre dichas infraestructuras habilita formas de poder equivalentes al dominio de rutas marítimas o aéreas en siglos anteriores. Colombia, en este sentido, tienen una posición privilegiada, al contar con costas en dos océanos y ser punto de conexión de múltiples cables submarinos, lo cual la convierte en un activo estratégico para la región. Sin embargo, esa ventaja geoestratégica no ha sido acompañada de una estrategia nacional de protección y aprovechamiento soberano de la infraestructura digital.

Asimismo, se ha demostrado que los modelos de gobernanza digital se hallan en tensión. Mientras Europa promueve un paradigma de soberanía normativa basado en derechos fundamentales y regulación ética (Jelinek, 2023), China plantea una soberanía infraestructural, articulada a su estrategia de Ruta de la Seda Digital (Kokas, 2022). Estados Unidos, por su parte, defiende un modelo orientado al liderazgo de sus corporaciones tecnológicas. En este tablero, Colombia aún no define con claridad su posición, y oscila entre acuerdos de conectividad con proveedores extranjeros y esfuerzos internos fragmentados.

Uno de los elementos críticos abordados es la dependencia tecnológica. Como lo advierte la Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 (Gobierno de Colombia, 2025), el país presenta una vulnerabilidad estructural por su alta dependencia de servicios en la nube provistos por empresas extranjeras, la ausencia de centros de datos soberanos y la débil articulación entre defensa,

industria y academia. La Ley 1273 de 2009 representó un avance pionero, al tipificar delitos informáticos y proteger los datos personales, pero se ha quedado rezagada frente a la complejidad actual del ecosistema digital. Por su parte, el Decreto 338 de 2022 creó el marco institucional para la seguridad digital, pero su implementación sigue siendo parcial y centrada en aspectos técnicos, sin integrar de forma robusta las dimensiones estratégicas de soberanía, industria nacional y ciberinteligencia.

De los hallazgos enunciados se derivan algunas recomendaciones estratégicas para la comunidad de defensa en Colombia. En primer lugar, es imperativo avanzar hacia una doctrina nacional de ciberdefensa que reconozca el ciberespacio como dominio operacional, así como lo son el aire, el mar, la tierra y el espacio ultraterrestre. Esta doctrina debe articular capacidades ofensivas, defensivas y resilientes, integrando el Comando Conjunto Cibernético y los organismos de inteligencia y contrainteligencia.

En segundo lugar, se recomienda fortalecer la protección de la infraestructura crítica de la información mediante una política de redundancia soberana: eso incluye la instalación de centros de datos nacionales con estándares de seguridad clase Tier IV, la diversificación de rutas de conectividad y la consolidación de acuerdos internacionales para la defensa de cables submarinos. En dicha tarea las Fuerzas Militares podrían asumir un rol de custodia estratégica, tal cual ocurre ya en países como Israel, Francia o Australia.

En tercer lugar, debe promoverse una política de desarrollo industrial digital que permita sustituir importaciones tecnológicas clave (como *routers*, *firewalls* y soluciones de encriptación), y fomentar ecosistemas nacionales de innovación, mediante alianzas con universidades, centros de investigación y *startups*. El talento humano en ciberseguridad, IA y arquitectura de redes debe considerarse un activo estratégico, sujeto a políticas de formación, retención y certificación continua.

En cuarto lugar, se hace necesaria una reforma legislativa que actualice el marco jurídico vigente incorporando principios de soberanía de datos, localización estratégica, propiedad del algoritmo y gobernanza ética de la IA. Esta nueva legislación debería armonizarse con el Sistema Interamericano de Protección de Derechos y las normas internacionales sobre ciberconflictos.

Finalmente, se sugiere incluir la dimensión del ciberespacio como una prioridad transversal en la planificación de la seguridad nacional, la inteligencia estratégica y la política exterior. Esto requiere, a su vez, una narrativa política que eleve el debate sobre soberanía digital al más alto nivel decisonal del Estado, y una

institucionalidad robusta que supere la actual fragmentación de competencias entre ministerios, agencias y fuerzas.

En conclusión, Colombia enfrenta un doble desafío: proteger su soberanía digital frente a amenazas externas, y consolidar capacidades internas que le permitan ejercer de manera efectiva esa soberanía. La geopolítica del ciberespacio no admite vacíos, y quienes no lo habiten de forma estratégica corren el riesgo de quedar subordinados. Como lo advierte Kadlecová (2024), el futuro de la soberanía en el siglo XXI no se juega únicamente en las fronteras territoriales, sino también en los centros de datos, las líneas de código y las rutas invisibles por donde circula el poder informacional del mundo.

Referencias

- Abbate, J. (1999). *Inventing the Internet*. MIT Press.
- Abler, R. 1977. The Telephone and the Evolution of the American Metropolitan System. En Pool, S. (Ed.), *The Social Impact of the Telephone* (pp. 318-341). MIT Press.
- Adams, P. (1992). Television as Gathering Place. *Annals of the Association of American Geographers*, 82(1), 117-135.
- Adams, P. (1997). Cyberspace and Virtual Places. *Geographical Review*, 87(2), 155-171.
- Agencia Digital AMD. (2025). *Estadísticas de marketing digital 2025 en Colombia*. <https://agenciadigitalamd.com/marketing-digital/estadisticas-marketing-digital-2025-colombia>
- Alexa (2020). *The Top 500 Sites on the Web*. <https://www.alexa.com/topsites>.
- Alto Sentido Agencia. (2025). *Desarrollo de aplicaciones móviles en Colombia*. <https://altosentidoagencia.com/blog-noticias/desarrollo-de-aplicaciones-moviles>
- 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.; Murillo, S.; Hernández, J. y Urbina, J. (2019a). El Poder Espacial y la Seguridad Multidimensional. En Álvarez, C. y Corredor, C. (Eds.), *El Espacio Exterior: Una Oportunidad Infinita para Colombia, Volumen 1, Mirando Hacia las Estrellas: Una Constante Necesidad Humana* (pp. 21-85). Sello Editorial ESDEG.
- Álvarez, C., Benavides, E. y Ramírez, Y. (2019b). Geopolítica del Espacio Exterior: Dominio Estratégico del Siglo XXI para la Seguridad y Defensa. En Álvarez, C. y Corredor, C. (Eds.), *El Espacio Exterior: Una Oportunidad Infinita para Colombia, Volumen 1, Mirando Hacia las Estrellas: Una Constante Necesidad Humana* (pp. 85-194). Sello Editorial ESDEG.
- Álvarez, C.; Corzo, M.; Jaimes, G. y Paredes, R. (2019c). La Nueva Economía del Siglo XXI: El Sector Privado en el Espacio. En Álvarez, C. y Corredor, C. (Eds.), *El Espacio Exterior: Una Oportunidad Infinita para Colombia, Volumen 1, Mirando Hacia las Estrellas: Una Constante Necesidad Humana* (pp. 331-368). Sello Editorial ESDEG.
- Álvarez, C.; Corredor, C.; Quiroga, R. y Molano, A. (2019d). 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.
- Aitken, S. y Zonn, L. (1994). *Place, Power, Situation and Spectacle: A Geography of Film*. Rowman and Littlefield.
- Barnes, T. (1996). *The Logics of Dislocation: Models, Metaphors and Meanings of Economic Space*. Guilford Press.
- BB Media. (2024). *Global OTT Market Trends Report*. <https://bb.vision>
- Berners-Lee, T. y Fischetti, M. (2000). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its Inventor*. Harper Business.

- Brooker-Gross, S. (1985). The Changing Concept of Place in the News. En Burgess, J. y Gold, J. (Eds.), *Geography, the Media and Popular Culture* (pp. 63-85). St. Martin's Press.
- Bryson, J.; Daniels, P. y Warf, B. (2004). *Service Worlds: People, Organisations, Technologies*. Routledge.
- Burgess, J. (1985). News from Nowhere: The Press, the Riots and the Myth of the Inner City. En Burgess, J. y Gold, J. (Eds.), *Geography, the Media and Popular Culture* (pp. 192-228). St. Martin's Press.
- Burgess, J. (1987). Landscapes in the Living Room: Television and Landscape Research. *Landscape Research*, 12(3), 1-7.
- Capri, A. (2024a). *The new geopolitics of undersea cables*. Hinrich Foundation.
- Capri, A. (2024b). *The geopolitics of modern data centers*. Hinrich Foundation.
- Carter, L.; Burnett, D.; Drew, S.; Marle, G.; Hagadorn, L.; Bartlett-McNeil, D. e Irvine, N. (2009). *Submarine Cables and the Oceans: Connecting the World*. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC. https://www.unepwcmc.org/system/data-set_file_fields/files/000/000/118/original/ICPC_UNEP_Cables.pdf?1398680911
- Castells, M. (1998). *The Information Age: Economy, Society and Culture. Volume 1: The Rise of the Network Society*. Blackwell.
- Castells, M. (2009). *Communication Power*. Oxford University Press.
- Cavazos, E. y Morin, G. (1995). *Cyberspace and the Law: Your Rights and Duties in the Online World*. MIT Press.
- Chander, A. y Sun, H. (Eds.). (2023). *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press.
- Chesney, R.; Shires, J. y Smeets, M. (Eds.). (2023). *Cyberspace and Instability*. Edinburgh University Press.
- Cisco. (2023). *Cisco Annual Internet Report (2018–2023)*. Cisco Systems.
- Clark, G. (2007). *A Farewell to Alms: A Brief Economic History of the World*. Princeton University Press.
- Cole, H. (2014). *Warfare in the Electromagnetic Spectrum and Cyberspace: United States Air Force Cyber/Electromagnetic Warfare Command Construct*. Air War College.
- Comparitech. (2024). *Screen time statistics: Average time spent looking at screens*. <https://www.comparitech.com/tv-streaming/screen-time-statistics/>
- Consegic Business Intelligence. (2024). *Cloud Business Email Market Size, Share & Analysis 2031*. <https://www.consegicbusinessintelligence.com/cloud-business-email-market>
- Crain, J. (2012). *Assesing Resilience in the Global Undersea Cable Infrastructure*. Naval Postgraduate School.
- Dao, B. (2024). *The Metaweb: The next level of the Internet*. CRC Press.
- DataReportal (2024). *Digital 2024: Global Overview Report*. <https://datareportal.com>

- DataReportal. (2025a). *Digital 2025: Global Overview Report*. We Are Social & Meltwater. <https://datareportal.com/reports/digital-2025-global-overview-report>
- DataReportal (2025b). *Digital 2025 April Global Statshot Report*. <https://datareportal.com/global-digital-overview>
- DCD (2025). *Telconet elige a Vertiv para construir una estación de aterrizaje de cables en Colombia*. <https://www.datacenterdynamics.com/es/noticias/telconet-elige-a-vertiv-para-construir-una-estacion-de-aterrizaje-de-cables-en-colombia/>
- Dean, J. (2024a). *Mobile game spending to hit \$111B in 2024, says Data.ai*. VentureBeat. <https://venturebeat.com/games/dataai-mobile-game-spending-111b-2024-predictions/>
- Dean, B. (2024b). *Ad blocker users: Statistics & trends*. <https://backlinko.com/ad-blockers-users>
- Deetz, S. (1984). Metaphor Analysis. En Gudykunst W. y Kim Y. (Eds.), *In Methods for Intercultural Communication Research* (pp. 215-228). Sage Publications.
- DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.
- Dodge, M. y Kitchin, R. (2000). *Mapping Cyberspace*. Routledge.
- Dodge, M. y Kitchin, R. (2001). *Atlas of Cyberspace*. Pearson Education Ltd.
- Domo. (2024). *Data Never Sleeps: AI Edition*. <https://www.domo.com/learn/infographic/data-never-sleeps-ai-edition>
- Eberhard, D.; Simons, G. y Fennig, C. (Eds.). (2023). *Ethnologue: Languages of the World (26th ed.)*. SIL International.
- ECDB (2024). *Ecommerce revenue per capita*. <https://ecdb.com/insights/ecommerce-revenue-per-capita/5066>
- Elbert, B. (2003). *The Satellite Communication Applications Handbook (2nd ed.)*. Artech House.
- Elbert, B. (2008). *Introduction to Satellite Communication (3rd ed.)*. Artech House.
- Elbert, B. (2014). *The Satellite Communication Ground Segment and Earth Station Handbook*. Artech House.
- El Colombiano. (2025). *¿Cuáles son las aplicaciones más descargadas por los colombianos?* <https://www.elcolombiano.com/tecnologia/cuales-son-las-aplicaciones-mas-descargadas-por-colombianos-GH25221007>
- Ericsson (2024). *Mobility Report 2024*. <https://www.ericsson.com/4adb7e/assets/local/reports-papers/mobility-report/documents/2024/ericsson-mobility-report-november-2024.pdf>
- Everett, A. (2009). *Digital Diaspora*. State University of New York Press.
- Exploding Topics (2025a). *How Many Websites Are On The Internet?* <https://explodingtopics.com/blog/how-many-websites-on-the-internet>
- Exploding Topics (2025b). *Data Generated Per day*. <https://explodingtopics.com/blog/data-generated-per-day>
- Exploding Topics (2025c). *Worldwide Daily Social Media Usage*. <https://explodingtopics.com/blog/social-media-usage>

- Farhadi, A.; Sanders, R. y Masys, A. (2022). *The Great Power Competition, Volume 3: Cyberspace, the Fifth Domain*. Springer.
- Finklea, K. (2017). *Dark Web*. Congressional Research Service.
- Frecuencia Online. (2025). *Latinoamérica en el Mobile Economy Report 2025*. <https://noticias.frecuenciaonline.com/2025/03/06/latinoamerica-en-el-mobile-economy-report-2025-todo-sobre-latam>
- Funnel. (2024). *Ad blocker usage report*. <https://funnel.io/blog/ad-blockers-marketing>
- Glasze, G; Cattaruzza, A.; Douzet, F.; Dammann, F.; Bertran, M.; Bômont, C.; Braun, M.; Dagnet, D.; Desforges, A.; Géry, A.; Grumbach, S.; Hummel, P.; Limonier, K.; Münßinger, M.; Nicolai, F.; Pétiinaud, L.; Winkler, J. y Zanin, C. (2023). Contested Spatialities of Digital Sovereignty. *Geopolitics*, 28(2), 919-958.
- Global Web Index. (2024). *Global Media Consumption Trends*. <https://www.gwi.com>
- Global Web Index (2024a). *Digital Trends Report 2024*. <https://www.gwi.com/reports/commerce>
- Global Web Index (2024b). *Commerce Report 2024*. <https://www.gwi.com/reports/commerce>
- Gobierno de Colombia. (2025). *Estrategia Nacional de Seguridad Digital de Colombia 2025-2027*. https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
- Go-Globe (2025). *Digital Landscape in Asia: Statistics and Trends*. <https://www.go-globe.com/digital-landscape-in-asia-statistics-and-trends>
- Gold, J. (1985). From Metropolis to the City: Film Visions of the Future City. En Burgess, J. y Gold, J. (eds.), *Geography, the Media and Popular Culture* (pp. 123-143). St. Martin's Press.
- Gould, P. (1984). *The Structure of Television: Television, the World of Structure*. Pion.
- Graham, S. y Marvin, S. (1996). *Telecommunications and the City: Electronic Spaces*. Routledge.
- Graham, M. (2013). Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities? *The Geographical Journal*, 179(2), 177-182.
- Griffiths, J. (2021). *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. Zed Books.
- Headrick, D. (1991). *The Invisible Weapon: Telecommunications and International Politics 1851-1945*. Oxford University Press.
- Headrick, D. y Griset, P. (2001). Submarine Telegraph Cables: Business and Politics, 1838-1939. *Business History Review*, 75, 543-78.
- Hepworth, M. (1990). *Geography of the Information Economy*. Guilford Press.
- Hugill, P. (1999). *Global Communications Since 1844: Geopolitics and Technology*. Johns Hopkins University Press.
- Icon-Era (2024). *Global Games Market Report 2024*. <https://icon-era.com/threads/new-zoo-released-their-free-global-games-market-report-2024>
- IMARC Group. (2025). *Latin America Mobile App Development Market: Industry Trends, Share, Size, Growth, Opportunity and Forecast 2025-2033*. <https://www.imarcgroup.com/report/es/latin-america-mobile-app-development-market>

- Internet Society (2020). Internet Society Global Internet Report 2019: Consolidation in the Internet Economy. <https://future.internetsociety.org/2019/>
- Jelinek, T. (2023). *The Digital Sovereignty Trap: Avoiding the Return of Silos and a Divided World*. Springer.
- Jiang, B. y Ormeling, F. (1997). Cybermap: the Map for Cyberspace. *The Cartographic Journal*, 34(2), 111-116.
- Jiang, B. y Ormeling, F. (2000). Mapping Cyberspace: Visualizing, Analysing and Exploring Virtual Worlds. *The Cartographic Journal*, 37(2), 117-122.
- Kadlečová, L. (2024). *Cyber Sovereignty: The Future of Governance in Cyberspace*. Stanford University Press.
- Kaukiainen, Y. (2001). Shrinking the world: Improvements in the speed of information transmission, c. 1820–1870. *European Review of Economic History*, 5(1), 1-28.
- Kemp, S. (2025). *Digital 2025: Global Overview Report*. <https://datareportal.com/reports/digital-2025-global-overview>
- Kokas, A. (2022). *Trafficking Data: How China is Winning the Battle for Digital Sovereignty*. Oxford University Press.
- Konradova, N. (2020). The Rise of Runet and the Main Stages of Its History. En Davydov, S. (Ed.), *Internet in Russia: A Study of the Runet and Its Impact on Social Life* (pp. 39-64). Springer.
- Kota, S.; Pahlavan, K. y Leppänen, P. (2004). *Broadband Satellite Communications for Internet Access*. Springer.
- Lakoff, G. y Johnson, M. (1980). *Metaphors We Live By*. University of Chicago Press.
- Lanham, R. (1993). *The Electronic Word: Democracy, Technology, and the Arts*. University of Chicago Press.
- La República (18 de septiembre de 2024). *Mercado de los data center alcanzará inversiones por US\$10.000 millones hacia 2029*. <https://www.larepublica.co/alta-gerencia/mercado-de-los-data-center-alcanzara-inversiones-por-us-10-000-millones-hacia-2029-3954590>
- Leiner, B.; Cerf, V.; Clark, D.; Kahn, R.; Kleinrock, L.; Lynch, D.; Postel, J.; Roberts, L. y Wolff, S. (1997). *A Brief History of the Internet*. Internet Society.
- Leiner, B.; Cerf, V.; Clark, D.; Kahn, R.; Kleinrock, L.; Lynch, D. y Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, 39(5), 22-31.
- Lemley, M. (2003). Place and Cyberspace. *California Law Review*, 91(2), 521-542.
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books.
- Liberty Networks (2023). *Cables submarinos: el potencial de Colombia para convertirse en el "hub" de conexión para América Latina*. <https://www.libertynetworks.com/es/noticias-y-eventos/cables-submarinos-el-potencial-de-colombia-para-convertirse-en-el-hub-de-conexion>

- Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.
- LinkedIn (2025). *March 2025 Non-Gaming App Advertising Review*.
- Live Science (2016). *How Big Is the Internet, Really?* <https://www.livescience.com/54094-how-big-is-the-internet.html>
- Loneragan, E. y Lonergan, S. (2023). *Escalation Dynamics in Cyberspace*. Oxford University Press.
- Malecki, E. y Wei, H. (2009). A Wired World: The Evolving Geography of Submarine Cables and the Shift to Asia. *Annals of the Association of American Geographers*, 99(2), 360-382.
- Market Research Future. (2024). *Cloud-Based Email Security Software Market Size & Trends 2035*. <https://www.marketresearchfuture.com/reports/cloud-based-email-security-software-market-41801>
- MarketWatch. (2024). *YouTube viewership surpasses TV on connected devices*. <https://www.marketwatch.com>
- Marvin, C. (1988). *When Old Technologies Were New: Thinking about Electric Communication in the Late Nineteenth Century*. Oxford University Press.
- McCusker, J. (2005). The demise of distance: The business press and the origins of the information revolution in the early modern Atlantic World. *American Historical Review*, 110(2), 295-321.
- Mensah, T. (2000). The Rights of Submarine Cable Owners and Coastal States Under the United Nations Convention on the Law of the Sea. *Maritime Studies*, 114, 10-17.
- Mitchell, W. (1995). *City of Bits: Space, Place, and the Infobahn*. MIT Press.
- Minoli, D. (2015). *Innovations in Satellite Communication and Satellite Technology*. Wiley.
- Monmonier, M. (1989). *Maps with the News: The Development of American Journalistic Cartography*. University of Chicago Press.
- Mueller, M. (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Polity Press.
- Netcraft (2026). *Web Server Survey – Global Internet Statistics Report*. <https://www.netcraft.com/blog/february-2026-web-server-survey>
- Newman, N.; Fletcher, R.; Kalogeropoulos, A. y Kleis, R. (2019). *Reuters Institute Digital News Report 2019*. Reuters Institute for the Study of Journalism.
- Newzoo (2024). *Global Games Market*. <https://newzoo-global-games-market-report-2024-light-version/>
- Ning, H. (2022). A brief history of cyberspace. CRC Press.
- Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*, 7(2), 61-73.
- O'Hara, K. y Hall, W. (2013). Web Science. En Dutton, W. (Ed.), *The Oxford Handbook of Internet Studies* (pp. 48-68). Oxford University Press.
- Payments CMI (2024). *Colombia e-Commerce Market Overview*. <https://paymentscmi.com/insights/colombia-e-commerce-market>
- PCMag (2024). *Take a Look Inside 60 Seconds on the Internet*. <https://www.pcmag.com/news/gone-in-60-seconds-heres-what-happens-on-the-internet-every-minute>

- Phillipson, R. (2009). *Linguistic Imperialism Continued*. Routledge.
- Pickles, J. (1995). *Ground Truth: The Social Implications of Geographic Information Systems*. Guilford Press.
- Portafolio (2023). *Así está el mapa de los cables submarinos que llegan al país*. <https://www.portafolio.co/innovacion/cables-submarinos-este-es-el-panorama-en-colombia-579498>
- Radicati Group. (2023). *Email Statistics Report, 2023–2027*. The Radicati Group, Inc.
- Rattray, G. (2001). *Strategic Warfare in Cyberspace*. MIT Press.
- Reuters Institute. (2024). *Digital News Report 2024*. <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024reutersinstitute.politics.ox.ac.uk>
- Rheingold, H. (1993). *The Virtual Community: Homesteading on the Electronic Frontier*. Addison-Wesley.
- Rushkoff, D. (1995). *Cyberia: Life in the Trenches of Hyperspace*. Harper Collins.
- Russell, A. (2017). *Strategic A2/AD in Cyberspace*. Cambridge University Press.
- Sack, R. (1992). *Place, Modernity, and the Consumer's World: A Relational Framework for Geographical Analysis*. Johns Hopkins University Press.
- Sandvine (2022). *Global Internet Phenomena Report*. <https://www.applogicnetworks.com/global-internet-phenomena-report-2022>
- Semrush (2026). *Most Visited Websites in the World: 2026 Rankings*. <https://www.semrush.com/trending-websites/global/all/>
- Sensor Tower. (2025). *2025 State of Mobile: Consumers' \$150 Billion Spent on Mobile Highlights Another Record-Setting Year*. <https://sensortower.com/blog/2025-state-of-mobile-consumers-usd150-billion-spent-on-mobile-highlights>
- Shields, R. (1996). *Cultures of Internet: Virtual Spaces, Real Histories, Living Bodies*. Sage Publications.
- SimilarWeb (2025). *Top Websites Ranking*. <https://www.similarweb.com/top-websites>
- Smith, S. (1985). News and the Dissemination of Fear. En Burgess, J. y Gold, J. (eds.), *Geography, the Media and Popular Culture* (pp. 229-253). St. Martin's Press.
- Smith, M. (1999). *Communities in Cyberspace*. Routledge.
- Srivastav, P.; Singhal, P.; Roohani, B. y Sharma, N. (2024). *Web 3.0: The next generation's Internet and understanding the concept of the Metaverse*. CRC Press.
- Stacciarini, J. y Gonçalves, R. (2025). *Data Centers, Critical Minerals, Energy, and Geopolitics: The Foundations of Artificial Intelligence*. SocArXiv.
- Statista (2024a). *Share of languages used in websites worldwide*. <https://www.statista.com/statistics/262946/most-common-languages-on-the-internet/>
- Statista (2024b). *Most used programming languages among developers worldwide, as of 2024*. <https://www.statista.com/statistics/793628/worldwide-developer-survey-most-used-languages/>

- Statista (2025a). *Global number of internet users 2005-2024*. <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/#:~:text=As%20of%202024%2C%20the%20estimated,percent%20of%20the%20global%20population>.
- Statista (2025b). Most popular social networks worldwide as of January 2025, ranked by number of monthly active users. <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users>
- Statista (2025c). Leading countries by number of data centers as of March 2025. <https://www.statista.com/statistics/1228433/data-centers-worldwide-by-country/>
- Strategic Market Research. (2024). Smart Home Statistics and Trends 2024. <https://www.strategicmarketresearch.com/blogs/smart-home-statistics>
- Sunstein, C. (2006). *Republic.com 2.0*. Princeton University Press.
- TechJury. (2024). *Mobile App Download Statistics 2024*. <https://techjury.net>
- Telegeography (2020). *Global Internet Geography Database Research 2019*. <https://www2.telegeography.com/our-research>
- Telegeography (2025). *How Many Submarine Cables Are There, Anyway?* <https://blog.telegeography.com/how-many-submarine-cables-are-there-anyway>
- Tesfaye, T. (2023). Web's Progression: Moving from Passive Content Consumption to Active Content Creation and Content Validation. *International Journal of Business and Management*, 18(6), 135-142.
- Thorat, D. (2019). Colonial Topographies of Internet Infrastructure: The Sedimented and Linked Networks of the Telegraph and Submarine Fiber Optic Internet. *South Asian Review*, 40(3), 252-267.
- Tigren (2024). *Global eCommerce Statistics and Trends in 2024*. <https://www.tigren.com/blog/global-ecommerce/>
- Tsagourias, N. y Buchan, R. (Eds.) (2021). *Research handbook on international law and cyberspace*. Edward Elgar Publishing Ltd
- Tuan, Y. (1978). Sign and Metaphor. *Annals of the Association of American Geographers*, 68(3), 363-372.
- Turkle, S. (1995). *Life on the Screen: Identity in the Age of the Internet*. Simon and Schuster
- Van Logchem, Youri (2014). Submarine Telecommunication Cables in Disputed Maritime Areas. *Ocean Development & International Law*, 45(1), 107-122.
- Vartanova, E. (2020). The Internet in the Structure of the Russian Media System. En Davydov, S. (Ed.), *Internet in Russia: A Study of the Runet and Its Impact on Social Life* (pp. 17-38). Springer.
- Warf, B. (1995). Telecommunications and the Changing Geographies of Knowledge Transmission in the Late 20th Century. *Urban Studies*, 32(2), 361-378.
- Winde, G. (2006). Webs of Enterprise 1850-1914: Applying a Broad Definition of FDI. *Annals of the Association of American Geographers*, 96, 788-806.

- Zittrain, J. (2008). *The Future of the Internet and How to Stop It*. Yale University Press.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Capítulo 3

La arquitectura ilícita del ciberespacio: cibercrimen y ecosistemas de la dark web*

DOI: <https://doi.org/10.25062/9786287818705.03>

Carlos Enrique Álvarez Calderón

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo analiza la arquitectura y el funcionamiento del cibercrimen organizado en la red oscura, las redes sociales y los entornos metaversos enmarcando estos dominios como componentes de un ecosistema criminal transnacional que convergen. A partir de la teoría criminológica, la literatura sobre cibercrimen y el modelo de los ecosistemas criminales, el estudio identifica los facilitadores estructurales, tecnológicos y culturales que sustentan las economías digitales ilícitas. Explora, además, cómo los roles especializados, las infraestructuras de anonimato y las plataformas descentralizadas posibilitan formas modulares y resilientes de organización criminal. El capítulo también introduce el concepto de desviación digital, como precursor cultural del comportamiento cibercriminal, y analiza los delitos emergentes en entornos inmersivos (metacrímenes). Finalmente, ofrece recomendaciones estratégicas para la seguridad nacional colombiana, incluyendo reformas institucionales, actualizaciones legales, marcos de ciberinteligencia y rendición de cuentas de las plataformas, para contrarrestar las amenazas en constante evolución dentro del ecosistema criminal digital. valorar de manera efectiva cómo contribuyen al IS a través de sus dimensiones de análisis.

Palabras clave: cibercrimen; ecosistema criminal; metacrímenes; red oscura

* 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

Citación APA: Álvarez Calderón, C. E. (2026). La arquitectura ilícita del ciberespacio: cibercrimen y ecosistemas de la dark web. 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. 177-236). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818705.03>

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

La *dark web* se ha vuelto un terreno crítico en el campo de la batalla digital, y ha permitido el auge de ecosistemas complejos de ciberdelincuencia organizada. A diferencia de los ciberdelincuentes convencionales, que operan de forma aislada o con poca coordinación, las redes cibercriminales organizadas aprovechan las ventajas tecnológicas de las herramientas de anonimización¹, las comunicaciones cifradas y los mercados descentralizados para escalar y mantener operaciones ilícitas en jurisdicciones globales (Lusthaus, 2018; Holt & Bossler, 2020). Estos actores constituyen un submundo digital caracterizado no solo por la delincuencia transaccional (por ejemplo, la venta de narcóticos, armas, *malware* y datos robados), sino también por una lógica cada vez más corporativa de prestación de servicios ilícitos, división del trabajo y optimización de beneficios (Graham & Smith, 2024; Alexandrou, 2021).

La arquitectura de la *dark web*, en particular de las plataformas que operan a través del rutador Onion (Tor) e I2P, ha permitido la ocultación de identidades, geolocalizaciones y huellas digitales, lo que la convierte en un terreno fértil para mercados criminales como Silk Road, AlphaBay, Dream Market e Hydra (Ozkaya & Islam, 2019; Nearchou, 2023). Estas plataformas no solo facilitan las transacciones lícitas e ilícitas, sino que también replican los mecanismos de confianza del legítimo y popular comercio electrónico, como las calificaciones de los proveedores, los servicios de depósito en garantía y la resolución de disputas, lo que refuerza la retención de usuarios y la continuidad operativa (Watters, 2024; Holt et al., 2022). Por ende, la convergencia del anonimato, alcance transnacional y alta rentabilidad

¹ La "anonimización" es un proceso que transforma datos personales de manera que ya no se pueda identificar a las personas a las que se refieren. Esto se logra eliminando o modificando los datos identificables para obtener información anónima. La anonimización es crucial para proteger la privacidad de los individuos y cumplir con la normativa de protección de datos.

permiten que las empresas criminales prosperen pese a la intensificación de las intervenciones policiales y el cierre de mercados (Jenkinson, 2022; Viano, 2017).

Cabe señalar que la ciberdelincuencia organizada en la *dark web* no es tan solo un fenómeno económico: es también una configuración sociotécnica que difumina las fronteras entre la desviación, delincuencia y las subculturas digitales. Si bien este capítulo se centra en el análisis de las organizaciones cibercriminales y las infraestructuras de la *dark web*, es importante reconocer el papel de la desviación digital como entorno propicio. Las comunidades digitales desviadas (incluidos los foros de *hackers*, redes de piratería y culturas del *troleo*), suelen servir de incubadoras de conductas delictivas al normalizar prácticas ilícitas y proporcionar formación técnica entre iguales (Graham & Smith, 2024; Noble et al., 2017). Estos elementos subculturales, aunque no son delictivos *per se*, reducen las barreras a la ciberdelincuencia y refuerzan identidades arraigadas en ideologías antisistémicas o libertarias (Holt et al., 2022; Kremling & Sharp Parker, 2017).

Lo anterior plantea la pregunta central de investigación de este capítulo del libro: ¿Cómo operan y evolucionan las redes cibercriminales organizadas dentro de los ecosistemas de la web oscura, y cuáles son las dinámicas estructurales, tecnológicas y criminológicas que sustentan estas economías ilícitas? Es imperativo abordar ese interrogante desde los estudios en seguridad y defensa, con el propósito de desarrollar contramedidas eficaces que vayan más allá de la mitigación técnica y abarquen dimensiones legales, culturales y estratégicas.

La relevancia teórica y política de este campo de estudio se ve subrayada por los desafíos que el cibercrimen organizado plantea a los sistemas legales, a las agencias de inteligencia y a las arquitecturas de ciberseguridad. Los modelos tradicionales de control de la delincuencia organizada son cada vez más inadecuados en el ciberespacio, debido a su naturaleza fluida, sin fronteras y cifrada (Clough, 2015; Donalds et al., 2022). Para responder a eso, Estados y organizaciones internacionales han desarrollado instrumentos jurídicos transnacionales (por ejemplo, el Convenio de Budapest), así como respuestas tácticas que incluyen la informática forense digital, la OSINT² y las estrategias de ciberinfiltración (Holt & Bossler, 2020; Bandler & Merzon, 2020; Akhgar et al., 2021). Sin embargo, la ecología de la red oscura, en rápida evolución, continúa superando a los marcos regulatorios y de aplicación de la ley.

² Open Source INTelligence (Inteligencia de Fuentes Abiertas), es una disciplina que se enfoca en recolectar, analizar e interpretar información de fuentes públicas y accesibles legalmente.

En consecuencia, el presente capítulo se propone analizar los elementos estructurales, tecnológicos y criminógenos de la ciberdelincuencia organizada en la red oscura situando dichos fenómenos en contextos sociológicos y criminológicos más amplios. El documento comienza describiendo la dinámica operativa de los grupos cibercriminales, para explorar posteriormente la arquitectura y la gobernanza de los mercados ilícitos y, finalmente, analizar los facilitadores criminógenos y los desafíos para la aplicación de la ley. La desviación digital se examinará como una capa contextual secundaria que configura el entorno cultural y psicológico de este ecosistema.

La ciberdelincuencia organizada en la era digital

El cibercrimen se ha convertido en un fenómeno global donde actores ilícitos utilizan tecnologías en red para cometer delitos a escala transnacional. En ese contexto, el cibercrimen se solapa con el crimen organizado tradicional, pero opera a través de plataformas digitales, como los mercados, productos y servicios ilícitos de la web oscura, el *ransomware* y el fraude en línea. El alcance de la ciberdelincuencia organizada ahora incluye mercados delictivos (por ejemplo, de drogas o datos), ofertas de delincuencia como servicio (CaaS), e incluso, operaciones cibernéticas habilitadas por Estados mafiosos y cleptocráticos. Como observa Viano (2017), estos avances se deben a la convergencia de oportunidades de bajo riesgo y alta rentabilidad en el ciberespacio para el crimen organizado, ya que Internet facilita el tráfico global y el movimiento de dinero. Asimismo, actores criminales patrocinados por algunos Estados han perseguido objetivos estratégicos y financieros mediante la perpetración de ciberdelitos.

Definición de cibercrimen y de ciberdelincuencia organizada

En principio, el cibercrimen podría conceptualizarse como los delitos perpetrados a través de redes informáticas o sistemas digitales atacando la infraestructura digital o utilizándola como medio para facilitar las actividades ilícitas. Empero, las definiciones de "cibercrimen" y "ciberdelincuencia organizada" han cambiado en las últimas dos décadas, a medida que la evolución de las tecnologías digitales ha transformado la naturaleza del comportamiento delictivo. Si bien no existe una definición universalmente consensuada, académicos, organismos internacionales e

instituciones jurídicas han proporcionado múltiples marcos que intentan delinear estos fenómenos en términos tanto conceptuales como operativos.

Según Payne (2020), las definiciones con relación al “cibercrimen” son importantes por al menos siete razones que se superponen: 1) la forma como las personas definen el cibercrimen determinará las estimaciones sobre su alcance; 2) las definiciones de cibercrimen influirán en las consecuencias (o respuestas individuales) a comportamientos específicos; 3) las definiciones de cibercrimen tienen implicaciones en la forma como los criminólogos intentan explicar los delitos cibernéticos; 4) las definiciones guiarán las estrategias de intervención utilizadas para responder a ciertos tipos de comportamiento; 5) las definiciones guiarán las estrategias de prevención utilizadas para prevenir ciertos tipos de comportamientos cibercriminales; 6) las definiciones determinarán también las metodologías de investigación utilizadas para estudiar el comportamiento cibercriminal, y 7) en consecuencia con lo anterior, las definiciones determinarán cómo los académicos enseñan sobre el comportamiento.

En términos académicos las definiciones de cibercrimen tienen ramificaciones en la aplicación de las teorías criminológicas. Siguiendo una perspectiva durkheimiana, por ejemplo, algunos podrían definir el cibercrimen como un comportamiento normal. Desde esa perspectiva, el cibercrimen podría considerarse un fenómeno que cumple al menos cuatro funciones: 1) podría advertir sobre problemas específicos que deben abordarse (el aumento de los fraudes en internet dio lugar a nuevas formas de hacer más seguras las compras en línea); 2) podría, de hecho, impulsar el cambio social (el *hacktivismo* podría ser un ejemplo); 3) podría promover la integración comunitaria, y 4) las definiciones de cibercrimen ofrecen ejemplos de cuáles comportamientos se consideran aceptables, y cuáles, inaceptables. Las definiciones de cibercrimen también impulsan (o al menos se relacionan con eso) las estrategias de investigación. Desde la perspectiva de Payne (2020), quienes definen el cibercrimen con una orientación más social, por ejemplo, podrían ser más propensos a utilizar estrategias de investigación en ciencias sociales para estudiar este fenómeno; mientras, quienes definen el cibercrimen desde una perspectiva más tecnológica probablemente utilizarían otras estrategias.

Ahora bien, una simple revisión de la investigación sobre cibercrimen en el ámbito de la justicia penal confirma que el término no ha existido durante mucho tiempo. Antes de su introducción se utilizaba la frase “delito informático”, y es a Parker (1976) a quien se le atribuye el desarrollo de una de las primeras taxonomías sobre delitos informáticos. La taxonomía de Parker (1976) define los delitos informáticos como aquellos en los que un computador es: 1) el objeto del delito,

2) el entorno donde se comete el delito, 3) el instrumento para cometerlo, y 4) el símbolo del delito (por ejemplo, cuando las personas afirman engañosamente que utilizan recursos informáticos para fundamentar decisiones que conducen a una conducta delictiva). Más tarde, Hollinger y Lanza-Kaduce (1988) desarrollaron uno de los primeros trabajos de criminología sobre el tema centrándose en cómo se llegó a penalizar el delito informático. Luego, la Convención de Budapest sobre Ciberdelincuencia, firmada en 2001, caracterizó estos delitos de una manera que se asemejaba vagamente a la taxonomía de Parker (1976).

Tras la aparición del término "delito informático" los investigadores interesados en estas conductas empezaron a introducir otros términos, tales como: el "delito digital", consistente en "cualquier actividad delictiva que implique el uso de computadores y redes o cualquier otro dispositivo digital" (Sabell et al., 2012, p. 558); el "delito electrónico", caracterizado como "un acto ilegal que se lleva a cabo utilizando una computadora o medios electrónicos" (Kardya & Mitrou, 2007, p. 2); el "delito en internet", definido por el Centro de Quejas de Delitos en Internet como cualquier actividad ilegal que involucre uno o más componentes de internet, como sitios web, salas de chat o correo electrónico; el "delito en la red", el cual se ha descrito como "no solo [...] una forma de interceptación de datos, sino que también implica la intrusión en redes para obtener acceso no autorizado a los datos, o incluso modificarlos, destruirlos, hacer un uso no autorizado de los recursos de la red, etc." (Wang, 2012, p. 1); el "tecnocrimen", que incluye una amplia gama de delitos cometidos en el sistema tecnológico (Friedrichs, 2009), y el "delito virtual", referido a los delitos cometidos en entornos de realidad virtual o juegos virtuales (Lastowka & Hunter, 2004).

Pero ninguno de estos términos ha tenido la misma difusión que el "cibercrimen", aunque sigue siendo un término relativamente nuevo. En este orden de ideas, y según el Convenio del Consejo de Europa sobre Ciberdelincuencia, considerado ampliamente el primer tratado internacional que aborda los delitos cometidos a través de internet y otras redes informáticas, el "cibercrimen" se define como los "delitos contra datos y sistemas informáticos, delitos informáticos, delitos de contenido y delitos contra los derechos de autor" (Krone, 2005, p.1). Wall (2007) ofrece una perspectiva más analítica afirmando que "los ciberdelitos son actividades delictivas o dañinas que son informativas, globales y están interconectadas, y deben distinguirse de los delitos que simplemente utilizan computadoras" (p. 4).

Una definición tecnológica propuesta por Clough (2012) considera el cibercrimen como "el uso de tecnología digital para la comisión o facilitación de delitos" (p. 364). Dicha perspectiva enfatiza la naturaleza instrumental del cibercrimen, al

distinguir entre la intención del delincuente y el medio de ejecución. Por su parte, Interpol añade una dimensión práctica al definir el ciberdelito como un “área delictiva en rápido crecimiento” que aprovecha “la velocidad, la comodidad y el anonimato de internet” para una amplia gama de delitos que “no conocen fronteras, ni físicas ni virtuales” (Ozkaya & Islam, 2019, p. 6). Por eso, el cibercrimen se entiende mejor como un fenómeno multidimensional que incorpora perspectivas jurídicas, tecnológicas, criminológicas y sociológicas. Abarca conductas que van desde la filtración de datos y fraude financiero hasta el ciberacoso y actividades relacionadas con el terrorismo, con una escala e impacto amplificadas por la interconectividad global. El autor de este capítulo lo define como las actividades ilegales realizadas mediante sistemas informáticos, dispositivos digitales o redes, ya sea como medio o como objetivo del delito.

Mientras que el cibercrimen se refiere a la naturaleza del delito y a sus medios, la “ciberdelincuencia organizada” describe la estructura y la coordinación de dichas actividades. La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Convención de Palermo) ofrece una definición amplia describiendo a un “grupo delictivo organizado” como un “grupo estructurado de tres o más personas, que existe durante un tiempo y actúa concertadamente con el fin de cometer delitos graves (...) para obtener un beneficio económico o material” (UNODC, 2004, art. 2a). Al aplicarlo al contexto digital, Lavorgna (2018) identifica tres características del crimen organizado convencional que se traducen, a su juicio, en la ciberdelincuencia organizada: 1) un conjunto de actividades delictivas, tanto sofisticadas como continuas, a menudo mantenidas mediante corrupción u ofuscación técnica; 2) una organización estructurada con una jerarquía y división del trabajo definidas, y 3) una infiltración sistémica en las esferas económicas o políticas.

La Oficina de las Naciones Unidas contra la Droga y el Delito (en inglés, UNODC, por las iniciales de United Nations Office on Drugs and Crime) establece que por “ciberdelincuencia organizada” se entiende “un delito cibernético [...] que sea: a) cometido por un grupo delictivo organizado, según se define en el artículo 2 [...] de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, [...]; o b) que implique un delito tipificado con arreglo al artículo 5 de la Convención, que abarca la penalización de la participación en un grupo delictivo organizado” (UNODC, 2022, p. 8). A su vez, Graham y Smith (2024) señalan que los grupos de ciberdelincuencia organizada son “organizaciones jerárquicas y estructuradas que realizan actividades delictivas sofisticadas en las que sus miembros desarrollan su propia cultura interna y una reputación de criminales” (p. 135). Estos grupos pueden surgir completamente en el ciberespacio (por ejemplo, colectivos

de *hackers*), o tener su origen en organizaciones tradicionales del crimen organizado que expanden sus operaciones en línea (por ejemplo, grupos mafiosos que realizan ataques de *ransomware* o trafican con contrabando digital). Neto (2017) clasifica, además, a las redes cibercriminales organizadas en tres diferentes tipos: 1) redes híbridas (grupos criminales tradicionales que usan la tecnología para mejorar sus operaciones); 2) redes cibercriminales puras (colectivos descentralizados nacidos en línea que rara vez se reúnen en el mundo físico), y 3) redes con motivaciones ideológicas (como grupos ciberterroristas y hacktivistas, que aprovechan sus habilidades técnicas para alcanzar fines políticos).

Al respecto, lo que distinguiría la ciberdelincuencia organizada de los delitos cibernéticos individuales o poco coordinados sería su escala, continuidad y capacidad para causar daños. Estos grupos suelen participar en empresas delictivas complejas, como el *ransomware* en forma de servicio (RaaS), distribución de *malware*, fraude con tarjetas de crédito, redes de explotación sexual infantil y ciberespionaje. La aparición de los mercados digitales y el modelo de delincuencia como servicio (CaaS) permite a estos grupos externalizar componentes clave (creación de *malware*, blanqueo de capitales o ataques DDoS), lo que mejora tanto la eficiencia como el anonimato. Otra característica de la ciberdelincuencia organizada es su capacidad para trascender fronteras geográficas manteniendo la cohesión funcional, ya que, a diferencia de las bandas callejeras o las mafias, las organizaciones cibercriminales pueden estar formadas por miembros de distintos continentes, comunicarse mediante plataformas cifradas y, a menudo, operar en diferentes zonas horarias (Graham & Smith, 2024).

En resumen, ni el fenómeno del cibercrimen ni la ciberdelincuencia organizada son construcciones jurídicas estáticas, sino fenómenos sociotécnicos dinámicos moldeados por la evolución de las tecnologías y las fuerzas económicas globales, así como las de los entornos criminógenos en línea. Definir el cibercrimen implica reconocer su complejidad y multiplicidad, desde los ataques puramente digitales hasta el fraude cibernético. Definir la ciberdelincuencia organizada requiere prestar atención a la estructura, intención, coordinación y persistencia de los delitos, con crecientes implicaciones para las fuerzas del orden transnacionales y para las políticas de ciberseguridad.

Evolución histórica del cibercrimen

La historia del cibercrimen está profundamente entrelazada con la evolución de las tecnologías informáticas y de internet. Lo que empezó como experimentos de *hacking* inofensivos se ha convertido en una empresa criminal global que involucra

actores estatales, grupos organizados e infraestructuras sofisticadas. Por lo tanto, enseguida se desarrollan los principales hitos en la evolución del cibercrimen, desde sus orígenes exploratorios hasta su forma industrializada actual.

La fase exploratoria: décadas de 1960-1980

Como ya se mencionó, las raíces conceptuales del cibercrimen se hallan en la manipulación temprana de sistemas informáticos durante la década de 1960. Según Clough (2015), los delitos informáticos inicialmente abarcaban actos como el sabotaje y la manipulación informática, que ocurrían sobre todo dentro de instituciones con acceso a sistemas *mainframe*. Pero durante la década de 1970 dos desarrollos clave sentaron las bases del cibercrimen moderno: en primer lugar, surgió la práctica del *phone phreaking*, que consistía en la explotación de las vulnerabilidades relacionadas con los sistemas de telecomunicaciones para realizar llamadas de larga distancia gratuitas. Cabe destacar que un personaje llamado John Draper, apodado Capitán Crunch, se convirtió en una figura simbólica de esta subcultura. En segundo lugar, la creación del gusano "Creeper", en 1971, representó el primer *malware* autorreplicante conocido, aunque no era en especial dañoso, pues tan solo dejaba un mensaje inofensivo: "Soy el Creeper: atrápenme si pueden".

Sin embargo, para la década de 1980 los delitos informáticos comenzaron a atraer la atención legal y pública. En 1981 Ian Murphy (alias Capitán Zap) se convirtió en la primera persona condenada por un delito informático en Estados Unidos, tras alterar los horarios de facturación en el sistema de AT&T. Y en 1986 el *hacker* alemán Markus Hess se infiltró en las redes militares estadounidenses y vendió el acceso a la KGB, lo que marcó un nuevo nivel de espionaje por medios digitales. Pero el punto de inflexión llegaría en 1988, con el gusano 'Morris', creado por un estudiante de Cornell llamado Robert Morris. Este código autorreplicante causó involuntarias, pero importantes, interrupciones, al bloquear 6.000 sistemas y causar daños estimados en 98 millones de dólares (Alexandrou, 2021).

La era de los virus y la respuesta legal: década de 1990

La década de 1990 marcó la popularización de internet y el consiguiente aumento del cibercrimen. Esta década presenció el desarrollo de sistemas operativos y correos electrónicos intuitivos, que se convirtieron en vectores de transmisión de virus. Ejemplos infames incluyen el virus 'Michelangelo' (1991), el virus 'Melissa' (1999) y el gusano 'ILOVEYOU' (2000), que se propagaron rápidamente a través de archivos adjuntos en correos electrónicos. Al mismo tiempo los gobiernos empezaron a formular marcos legales para contrarrestar las amenazas emergentes.

Estados Unidos aprobó en 1986 la Ley de Fraude y Abuso Informático (en inglés, CFAA, por las iniciales de Computer Fraud and Abuse Act), que se convirtió en una piedra angular para la persecución del cibercrimen. Y a nivel internacional iniciativas como el Convenio sobre Ciberdelincuencia del Consejo de Europa (2001) comenzaron a sentar las bases jurídicas transnacionales. De acuerdo con Nearchou (2023), este período también fue testigo del auge del *phishing*, una forma de ingeniería social en la que actores maliciosos se hacen pasar por entidades legítimas para extraer información confidencial. Suelen incluir imágenes de aspecto oficial, direcciones de correo electrónico y sitios web falsos para engañar al usuario. Los *hackers* envían este tipo de correos electrónicos para robar contraseñas y números de cuentas bancarias o infectar sistemas con virus.

La industrialización de la ciberdelincuencia: década de 2000

A principios de la década de 2000 se inició una nueva era: la profesionalización y comercialización del cibercrimen. A medida que la economía digital se popularizaba, también lo hicieron los incentivos para la explotación criminal. Grupos cibercriminales organizados empezaron a ofrecer lo que se ha venido a denominar *Crime-as-a-Service* (CaaS), mediante el cual herramientas maliciosas como *keyloggers*, *ransomware* y *bots* de *spam* podían comprarse o alquilarse en mercados de la *darknet*.

Desde la perspectiva de Choi et al. (2020), este período coincide con la "Tercera Revolución Industrial" de la ciberdelincuencia, caracterizado por fraudes financieros, robo de identidad y campañas organizadas de *phishing* (tabla 1). El famoso atraco al Citibank, en 1994, cuando Vladimir Levin robó 10 millones de dólares a través de sistemas de banca por internet, es emblemático de esta época. Surgieron foros dedicados a las operaciones de los cibercriminales, que alcanzaron su apogeo a principios de la primera década del siglo XXI. Lusthaus (2018) documenta cómo dichos foros en línea facilitaron el desarrollo de una infraestructura cibercriminal, con sistemas de reputación criminal, servicios de depósito en garantía y roles especializados: desde desarrolladores de *malware* hasta mulas de dinero.

Tabla 1. Las cuatro revoluciones industriales, avances tecnológicos y nuevos tipos de crimen

Revolución industrial	Periodo	Avances tecnológicos	Nuevos tipos de crimen
Primera Revolución Industrial	1760-1840	Fábricas; ferrocarriles; minería de carbón; textiles	Robo de trenes; contrabando; productos falsificados
Segunda Revolución Industrial	1870-1914	Electricidad; automóviles; bombillos; teléfono; radio; industria petrolera	Robo de automóviles; fraude telefónico; robo de servicios públicos; interferencias de radio; robo a bancos
Tercera Revolución Industrial	1969-2010	Microprocesadores; comunicación por internet; transistores informáticos; energía nuclear; biotecnología; automatización robótica	Hacking; intrusión cibernética; robo cibernético; manipulación de datos; malware; spyware
Cuarta Revolución Industrial	2010- actualidad	Nanotecnología; Internet de las cosas (IoT); inteligencia artificial (IA); criptomonedas	Ransomware para bitcoin; fraude mediante deep fake

Fuente: elaboración propia, con base en Choi et al. (2020).

Cada revolución industrial se caracteriza por las tecnologías más significativas de su época. En efecto, la Primera Revolución Industrial fue una era dominada por el vapor y la fabricación mecánica, y estuvo acompañada del auge de la producción en serie característico de la Segunda Revolución Industrial, mientras que la Tercera Revolución Industrial y la Cuarta Revolución Industrial se caracterizaron por la tecnología de la información y las estructuras ciber físicas, que pueden considerarse épocas distintivas, debido a su velocidad, alcance e impacto en la economía global. Desde finales de las décadas de 1960 y 1970 la Tercera Revolución Industrial se ha caracterizado por el desarrollo de las tecnologías de la información y la comunicación (TIC), así como por una creciente industrialización y globalización, y los delitos cibernéticos originados en esta revolución industrial están evolucionando actualmente, debido a las nuevas condiciones de la Cuarta Revolución Industrial. Es decir, si bien persisten los delitos cibernéticos tradicionales, como las estafas en línea, el hackeo y los ataques DDoS, en las últimas décadas se han desarrollado nuevas variantes de estos delitos.

Ciberdelincuencia globalizada y vinculada al Estado: década de 2010-presente

La Cuarta Revolución Industrial comenzó en la década de 2010 (Schwab, 2016). Esta revolución ha provocado transformaciones significativas tanto en la vida cotidiana de las personas como en la naturaleza del cibercrimen. Schwab (2016) caracteriza esta era como una marcada por el surgimiento de nuevas tecnologías

que integran los ámbitos biológico, digital y físico, e impactan diversas industrias, economías y campos de estudio. Afirma también que la Cuarta Revolución Industrial genera un entorno global donde los sistemas de fabricación virtuales y físicos colaboran de forma flexible y cohesionada (Schwab, 2016). Esta nueva revolución abarca no solo máquinas y sistemas inteligentes e interconectados, sino también la integración de estas innovaciones y su colaboración en los ámbitos físico, digital y biológico, lo que distingue a la Cuarta Revolución Industrial de sus predecesoras. Durante esta revolución tecnologías emergentes y la innovación generalizada se difunden con mayor rapidez y amplitud que en revoluciones anteriores, y persisten en regiones específicas del mundo (Schwab 2016).

Estas transformaciones tecnológicas y sociales también han introducido nuevas vulnerabilidades y riesgos, sobre todo en lo que respecta a la ciberdelincuencia y la ciberseguridad, por lo que el cibercrimen ha entrado en su fase más compleja hasta el momento. Esta "Cuarta Revolución Industrial" del cibercrimen se caracteriza por ataques patrocinados por Estados, ciberguerra, esquemas de *ransomware* a sueldo y filtraciones masivas de datos. Incidentes notables incluyen el hackeo de Sony PlayStation, en 2011, cuando más de 77 millones de cuentas se vieron comprometidas; la violación de Yahoo, entre 2013 y 2014, que afectó a más de 3 mil millones de usuarios a nivel mundial, y el *ransomware* "WannaCry", de 2017, lanzado por Corea del Norte y que afectó a hospitales y sistemas gubernamentales en alrededor de 150 países. Estas operaciones indican no solo motivaciones financieras, sino también agendas geopolíticas, por lo que algunos académicos, incluyendo a Lusthaus (2018), argumentan que Estados como China y Rusia utilizan cada vez más tácticas de ciberdelincuencia como parte de sus estrategias de gobierno.

En el contexto de la Cuarta Revolución Industrial varios factores críticos pueden contribuir a los desafíos de la ciberdelincuencia y la ciberseguridad: Inicialmente, internet y los ecosistemas tecnológicos, conocidos como "sistemas ciber-físicos" (Schwab 2016), y que abarcan el Internet de las Cosas (IdC; en inglés, IoT) y la computación en la nube crean nuevas oportunidades para que los ciberdelincuentes accedan simultáneamente a los datos y archivos de numerosas personas mediante la infiltración ilegal en los sistemas de computación en la nube (Chaka & Marimuthu 2018). Además, la proliferación de hogares "inteligentes" y los dispositivos del IdC, como Alexa y Google Home, junto con artículos tradicionales como iluminación y mandos a distancia para electrodomésticos, entre otros, permiten a los *hackers* manipular y alterar remotamente estos dispositivos. Los sistemas de reconocimiento facial también pueden ser vulnerados por ciberdelincuentes expertos para obtener acceso no autorizado a teléfonos inteligentes, tabletas y portátiles.

En segundo lugar, en relación con estos nuevos ecosistemas, la integración de dispositivos inteligentes en una red global ha facilitado métodos bancarios innovadores, como Venmo y Zelle. Los sistemas de pago emergentes, como las criptomonedas (Bitcoin y Ethereum), la tecnología *blockchain* y los códigos QR, pueden percibirse como una oportunidad innovadora para los delincuentes, junto con desafíos significativos para las víctimas y las fuerzas del orden (Brenner, 2012). Recientes incidentes de *ransomware* de gran repercusión involucran a ciberdelincuentes que exigen pagos en Bitcoin para evitar la destrucción de datos y archivos personales o comerciales (Luo & Liao, 2009). En este sentido, el anonimato y la confidencialidad de las criptomonedas para ambas partes permiten que este novedoso método de transferencia global de dinero fomente el avance de la ciberdelincuencia transnacional mediante el pago de rescates para la protección de datos valiosos (Mansfield-Devine, 2016).

En tercer lugar, la aceleración de la IA y la automatización se ha visto marcada por la aparición de vehículos sin conductor, aeronaves no tripuladas y sistemas automatizados de venta minorista, como cajeros automáticos y cajas de autoservicio. Estos avances conllevan la aparición de sistemas inteligentes autónomos, que en ocasiones se manifiestan en robots humanoides. Como la IA puede considerarse una convergencia de tecnologías que difumina las distinciones entre los ámbitos físico, digital y biológico, las ramificaciones de la revolución de la IA para el comercio, la industria y la vida siguen siendo parcialmente especulativas. Los problemas más evidentes en este contexto se refieren a la naturaleza cambiante del trabajo y el mercado laboral, que están experimentando una rápida transformación y seguirán haciéndolo (Schwab, 2016).

En resumen, la evolución del cibercrimen refleja transformaciones tecnológicas y sociopolíticas más amplias en comparación con sus formas iniciales, caracterizadas por prácticas aisladas, motivaciones experimentales y capacidades limitadas. Desde los inicios del hackeo motivado por la curiosidad y los gusanos bromistas hasta el *ransomware* actual y las economías de la *darknet* a escala industrial, el cibercrimen se ha convertido en un rasgo característico de la era digital. Asimismo, el cibercrimen también se ha adaptado a nuevas plataformas y tecnologías; la manipulación de redes sociales, *cryptojacking* (minería no autorizada de criptomonedas) y el fraude impulsado por IA ejemplifican esta evolución. Por consiguiente, las tecnologías como la IA, el *big data*, el IdC, la computación en la nube, la realidad aumentada, el Bitcoin y el *blockchain*, entre otras, si bien facilitan la investigación, detección y predicción de actividades delictivas, también introducen nuevas vulnerabilidades que van a ser explotadas por el cibercrimen.

Tipologías del cibercrimen y la ciberdelincuencia organizada

Comprender las diversas manifestaciones del cibercrimen y la ciberdelincuencia organizada requiere tipologías sólidas que distingan entre comportamientos individuales, métodos tecnológicos y estructuras criminales. Estas tipologías no solo facilitan la claridad analítica, sino que también proporcionan una base estratégica para la aplicación de la ley, el desarrollo legislativo y la inteligencia sobre cibermenazas. En este orden de ideas, la tipología de David Wall (2007) sigue siendo un modelo fundamental en la investigación sobre ciberdelincuencia, en el cual clasifica el cibercrimen en cuatro tipos generales: ciberintrusión, ciberengaño y robo, ciberpornografía y obscenidad, y ciberviolencia. Estas categorías se basan tanto en clasificaciones legales como en distinciones conductuales en la ciberdelincuencia.

La "ciberintrusión" consiste en el acceso no autorizado a los sistemas digitales, comúnmente conocido como *hacking* o *cracking*. Esta categoría abarca tanto intrusiones en sistemas como brechas de red y la implementación de *malware* destinado a comprometer la confidencialidad, la integridad o la disponibilidad. El ciberengaño y el robo incluyen fraudes en línea como el *phishing*, el robo de identidad, las estafas en línea y las violaciones de la propiedad intelectual. Esta suele ser la categoría con más impacto económico, al relacionarse estrechamente con grupos de ciberdelincuencia organizada. La "ciberpornografía" y la obscenidad se refieren a la producción y difusión de contenido sexual ilegal en línea, incluyendo materiales de abuso sexual infantil (MASI) y pornografía no consentida. La "ciber-violencia" comprende actividades que infligen daño psicológico o incitan a la violencia en el mundo real, como el ciberacoso, el ciber-acecho y el discurso de odio en línea.

Estas categorías no son mutuamente excluyentes. Por ejemplo, el uso de *malware* para extorsionar a las víctimas (*ransomware*) puede clasificarse tanto en ciberintrusión como en ciberengaño. Además, la tipología de Wall (2007) ha demostrado ser adaptable, lo que permite su integración con ciberdelitos emergentes como el *cryptojacking*, la sextorsión y las campañas de desinformación (Lusthaus, 2018). Además, los marcos alternativos se centran en las características del objetivo y del actor. Ozkaya e Islam (2019) clasifican el ciberdelito según el objetivo (individuos, propiedades o instituciones gubernamentales), y ahí destaca el ciberterrorismo como una amenaza específica contra las estructuras estatales.

El modelo heurístico de McGuire (2012) ofrece otra perspectiva, al organizar los ciberdelitos en tres niveles: 1) delitos que ocurren exclusivamente en línea, 2)

delitos que combinan componentes en línea y fuera de línea, y 3) delitos fuera de línea facilitados por herramientas digitales. Este enfoque enfatiza la permeabilidad entre comportamientos delictivos digitales y físicos. Y desde una perspectiva psicológica, los actores cibercriminales también se clasifican en perfiles como “*black hat*” (intenciones maliciosas), “*white hat*” (*hacking* ético) y “*gray hat*” (motivaciones ambiguas), lo que refleja la interacción entre las habilidades técnicas y la intención. La UNODC (2022) diferencia dos grandes categorías: los delitos basados en la cibernética y los delitos facilitados por la cibernética. Los primeros son los que no pueden cometerse sin las TIC, como el acceso ilegal a sistemas, el sabotaje digital, la interferencia de datos o la producción y distribución de *malware*. Los segundos incluyen delitos tradicionales que se potencian a través de la tecnología, como el fraude, la falsificación, la trata de personas o el blanqueo de capitales en línea.

Mientras que las tipologías del cibercrimen se centran en los actos, las tipologías de la ciberdelincuencia organizada examinan las estructuras delictivas. Cabe señalar que no todos los delitos cibernéticos son necesariamente organizados, ni todos los grupos delictivos organizados operan en el ciberespacio. No obstante, con la expansión de las economías ilícitas y las tecnologías de anonimización, el delito cibernético organizado se ha convertido en un fenómeno prominente y distintivo. Lavorgna (2020) sugiere que las redes de ciberdelincuencia organizada a menudo cumplen con las definiciones legales de delincuencia organizada (criterios de estructura, continuidad y propósito delictivo de la Convención de Palermo), sin cumplir obligatoriamente con criterios académicos como el control territorial, el uso de la violencia o la monopolización de los mercados.

Graham y Smith (2024) amplían este análisis identificando categorías operativas dentro del delito cibernético organizado: 1) piratería digital, donde los grupos se dedican a la reproducción y venta masiva de contenido protegido por derechos de autor; 2) falsificación de documentos, a menudo utilizada para facilitar el fraude de identidad o actividades ilícitas transfronterizas; 3) lavado de dinero, mediante técnicas como la estratificación de transacciones financieras; 4) ciberterrorismo, que implica violencia ideológica o política mediada por herramientas digitales, y 5) ataques de amplio alcance, incluyendo campañas de implementación de *malware* a escala global.

Por su parte, Leukfeldt et al. (2017) ofrecen una tipología empírica, basada en las redes de *phishing* en Dinamarca. Identifican tres tipos de ciberdelincuencia organizada: 1) las del tipo I, caracterizadas por una baja tecnología y alta interacción, que se basan en ingeniería social y comunicación directa con las víctimas; 2) las

del tipo II, caracterizadas por una baja tecnología y baja interacción (algunos ejemplos incluyen herramientas de *phishing* automatizadas que reducen la interacción personal), y finalmente, 3) las del tipo III, caracterizadas por una alta tecnología y baja interacción, que utilizan *malware* avanzado, troyanos o *rootkits* para extraer datos de forma invisible y automatizar el blanqueo de capitales. Este modelo ilustra un espectro de sofisticación e intensidad de interacción, lo que ayuda a las fuerzas del orden a evaluar el nivel de amenaza y las contramedidas técnicas necesarias.

Otra conceptualización influyente distingue entre el crimen organizado tradicional que se expande al ciberespacio y los grupos organizados nativos en línea. Los primeros pueden usar tecnologías digitales para potenciar el narcotráfico o el tráfico de personas, mientras que los segundos son nativos digitales y operan por completo dentro de los ecosistemas cibercriminales, como los mercados de la red oscura, organizaciones de *ransomware* o proveedores de alojamiento web. El grupo "Carbanak/Cobalt" ejemplifica la complejidad del cibercrimen organizado: operando desde 2013, el grupo utilizó correos electrónicos de *phishing* selectivo y *malware* personalizado para penetrar en instituciones financieras en más de catorce países. Sus operaciones incluían roles como codificadores, mulas de dinero y coordinadores de retiro de efectivo, e involucraban el lavado de fondos a través de criptomonedas y mercados negros. La respuesta transnacional a su arresto, liderada por Europol y el FBI, demuestra tanto la sofisticación de la empresa criminal como el esfuerzo coordinado necesario para combatirla.

De acuerdo con la UNODC (2022), la estructura interna de los grupos delictivos en el ciberespacio varía entre dos extremos: organizaciones jerárquicas con división del trabajo y liderazgos claros, así como las redes distribuidas o "enjambres" sin estructura fija. Un ejemplo del primer tipo lo constituye DrinkorDie, un grupo dedicado a la piratería digital que tenía una estructura organizativa compleja con funciones definidas como codificadores, empaquetadores y proveedores de distribución. Este tipo de grupos se asemeja a organizaciones criminales tradicionales, con roles funcionales y cadenas de mando bien definidas. En el otro extremo se encuentran redes como "Dream Market", donde la descentralización y anonimato dificultan la atribución de responsabilidades. Según la UNODC (2022), las redes difusas suelen organizarse en torno a servicios específicos sin establecer estructuras jerárquicas estables, y operando a menudo como mercados entre pares que conectan compradores y vendedores. Dichas estructuras maximizan la resiliencia ante intervenciones policiales y fragmentan la trazabilidad del delito. Entre estos dos modelos se ubican formas híbridas, donde coexisten niveles de jerarquía

funcional con dinámicas de red. La combinación de liderazgo técnico y libertad operacional permite a estos grupos adaptarse rápidamente a cambios tecnológicos o amenazas legales.

Desde una perspectiva operativa, la UNODC (2022) clasifica a los grupos de ciberdelincuencia organizada en tres categorías principales: grupos predominantemente en línea, grupos híbridos y grupos predominantemente *offline* que utilizan tecnologías digitales para facilitar sus actividades ilícitas. Los primeros son grupos que realizan todas sus operaciones en entornos digitales y se organizan como enjambres o como nodos. Los enjambres se caracterizan por ser agrupaciones temporales y autoorganizadas que se disuelven tras lograr un objetivo específico. Por otro lado, los nodos son más estables y funcionan como células especializadas que colaboran de forma flexible en distintas etapas del ciclo criminal. Ejemplos de esas estructuras incluyen foros de intercambio de *malware*, grupos de *Ransomware-As-A-Service* y comunidades de *hacking* orientadas al lucro (tabla 2).

Tabla 2. *Tipologías de ciberdelincuencia organizada según la UNODC*

Categoría	Descripción	Ejemplos	Características Clave
Jerárquicos (tradicionales)	Estructuras organizadas con liderazgo definido, división de tareas y operaciones coordinadas	<i>DrinkorDie</i>	Organización vertical; roles funcionales claros; control centralizado
Redes descentralizadas (enjambres/nodos)	Grupos sin jerarquía fija que se autoorganizan para tareas específicas. Utilizan plataformas digitales y comunicación cifrada	<i>Dream Market</i> ; foros de <i>hacking</i>	Flexibilidad; anonimato; cooperación horizontal
Híbridos agrupados	Combinan operaciones físicas y digitales. Hay interacción presencial para coordinar delitos que ocurren en línea.	Redes de fraude con tarjetas	Dualidad operativa (online/offline), coordinación presencial
Híbridos extendidos	Grupos descentralizados con mínima o nula interacción física. Operan en la <i>dark web</i> y en mercados virtuales	<i>Silk Road</i> ; redes de <i>Ransomware-As-A-Service</i>	Descentralización; anonimato extremo; presencia transnacional
Tradicionales digitalizados	Grupos criminales <i>offline</i> que integran tecnologías para mejorar sus actividades (publicidad, pagos, captación)	Mafias en apuestas ilegales; prostitución virtual	Uso instrumental de TIC; estructura criminal preexistente

Fuente: elaboración propia, con base en UNODC (2022).

Por su lado, los grupos híbridos combinan operaciones en línea y fuera de línea. Según la UNODC (2022), se dividen en híbridos agrupados, que interactúan físicamente para coordinar operaciones digitales como fraudes con tarjetas, e híbridos extendidos, que mantienen una estructura descentralizada con vínculos personales mínimos, tal cual ocurre con plataformas de la *dark web* tipo Silk Road. Este tipo de organizaciones representa un punto medio entre las mafias tradicionales y los colectivos cibernéticos descentralizados. Y finalmente se encuentran los grupos predominantemente *offline* con apoyo digital. Estas organizaciones son criminales tradicionales que utilizan tecnologías de la información para aumentar su capacidad de acción. Por ejemplo, redes dedicadas a apuestas ilegales o prostitución utilizan herramientas digitales para el reclutamiento, la publicidad y el lavado de dinero. Aunque su núcleo operativo sigue siendo físico, el uso de entornos digitales amplía su alcance y reduce sus riesgos.

Una característica común en estas organizaciones es la fragmentación funcional. Como señala la UNODC (2022), la prestación de servicios criminales se distribuye entre múltiples actores especializados: programadores, diseñadores de *malware*, operadores de infraestructuras de anonimato, expertos en cifrado, mulas de dinero y coordinadores de pagos. Este tipo de esquema modular permite a los grupos subcontratar capacidades y mantener el anonimato entre sus miembros, lo que dificulta las tareas de inteligencia y judicialización. A su vez, la existencia de mercados criminales digitales, donde se venden y alquilan herramientas ilícitas, ha dado lugar a lo que algunos expertos llaman Crimen como Servicio (CaaS), el cual permite incluso a individuos sin conocimientos técnicos participar en campañas delictivas sofisticadas mediante el acceso a kits prefabricados y soporte técnico (tabla 3).

Casos como el de "Shadowcrew" y "Card Planet" ilustran cómo operan estos grupos: estructuras de cientos o miles de miembros organizados en función de habilidades específicas, regulados por foros, sistemas de reputación y filtros de admisión. En el caso de "Dreamboard", los miembros debían aportar imágenes ilegales de forma continua para mantener su membresía, lo que refleja una cultura interna orientada al control, la exclusividad y la complicidad activa. Además, el uso de criptomonedas, redes privadas virtuales (en inglés, VPN, por las iniciales de *Virtual Private Network*), cifrado de extremo a extremo, plataformas de mensajería efímera y mercados de la *dark web* forman parte del arsenal tecnológico que estas redes utilizan para ocultar sus operaciones y dificultar la investigación criminal.

Tabla 3. Especialización criminal y Crimen como Servicio (CaaS)

Categoría	Descripción	Ejemplos	Características clave
División funcional interna	Especialización por tareas: programadores, diseñadores de <i>malware</i> , mulas, operadores de pagos, administradores de servidores, etc.	Todos los anteriores (tabla 2)	Modularidad; subcontratación; anonimato entre miembros
Crimen como Servicio (CaaS)	Modelo económico donde se comercializan servicios ilícitos listos para usar: kits de <i>malware</i> , <i>hosting</i> anónimo, herramientas de cifrado, etc.	Foros criminales; <i>marketplaces</i> de servicios ilícitos	Profesionalización; acceso para no expertos; economía criminal sofisticada

Fuente: elaboración propia, con base en UNODC (2022).

En conclusión, las tipologías del cibercrimen y la ciberdelincuencia organizada son herramientas esenciales en los contextos académicos y operativos. La tipología de Wall (2007) ofrece una base estructurada para analizar el cibercrimen según su función y daño, mientras que las tipologías de la ciberdelincuencia organizada ayudan a delinear la infraestructura, motivaciones y el carácter transnacional de los grupos cibercriminales. La ciberdelincuencia organizada no es una réplica digital del crimen tradicional, sino una evolución estructural que explota las oportunidades técnicas y sociales del ciberespacio. Desde enjambres efímeros hasta mafias híbridas digitalizadas, estas organizaciones redefinen los parámetros de la criminalidad moderna. Y a medida que evolucionen las tecnologías también deben evolucionar estas tipologías, especialmente para considerar amenazas emergentes como el *ransomware* como servicio, el fraude basado en IA y los actores de amenazas híbridos que difuminan la línea entre las operaciones cibernéticas estatales y no estatales.

Funciones en la ciberdelincuencia organizada

La ciberdelincuencia organizada es un fenómeno delictivo complejo, transnacional y dinámico, caracterizado por estructuras flexibles, alta especialización y uso estratégico de tecnologías de la información y la comunicación (TIC). A diferencia de otras formas de crimen tradicional, los grupos ciberdelincuenciales organizados operan, en la mayoría de los casos, como empresas con funciones diferenciadas, distribución de tareas, prestación de servicios y control de calidad interno. Como señala Lusthaus (2018), la ciberdelincuencia organizada opera como una “industria de la anonimidad”, donde “los actores criminales participan en un mercado interconectado donde se compran, venden y alquilan servicios ilícitos con reglas internas y reputaciones compartidas” (p. 21). Esta lógica industrial también se manifiesta en la separación de funciones dentro de las organizaciones ilegales, lo que permite la maximización de eficiencia y la reducción de riesgos operacionales.

La UNODC (2022) refuerza la idea de la ciberdelincuencia organizada como un sistema productivo de tipo empresarial, al documentar cómo estos grupos de ciberdelincuencia organizada se componen de múltiples perfiles funcionales, incluyendo codificadores, piratas informáticos, técnicos de infraestructura, encargados de pagos, especialistas en cifrado, ingenieros sociales y mulas de dinero, entre otros. Estos roles son comparables a los departamentos funcionales de una empresa, donde cada unidad cumple con una función específica dentro del ciclo delictivo. Ese diseño funcional permite no solo la sostenibilidad del grupo a largo plazo, sino la escalabilidad de sus operaciones a nivel global.

Los grupos de ciberdelincuencia organizada incluyen diversos roles operativos altamente especializados. Por ejemplo, los codificadores desarrollan *malware*, *exploits* y herramientas personalizadas para cometer delitos cibernéticos. Por su lado, los piratas informáticos (*hackers*) aprovechan vulnerabilidades en sistemas, redes o aplicaciones, ya sea para obtener acceso no autorizado, insertar código malicioso, sustraer información o mantener persistencia dentro de un sistema comprometido. Los responsables del soporte técnico son los encargados de mantener la infraestructura digital del grupo. Esto incluye servidores, VPN, plataformas cifradas de comunicación, canales seguros de intercambio de archivos y actualizaciones de herramientas técnicas. Los anfitriones proveen el entorno técnico necesario para alojar actividades ilícitas en servidores, a menudo bajo servicios de "*hosting* blindado" diseñados para eludir la detección policial y sostener operaciones prolongadas en la red oscura (UNODC, 2022).

Por otra parte, se encuentran los especialistas, o personas con habilidades técnicas excepcionales. Algunos se dedican a desarrollar cifradores, herramientas diseñadas para evitar la detección de programas antivirus. Otros pueden ser expertos en ingeniería social, por lo que se enfocan en manipular víctimas o empleados internos para obtener acceso a sistemas sensibles. Los cajeros y mulas de dinero son los encargados de convertir activos ilícitos en dinero limpio. Pueden operar tanto en el escenario físico, retirando dinero de cuentas comprometidas, como digitalmente, a través de criptomonedas y plataformas de transferencia. Finalmente se encuentran los administradores y moderadores, que operan en las plataformas criminales como los foros de *carding* o los mercados de la *dark web*. Dichos miembros establecen normas internas, filtran nuevos usuarios, organizan jerarquías y aplican sanciones, para así garantizar el orden interno y la confianza entre pares (UNODC, 2022).

La expansión de modelos de Crimen como Servicio (*Crime-as-a-Service* [CaaS]) ha propiciado una industria delictiva en la que muchas de estas funciones

pueden incluso ser subcontratadas. De acuerdo con Lavorgna (2020), los mercados digitales permiten que desarrolladores ofrezcan *ransomware*, kits de *phishing*, servidores anónimos y acceso a *botnets* como productos comercializables. Estos servicios facilitan que incluso personas sin mayores conocimientos técnicos puedan participar en campañas delictivas complejas mediante la adquisición de herramientas “listas para usar”. El “apoyo técnico” también puede ser parte de estos servicios, como ocurre en foros donde se venden tutoriales sobre cómo utilizar *malware*, enmascarar IP o crear documentos falsificados. En este contexto muchos grupos del cibercrimen no actúan como una sola organización vertical, sino como consorcios informales, donde los diversos proveedores interactúan temporalmente para ejecutar una operación específica, una estructura típica de los “enjambres” cibernéticos.

Finalmente, y más allá de funciones operativas, estos grupos cibercriminales organizados implementan medidas de control interno y anonimato altamente sofisticadas. Plataformas de la *dark web* como “Dreamboard” y “Card Planet” utilizaban sistemas de membresía controlada con verificación por parte de usuarios activos, cuotas de ingreso y votación interna para aceptar nuevos miembros. En “Card Planet”, por ejemplo, se requería hasta hace poco el pago de 5.000 dólares como garantía para acceder al foro. Estas medidas no solo limitan el acceso de infiltrados policiales, sino que también refuerzan la confianza entre actores anónimos, lo cual es decisivo en entornos sin interacción cara a cara. De hecho, no pocas plataformas adoptan políticas estrictas como la prohibición de acceso a miembros arrestados o inactivos, para así minimizar el riesgo de comprometer las operaciones globales.

En resumen, la ciberdelincuencia organizada no puede entenderse tan solo como un delito cometido con computadores, sino como un entramado funcional, técnico y social donde convergen múltiples actores especializados. En efecto, desde los desarrolladores de *malware* hasta las mulas financieras, cada función cumple un papel clave en una cadena criminal altamente eficiente. Comprender esta lógica funcional es indispensable para diseñar políticas públicas, estrategias de ciberseguridad e intervenciones policiales que respondan al carácter industrial, distribuido y anónimo del crimen organizado en el ciberespacio.

El estado del mercado y los ingresos del cibercrimen

En 2025 la economía del cibercrimen ha alcanzado niveles sin precedentes de complejidad, madurez y rentabilidad. Es decir, ya no se compone tan solo de actores de amenazas aislados o explotadores *ad hoc*, sino que el mercado actual

del cibercrimen opera como un ecosistema adaptativo altamente estructurado, multinivel y orientado a la rentabilidad, comparable en función y escala a las economías digitales legítimas. Los actores de amenazas se involucran en la especialización, la división del trabajo, el desarrollo de marca, el reclutamiento de afiliados y la innovación competitiva, impulsados por una red global de mercados en la *dark web*, proveedores de *malware* como servicio y canales de monetización de datos (Check Point, 2025).

Como detalla el *Informe de Ciberseguridad 2025*, las campañas de *ransomware* y robo de información se han convertido en los motores económicos de un submundo digital que ahora respalda una amplia gama de servicios, incluyendo el desarrollo de *malware*, la intermediación de acceso inicial, la logística de extorsión, el lavado de dinero, e incluso, la atención al cliente para transacciones ilícitas (Check Point, 2025). Cabe destacar que los ataques de *ransomware* causaron pérdidas por 872 millones de dólares solo a UnitedHealth y Change Healthcare durante el primer trimestre de 2024, lo que ilustra la capacidad de una sola campaña para infligir daños a nivel estratégico. Asimismo, la mercantilización del *software* malicioso, en particular a través de modelos de *ransomware* como servicio (RaaS) y *malware* como servicio (MaaS), ha reducido la barrera técnica de entrada. Los afiliados licencian kits de herramientas como “RedLine Stealer” por entre 150 y 200 dólares al mes y pueden esperar monetizar los registros a aproximadamente 10 dólares por víctima (Check Point, 2025, p. 21). Este modelo refleja una economía de franquicia, donde los desarrolladores se centran en la infraestructura y el soporte, mientras que las filiales ejecutan las operaciones de forma independiente. El resultado es un mercado criminal ágil, descentralizado y difícil de dismantelar.

Los *infostealers* han eclipsado a las *botnets* y troyanos tradicionales como el método más eficaz para el acceso inicial y la vulneración de la identidad. Su popularidad se debe a su bajo coste, facilidad de uso y alto rendimiento. Herramientas como Lumma, RedLine y StealC permiten a los ciberdelincuentes recopilar credenciales, *cookies* de navegador y *tokens* de sesión, que luego se revenden o se utilizan directamente para infiltrarse en entornos corporativos (Check Point, 2025). La economía de los *infostealers* es robusta, con más de 10 millones de registros a la venta en plataformas como Russian Market, algunos de los cuales se dirigen a cuentas de alto valor, como Microsoft 365, VPN y sistemas financieros. De hecho, un análisis de 2024 reveló que el 90 % de las organizaciones vulneradas por *ransomware* ya habían sufrido filtraciones de credenciales en registros de robo de información, lo que subraya el papel decisivo que estas herramientas desempeñan

en la cadena de suministro delictiva (Check Point, 2025, p. 22). La demanda de registros ha incentivado la innovación en los mecanismos de distribución (*phishing*, *malvertising* y repositorios de *software* falsos), así como la automatización de clasificación y transmisión de registros a plataformas como Telegram.

Por consiguiente, el *ransomware* sigue dominando el panorama de ingresos de la ciberdelincuencia. Si bien las operaciones de las fuerzas del orden en 2024 afectaron a actores clave como "LockBit" y "ALPHV", el número total de ataques de *ransomware* ha aumentado, con la incorporación de nuevos actores como "RansomHub", "Play" y "Akira" (Check Point, 2025). Las operaciones de *ransomware* priorizan cada vez más la extorsión por exfiltración de datos (DXF) sobre el cifrado, adoptando un modelo de negocio que minimiza el riesgo técnico y maximiza la presión psicológica. Es necesario señalar que este modelo DXF es particularmente rentable: los datos robados a las organizaciones se subastan en sitios de filtración de datos (DLS) de la *dark web*, o se extorsiona a las víctimas para que paguen, y así evitar la publicación de archivos confidenciales. Grupos como "Bashe" (Eraleign) operan ahora exclusivamente como plataformas de venta de datos evitando por completo el cifrado y diversificando aún más las fuentes de ingresos disponibles para los ciberdelincuentes (Check Point, 2025).

Este cambio también facilita el reciclaje y la atribución falsa de datos, donde los atacantes presentan filtraciones antiguas como nuevos ataques para obtener múltiples rescates. Como resultado, la atribución, la respuesta a incidentes y la adjudicación de seguros cibernéticos se vuelven más complejas y propensas a errores. Además, el ecosistema actual del cibercrimen se asemeja a un sector industrial multicapa. En la cima se encuentran las APT de élite y los desarrolladores de *malware*, mientras que por debajo se encuentran los proveedores de infraestructura que ofrecen alojamiento anónimo, paneles C2 y soporte para afiliados. Los actores de nivel medio incluyen operadores de robo de información, vendedores de kits de *phishing* y agentes de acceso inicial (IAB) que monetizan las vulnerabilidades del sistema y revenden credenciales. Finalmente, los actores de nivel inferior incluyen compradores de registros, ladrones de identidad y estafadores que compran acceso o datos para aplicaciones delictivas especializadas (Check Point, 2025, p. 23). Esa estructura refleja la especialización funcional: en efecto, de modo similar a como las industrias legítimas hacen uso de las plataformas en la nube, procesadores de pagos y proveedores de análisis, los ciberdelincuentes también externalizan el alojamiento, el cifrado y la ofuscación de *exploits* a proveedores de servicios. El resultado es una economía delictiva cada vez más resiliente y con una escalabilidad horizontal.

El mercado del cibercrimen tiene asimismo un alcance profundamente global, pero está controlado de forma asimétrica. Si bien América del Norte y Europa soportan la mayor parte de las pérdidas financieras y el número de víctimas, una gran proporción de la infraestructura, los actores y los registros robados provienen de regiones en desarrollo con mecanismos de control deficientes. Según Check Point (2025), más del 55 % de los registros de robo de información vendidos en mercados clandestinos provienen de países como la India, Brasil, Egipto e Indonesia, donde la adopción de internet es alta y la protección de los *endpoints* es baja. Esta asimetría fomenta un entorno de bajo riesgo y alta recompensa para los perpetradores. El uso de criptomonedas, alojamiento web seguro y redes de anonimización dificulta aún más la aplicación de la ley. Incluso cuando se desmantelan los principales grupos de RaaS, la resiliencia del ecosistema en su conjunto (mediante la reutilización de código, la migración de afiliados y la infraestructura descentralizada) garantiza la continuidad de las operaciones (Check Point, 2025).

Finalmente, si bien las valoraciones precisas del mercado son difíciles, debido a la naturaleza clandestina del cibercrimen, las estimaciones del sector sugieren que los ingresos por ciberdelincuencia a nivel mundial superan los 10 billones de dólares anuales, de los que el *ransomware* y el robo de credenciales representan una parte significativa. Por ejemplo, tan solo la filtración de datos de Change Healthcare en 2024 generó un impacto financiero de casi 900 millones de dólares y pagos de rescates por un total de más de 20 millones de dólares (Check Point, 2025). Estas cifras sugieren que la escala económica de la ciberdelincuencia rivaliza con la de las principales industrias globales, como la energética, la farmacéutica y la del entretenimiento. A medida que los actores de amenazas se profesionalizan, la ciberdelincuencia se conceptualiza cada vez más no solo como un problema de seguridad, sino también como una amenaza estratégica, económica y geopolítica. El Grupo "Lazarus" de Corea del Norte ejemplifica este tipo de convergencia, al realizar robos de criptomonedas para financiar objetivos estatales, mientras que grupos chinos e iraníes combinan la ciberdelincuencia con el espionaje, la guerra híbrida y el sabotaje industrial.

La *dark web* como ecosistema criminal

Internet es una extensa red global de computadores y dispositivos interconectados que permite a los usuarios acceder a información de la World Wide Web. La World Wide Web es un sistema de información que interconecta documentos mediante

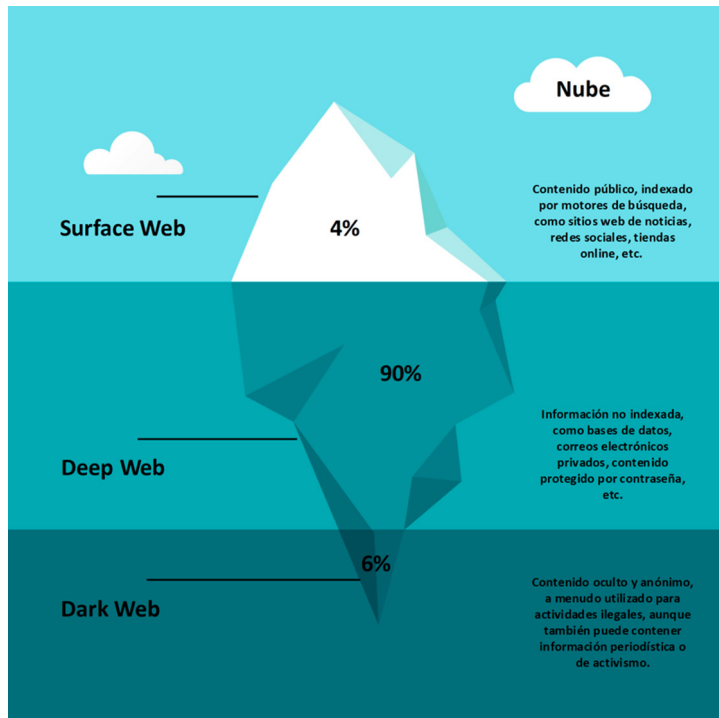
enlaces de hipertexto, lo que permite a los usuarios navegar sin problemas de un documento a otro (Gehl, 2018). Motores de búsqueda destacados, como Google, Yahoo y Bing, utilizan estos enlaces para catalogar diversos documentos, lo que facilita la exploración y la búsqueda de información (East, 2017).

Internet comprende múltiples niveles de accesibilidad. La web superficial, o *surface web*, comprende todos los sitios web de fácil acceso al público, ya que están indexados por los principales motores de búsqueda. Sin embargo, ciertos sitios web permanecen inaccesibles al público, ya que no se encuentran indexados por los principales motores de búsqueda. Dicho estrato de Internet se denomina *deep web* (Symanovich, 2019). Para acceder a estos sitios de la web profunda se debe introducir directamente la URL en un navegador web como Chrome, Internet Explorer o Safari. Otros sitios de la web profunda son inaccesibles al público general debido a la protección con contraseña o cifrado. Este nivel de la web profunda alberga contenido inaccesible para los motores de búsqueda (Symanovich, 2019).

La banca en línea de la actualidad ejemplifica tanto la web abierta como la web profunda. Una persona puede utilizar cualquier motor de búsqueda popular para localizar la página de inicio de banca en línea de su banco preferido. El sistema de banca en línea está protegido por una contraseña, que requiere que los usuarios inicien sesión para acceder a sus cuentas personales. Si bien las páginas de inicio pueden ser indexadas por múltiples motores de búsqueda y son accesibles en la web de superficie, el contenido específico de las cuentas bancarias permanece oculto al público (por ejemplo, la web profunda). Por consiguiente, se estima que la web profunda constituye la mayor parte de internet (Gehl, 2018).

Un computador se reconoce por su dirección de Protocolo de Internet (IP), lo que facilita la comunicación dentro de la red. Esta dirección IP funciona de forma análoga a una dirección residencial en su capacidad para identificar y localizar un dispositivo o computador que accede a internet. Las direcciones IP asocian el historial de navegación a la identidad del usuario (Gehl, 2018). Para mantener el anonimato en línea, los usuarios pueden instalar *software* criptográfico especializado que oculta su ubicación, lo que les permite acceder a internet y a la World Wide Web sin revelar la dirección física del computador y preservando la confidencialidad de su historial de navegación (figura 1). El *software* criptográfico más común es Tor, una aplicación de código abierto que permite a los usuarios acceder a internet a través de una red de servidores virtuales sin establecer una conexión directa (East, 2017).

Figura 1. Los niveles de la World Wide Web



Fuente: elaboración propia.

La *dark web* se refiere a un segmento de internet que no está indexado por los motores de búsqueda convencionales y al que solo se puede acceder mediante *software* de anonimización, tales como Tor, I2P o Freenet. Dichos sistemas permiten a los usuarios ocultar su identidad, cifrar las comunicaciones y alojar servicios ocultos sin revelar su ubicación física ni sus identificadores de red. Si bien gran parte del discurso público describe a la *dark web* como un submundo distópico repleto de delincuencia, también sirve a usuarios legítimos, como disidentes políticos, denunciantes y periodistas que operan bajo regímenes autoritarios (Gehl, 2018; Nearchou, 2023). Sin embargo, su arquitectura es inherentemente propicia para las transacciones ilícitas, la coordinación de ciberdelinquentes y operaciones clandestinas que son muy difíciles de interceptar para las fuerzas del orden (Ozkaya e Islam, 2019; Akhgar et al., 2021).

El ecosistema de la *dark web* se basa en infraestructuras técnicas que priorizan el cifrado, la descentralización y la ofuscación de identidad. Tor, la más conocida de estas tecnologías, enruta los datos de los usuarios a través de múltiples

capas de “cebolla”, lo que hace casi imposible rastrear el origen o el destino del tráfico si no se cuenta con herramientas avanzadas de desanonimización (Liggett et al., 2020). Tor permite no solo la navegación anónima, sino también el alojamiento de servicios ocultos, a los que solo pueden acceder los usuarios que utilizan el mismo *software* de anonimización.

Los usuarios de la *dark web* también utilizan las criptomonedas (Bitcoin, Monero y Ethereum), para el anonimato transaccional. Por ende, las criptomonedas son clave para mantener el seudonimato en los ecosistemas criminales, respecto a lo que actúan como el principal medio de intercambio de bienes y servicios que abarcan desde narcóticos y armas de fuego hasta *malware* y tráfico de personas (Nearchou, 2023; Akhgar et al., 2021). Como resultado, estos activos digitales cumplen propósitos tanto funcionales como simbólicos dentro de la economía subterránea: permiten pagos irrastreables y refuerzan el espíritu libertario de las subculturas digitales anti-vigilancia (Gehl, 2018).

Como ya se ha mencionado, una de las características que definen a la *dark web* es la presencia de redes cibercriminales organizadas que imitan las jerarquías corporativas y adoptan los modelos operativos similares a los de las empresas legítimas, por lo que estos grupos no son simplemente colectivos coordinados de forma flexible, sino, por el contrario, entidades estructuradas con roles y especializaciones definidos. Nearchou (2023) destaca que los actores organizados en la red oscura mantienen la continuidad operativa adaptándose a las presiones legales y la volatilidad del mercado: por ejemplo, cuando las fuerzas del orden cierran un mercado (como “Silk Road” o “AlphaBay”), sus usuarios y proveedores suelen migrar a otro, a menudo con mayor seguridad operativa. Por lo tanto, esta evolución cíclica de los mercados es emblemática de un ecosistema criminal resiliente y adaptable.

Mercados y servicios ilícitos en la dark web

La *dark web* alberga una variedad de mercados ilícitos donde se comercializan abiertamente diversas formas de contrabando y servicios delictivos, por lo que, en cierto sentido, estos mercados suelen parecerse a las plataformas de comercio electrónico convencionales, con categorías de productos, reseñas de clientes, calificaciones de proveedores y servicios de depósito en garantía (Liggett et al., 2021).

El tráfico de drogas es, quizá, el componente más investigado y económicamente significativo del comercio delictivo en la *dark web*. Si bien plataformas tempranas como “Silk Road” fueron pioneras en este ámbito, los mercados más nuevos han adoptado protocolos logísticos y de cifrado más sofisticados. Las

investigaciones estiman que los mercados oscuros de drogas generan cientos de millones de dólares al año, con vendedores que ofrecen una amplia gama de narcóticos, desde opioides y estimulantes hasta medicamentos recetados falsificados (Liggett et al., 2020; Nearchou, 2023). Eso sí, lo que distingue a dichas plataformas es su impersonalidad y eficiencia, ya que los vendedores y compradores nunca se encuentran físicamente, las comunicaciones están cifradas y las transacciones se realizan a través de las cuentas de depósito en garantía. Además, las calificaciones de proveedores, las descripciones detalladas de los productos y la confiabilidad del envío se muestran de forma destacada, lo que cultiva una apariencia de confianza y profesionalismo que desmiente la naturaleza criminal del intercambio (Akhgar et al., 2021).

Aunque no es tan frecuente como el tráfico de drogas, la venta de armas de fuego, municiones y explosivos ocupa un lugar destacado en ciertos mercados de la red oscura. Los vendedores ofrecen armas pequeñas, rifles modificados y, ocasionalmente, incluso explosivos, a menudo procedentes de zonas de conflicto o de arsenales militares (Akhgar et al., 2021). Debido al alto riesgo y a los desafíos logísticos, estas transacciones suelen limitarse a corredores regionales específicos, especialmente en Europa y Norteamérica.

El comercio de armas de fuego a menudo requiere coordinación logística fuera de línea, por lo que los vendedores pueden utilizar métodos de entrega en punto muerto o intermediarios de envío redirigidos. Akhgar et al. (2021) señalan que en varios casos documentados los traficantes de armas de la red oscura han estado estrechamente vinculados con redes paramilitares o del crimen organizado fuera de línea, aprovechando el anonimato de la red oscura para facilitar el tráfico sin exposición en la calle.

Por su parte, el fraude es un pilar de las economías criminales de la red oscura. Los mercados especializados ofrecen amplios catálogos de datos robados, incluyendo números de tarjetas de crédito, credenciales bancarias, credenciales de PayPal, números de la Seguridad Social y kits de identidad completos (Ozkaya & Islam, 2019). Estas plataformas centradas en el fraude, a menudo denominadas "foros de *carding*", sirven como sitios de comercio y espacios de formación donde los usuarios intercambian tutoriales, *software* y asesoramiento operativo (Holt & Bossler, 2020). Akhgar et al. (2021) detallan la existencia de servicios delictivos como la construcción de identidades sintéticas, el *phishing* como servicio y las soluciones integrales (comúnmente conocidas como FULZ), que permiten a los actores cometer fraudes bancarios, solicitar préstamos o llevar a cabo esquemas de

fraude fiscal con escasos conocimientos técnicos. Estos ecosistemas de fraude suelen asociarse a redes de mulas de dinero y servicios de blanqueo de capitales, para completar así una cadena de valor delictiva completa.

El desarrollo, la venta y la implementación de *software* malicioso (*malware*) es una característica destacada de la infraestructura delictiva de la *dark web*. Los proveedores ofrecen kits de explotación personalizados, paquetes de *ransomware*, *rootkits* y troyanos de acceso remoto (en inglés, RAT, por las iniciales de *Remote Access Trojan*), a menudo con precios diferenciados según la sofisticación y los servicios de soporte ofrecidos (Liggett et al., 2020; Ozkaya & Islam, 2019). Una innovación significativa ha sido la aparición del *ransomware* como servicio (RaaS). En este modelo los autores de *malware* ceden el acceso a sus herramientas a cambio de una participación en las ganancias o una comisión, lo que democratiza el acceso a ciberarmas destructivas. Ozkaya e Islam (2019) señalan que los programas de afiliados permiten a los actores novatos distribuir *ransomware* entre objetivos seleccionados con un mínimo esfuerzo, a menudo con el soporte de *backend* de los desarrolladores originales. Además, los *exploits* de día cero (vulnerabilidades desconocidas para los proveedores de *software*), también se comercializan en los mercados de la *darknet*, especialmente en foros privados, a los que solo se puede acceder con invitación. Estas herramientas son especialmente valiosas para los actores de los Estados nación y los grupos de amenazas persistentes avanzadas (en inglés, APT, por las iniciales de *Advanced Persistent Threat*), al difuminar la línea entre el crimen organizado y el ciberespionaje (Akhgar et al., 2021).

Entre los dominios más inquietantes de la *dark web* se encuentran foros y repositorios dedicados a la distribución y el consumo de material de abuso sexual infantil (MASI). Estas plataformas operan bajo rigurosos procesos de verificación, que a menudo exigen a los usuarios subir material nuevo o participar en actividades de captación de menores como requisito previo para acceder (Liggett et al., 2020; Nearchou, 2023). Gehl (2018) explora cómo estas comunidades justifican su comportamiento mediante una economía moral subcultural utilizando el cifrado y el anonimato para proteger a sus miembros, a la vez que imponen las normas comunitarias. Asimismo, la persistencia de dichos espacios, a pesar de los múltiples desmantelamientos policiales, demuestra tanto la resiliencia como la depravación de ciertos rincones de la *dark web*. Akhgar et al. (2021) destacan que el abuso sexual infantil a menudo está vinculado a redes más amplias de trata de niños y abusos fuera de línea, lo que representa una amenaza transnacional profundamente arraigada.

Gobernanza, reputación y confianza en el mercado

A pesar de ser espacios sin ley, los mercados de la *dark web* no carecen de orden. Se basan en mecanismos informales de gobernanza para generar confianza y garantizar la fiabilidad de las transacciones. Gehl (2018) describe esos sistemas como "capitalismo de plataforma desde abajo", con mecanismos como la puntuación de retroalimentación de los proveedores, la resolución pública de disputas y el acceso basado en la reputación.

Los foros suelen emplear moderadores y administradores que examinan a los nuevos usuarios, resuelven conflictos y hacen cumplir las normas. Estas prácticas reflejan los primeros ideales anarco-libertarios que buscaban construir órdenes sociales alternativos basados en la autorregulación en vez de la autoridad estatal (Gehl, 2018; Owen y Marshall, 2021). Algunos mercados también emplean servicios de depósito en garantía, donde los fondos son retenidos por agentes externos hasta que el comprador confirme su satisfacción. La introducción de monederos de criptomonedas multi-firma, que requieren múltiples claves para realizar pagos, ha reforzado la confianza en las interacciones entre vendedores y compradores (Ozkaya & Islam, 2019).

Más allá del comercio, la *dark web* también termina sirviendo como plataforma para el extremismo ideológico y el ciberterrorismo. Grupos extremistas explotan los foros de la red oscura para radicalizar a reclutas, distribuir propaganda y coordinar operaciones clandestinas (Liggett et al., 2020). Materiales como manuales para la fabricación de bombas, manifiestos yihadistas y guías para ataques de lobos solitarios se encuentran con frecuencia en archivos cifrados (Hannigan, 2021). Owen (2021) señala que el ciberterrorismo debe entenderse no solo como un ataque técnico a la infraestructura, sino también como un "acto simbólico" de violencia digital, y argumenta que el ciberterrorismo a menudo opera en el registro afectivo e ideológico con el objetivo primordial de intimidar, desestabilizar y ganar visibilidad en conflictos asimétricos. Cabe destacar que grupos como ISIS y Al-Qaeda han mantenido canales de comunicación cifrados en foros de la *dark web* para su reclutamiento y financiación. El anonimato en este espacio permite a dichos actores evitar la vigilancia, y mantener al mismo tiempo redes ideológicas a nivel global (Akhgar et al., 2021).

Como ya se ha señalado, las criptomonedas constituyen la columna vertebral financiera de la economía criminal de la *dark web*. Su naturaleza descentralizada y su seudonimia permiten transacciones entre pares que eluden los sistemas bancarios tradicionales y la supervisión gubernamental. Si bien Bitcoin sigue siendo la

divisa más reconocida de esta clase, las criptomonedas orientadas a la privacidad, como Monero, Zcash y Dash, son cada vez más preferidas por los delincuentes, debido a sus funciones de ofuscación mejoradas (Ozkaya & Islam, 2019). Gehl (2018) describe las criptomonedas como una forma de “confianza tecnológica”, que permite el comercio en entornos donde no existen mecanismos de aplicación legal. Asimismo, Akhgar et al. (2021) explican que los vendedores de la *dark web* suelen fijar el precio de sus productos en Bitcoin, pero ofrecen descuentos por transacciones en Monero, lo que refleja una tendencia hacia un mayor anonimato.

Los flujos de pago en los mercados oscuros suelen incluir servicios de depósito en garantía, contratos con límite de tiempo y mezcladores/*tumblers*, servicios que combinan múltiples transacciones de criptomonedas para ocultar el origen y el destino. Estos instrumentos, en conjunto, complican las investigaciones forenses dificultando a las fuerzas del orden rastrear las pistas financieras. Además, la integración de cajeros automáticos de criptomonedas, tarjetas de regalo prepagadas y redes de mulas de dinero permite blanquear activos digitales para convertirlos en moneda fiduciaria, y cerrar así el ciclo financiero ilícito. Según Liggett et. al (2020), esta integración refleja la maduración de las finanzas empresariales delictivas, comparable en su sofisticación al comercio global legítimo.

A pesar de las innovaciones estructurales y los mecanismos de confianza, los mercados de la *dark web* siguen siendo volátiles y vulnerables a la traición. Un riesgo importante es la estafa de salida, en la que los administradores del mercado desaparecen repentinamente con los fondos en custodia de los usuarios, que a veces ascienden a millones en criptomonedas (Akhgar et al., 2021). Por ejemplo, Evolution Market, una de las plataformas más exitosas de la *dark web*, desapareció repentinamente en 2015, supuestamente robando más de 12 millones de dólares en Bitcoin. Estas traiciones erosionan la confianza de los usuarios, pero, paradójicamente, no logran disuadir por completo la participación delictiva. Los usuarios suelen migrar a plataformas más nuevas con funciones mejoradas o una gobernanza comunitaria (Gehl, 2018).

La volatilidad del mercado también se ve agravada por las redadas policiales, el hackeo por parte de grupos rivales o las disputas internas. Estas disrupciones han dado lugar a un fenómeno de “salto de mercado”, en el que los proveedores conservan su reputación exportándola a nuevas plataformas, a veces verificadas mediante pruebas criptográficas (Ozkaya & Islam, 2019). Esta resiliencia refuerza la conceptualización de la *dark web* como un ecosistema criminal. No es solo un mercado, sino uno que se adapta, muta y se regenera tras crisis sistémicas.

Combatir la ciberdelincuencia organizada en la *dark web* plantea graves desafíos jurisdiccionales y tecnológicos. La arquitectura anónima de las plataformas,

la distribución global de servidores y el uso de comunicaciones cifradas crean barreras a la vigilancia policial tradicional. No obstante, los organismos internacionales encargados de hacer cumplir la ley han desarrollado nuevas estrategias. Operaciones conjuntas como la Operación Disruptor, la Operación Bayoneta y la Operación Onymous han logrado dismantelar importantes mercados como AlphaBay, Hansa y Silk Road (Liggett et al., 2020). Estas operaciones suelen basarse en la ciberinfiltración, *honeypots*, la implantación de *malware* y técnicas de análisis de *blockchain*.

Akhgar et al. (2021) argumentan que el intercambio colaborativo de inteligencia entre las unidades cibernéticas (Interpol, Europol, el FBI y los CERT nacionales como ColCERT) ha resultado vital. Sin embargo, advierten que la aplicación de la ley por sí sola no puede dismantelar el ecosistema. La descentralización de la *dark web*, las redes de confianza comunitaria y la innovación continua requieren respuestas multisectoriales, que incluyen la regulación de criptomonedas, colaboración con empresas de ciberseguridad e inversión en capacidades forenses digitales. Además, académicos como Owen (2021) abogan por una reevaluación criminológica de la ciberdelincuencia: en efecto, Owen (2021) sugiere que herramientas conceptuales como su "Marco Genético-Social" pueden ayudar a las fuerzas del orden a comprender mejor los perfiles, las motivaciones y los patrones de comportamiento de los delincuentes en contextos digitales.

La *dark web* como un ecosistema criminal complejo

La *dark web* no es simplemente una capa oculta de internet: es un ecosistema criminal complejo y en constante evolución que fusiona tecnología, comercio, ideología y desviación. Su estructura alberga grupos delincuenciales organizados interconectados, posibilita nuevas formas de comportamiento en el mercado y ofrece protección a actores que operan más allá de la supervisión estatal tradicional. Pero al mismo tiempo, la *dark web* revela paradojas, al ser un espacio que combina orden y volatilidad, confianza y traición, invisibilidad y vigilancia. Sus redes criminales reflejan y desafían los modelos convencionales del crimen organizado, y exigen, en consecuencia, nuevas herramientas teóricas y prácticas para el análisis y la intervención.

El concepto de "ecosistema criminal" no se utiliza como una metáfora descriptiva, sino como una categoría analítica anclada en la teoría de los sistemas complejos adaptativos. Desde esa perspectiva, la arquitectura ilícita del ciberespacio (y en particular, los entornos asociados a la *dark web*) puede entenderse como un sistema dinámico compuesto por múltiples agentes heterogéneos (actores criminales, intermediarios, plataformas, protocolos, infraestructuras técnicas

y usuarios), cuyas interacciones no lineales producen patrones emergentes de orden, adaptación y resiliencia.

De acuerdo con Thurner et al. (2018), los sistemas complejos se caracterizan por la ausencia de control centralizado, la interacción local entre agentes, la no linealidad de los procesos y la emergencia de propiedades globales que no pueden reducirse a la suma de sus componentes individuales. Aplicado al estudio del cibercrimen, este enfoque permite superar las aproximaciones tradicionales que conciben la criminalidad digital como una agregación de delitos aislados o como redes jerárquicas relativamente estables. En contraste, la *dark web* opera como un sistema abierto, evolutivo y autorregulado, en el que la innovación criminal, la especialización funcional, la cooperación táctica y la competencia interna emergen mediante procesos de aprendizaje distribuido y adaptación continua frente a presiones externas como la acción estatal, la regulación jurídica o la disrupción tecnológica. Tal como señalan Thurner et al. (2018), en los sistemas complejos adaptativos la estabilidad no implica equilibrio, sino capacidad de reorganización frente al cambio, una lógica que resulta en particular pertinente a comprender la persistencia del crimen digital.

Bajo este marco analítico, ni los mercados ilícitos digitales, ni los foros clandestinos, ni los servicios criminales *as-a-service* ni las infraestructuras técnicas que los sostienen constituyen entidades independientes, sino, más bien, nodos interconectados de un ecosistema criminal digital. Su estabilidad relativa no depende de la permanencia de actores específicos, sino de la capacidad del sistema para recombinar funciones, reemplazar nodos y reorganizar flujos de valor ilícito cuando se producen choques o intervenciones externas. En este sentido, la *dark web* se comporta como un entorno adaptativo complejo, donde la persistencia del crimen digital se explica menos por la fortaleza individual de sus actores, y más, por la lógica sistémica de autoorganización que estructura el conjunto.

Este enfoque permite comprender por qué las estrategias de represión centradas exclusivamente en la eliminación de plataformas, mercados o individuos tienden a generar efectos limitados o contraproducentes, pues al operar sobre nodos visibles sin alterar las dinámicas sistémicas subyacentes, el ecosistema criminal tiende a reconfigurarse, fragmentarse y reaparecer bajo nuevas formas funcionales. Por consiguiente, comprender la *dark web* desde la perspectiva de un "ecosistema criminal" ofrece un marco integral para interpretar su complejidad, resiliencia y potencial de amenaza en constante evolución.

El concepto de "ecosistema criminal", propuesto por Álvarez y Rodríguez (2018), se basa en la ecología funcional y la teoría general de sistemas para caracterizar los fenómenos criminales no como comportamientos aislados, sino como

sistemas en red de una variedad de actores, recursos y entornos interdependientes que sustentan la globalización desviada y erosionan la soberanía estatal (Álvarez & Zambrano, 2017). La *dark web* ejemplifica esta lógica de criminalidad ecosistémica en formato digital. Funciona como un hábitat donde actores ilegales como *hackers*, vendedores, terroristas y blanqueadores interactúan dentro de un territorio tecnológico (Tor, servicios ocultos, protocolos de criptomonedas), el cual sirve tanto de entorno físico como de infraestructura facilitadora. Y al igual que la descripción que hacen Álvarez y Rodríguez (2018) de los ecosistemas criminales territoriales en Colombia, la *dark web* alberga una constelación estructurada de nodos de actividad ilegal (mercados, foros, servicios), y de flujos de capital, *malware*, información y contenido ideológico.

De acuerdo con Álvarez y Rodríguez (2018), los ecosistemas se definen por sus ciclos de retroalimentación, la entrada de recursos y la interdependencia entre actores. Pues bien, en la *dark web* existen ciclos de retroalimentación positivos cuando las estafas exitosas financian un mayor desarrollo de *malware*, lo que, a su vez, aumenta la capacidad de ataque y las ganancias económicas. De igual manera, las rutas de flujo vinculan a los desarrolladores, los distribuidores y los consumidores de herramientas y servicios ilícitos formando una cadena de suministro descentralizada, pero funcionalmente integrada. Estos procesos reflejan la observación, hecha por Álvarez (2017), de que “los ecosistemas criminales generalmente prosperan gracias a las interacciones adaptativas entre los organismos criminales y las oportunidades del entorno” (p. 310).

Así como Álvarez y Rodríguez (2018) identifican a las “regiones portal” y a los “espacios vacíos” como características geográficas clave de los ecosistemas criminales físicos —es decir, las áreas donde la presencia estatal es débil o inexistente (Álvarez, 2017)—, la *dark web* también prospera en los vacíos jurisdiccionales y los puntos ciegos tecnológicos resistiendo la regulación estatal y trascendiendo las fronteras nacionales. Su arquitectura, basada en el anonimato, el cifrado y la infraestructura descentralizada, se asemeja a los factores ambientales que se hallan en ecosistemas físicos con control estatal limitado, como regiones fronterizas remotas o barrios marginales urbanos.

Además, de conformidad con lo señalado por Álvarez y Rodríguez (2018), los ecosistemas criminales se caracterizan por nodos de convergencia, donde se intersecan diferentes economías ilegales. La *dark web* es, precisamente, uno de esos nodos: un metaespacio donde convergen y coevolucionan la comercialización de narcóticos, el fraude cibernético, el terrorismo, la explotación infantil y el tráfico ilícito de armas. Estas formas de convergencia incrementan la complejidad y resiliencia del sistema, y dificultan a las autoridades dismantelar redes enteras

sin fragmentarlas en subredes más ágiles, un fenómeno similar a la descripción de Álvarez y Rodríguez (2018) de las "redes en malla", en las que los actores criminales interactúan de forma policéntrica sin estructuras de mando jerárquicas.

El análisis del cibercrimen (y en particular, el de los ecosistemas ilícitos que operan en la *dark web*) plantea desafíos metodológicos que desbordan los marcos tradicionales de estudio del crimen organizado. Los modelos clásicos, desarrollados principalmente para comprender organizaciones criminales territoriales, jerárquicas y relativamente estables (mafias, carteles, estructuras insurgentes), tienden a privilegiar categorías como liderazgo, cadena de mando, control territorial y economías ilegales delimitadas. Si bien estas aproximaciones han demostrado utilidad en los contextos físicos y estatales, resultan insuficientes para capturar la dinámica fluida, distribuida y transnacional del crimen digital contemporáneo.

Desde la perspectiva de la inteligencia y la defensa, el enfoque de sistemas complejos adaptativos ofrece ventajas analíticas decisivas. En primer lugar, permite comprender el cibercrimen no como un conjunto de actores discretos, sino como un sistema dinámico de interacciones no lineales, en el que múltiples agentes heterogéneos (humanos y tecnológicos) coevolucionan en función de incentivos, oportunidades y presiones externas. Este enfoque desplaza la atención desde las figuras visibles del delito hacia las condiciones sistémicas que posibilitan su reproducción y resiliencia.

En segundo lugar, los sistemas complejos adaptativos permiten explicar por qué muchas intervenciones represivas tradicionales (centradas en la captura de líderes, el cierre de plataformas o la eliminación de mercados específicos) generan efectos limitados o, incluso, contraproducentes. Al operar sobre nodos particulares sin alterar las dinámicas estructurales del sistema complejo, dichas intervenciones suelen provocar procesos de reorganización, fragmentación y adaptación, mediante los cuales el ecosistema criminal se reconfigura y persiste. Para la inteligencia estratégica ello implica que la disrupción efectiva del cibercrimen requiere identificar puntos de fragilidad sistémica, flujos críticos y mecanismos de retroalimentación, más que concentrarse exclusivamente en objetivos individuales.

En tercer lugar, este enfoque resulta en especial pertinente a la defensa en entornos de conflicto híbrido y guerra cognitiva, donde el cibercrimen, el espionaje, la desinformación y las operaciones encubiertas tienden a entrelazarse. Al concebir la *dark web* como un ecosistema adaptativo, se vuelve posible analizar cómo actores estatales y no estatales explotan infraestructuras criminales preexistentes, externalizan capacidades ilícitas o utilizan economías ilegales digitales como instrumentos indirectos de presión estratégica.

Finalmente, la adopción de una perspectiva de sistemas complejos favorece una lógica anticipatoria, central para la inteligencia moderna. En vez de limitarse a la atribución retrospectiva de incidentes, este enfoque permite detectar patrones emergentes, señales débiles y trayectorias de evolución criminal, y contribuye así al diseño de estrategias de prevención, disuasión y resiliencia institucional. En este sentido, el enfoque ecosistémico no solo amplía la comprensión académica del cibercrimen, sino que proporciona un marco metodológico más adecuado para la toma de decisiones en seguridad y defensa en el siglo XXI.

Una vez establecida la pertinencia del enfoque de sistemas complejos adaptativos para el análisis del cibercrimen, resulta posible (y metodológicamente necesario) traducir el concepto de ecosistema criminal a una lógica operativa que permita su utilización por parte de analistas de inteligencia, planificadores estratégicos y tomadores de decisión en seguridad y defensa. En este sentido, el valor del enfoque ecosistémico no reside únicamente en su capacidad explicativa, sino en su potencial para identificar regularidades funcionales, dependencias sistémicas y puntos de intervención estratégica dentro de sistemas criminales que operan sin control centralizado y bajo condiciones permanentes de adaptación.

Con base en lo anterior y a fin de operacionalizar este enfoque, el ecosistema criminal digital asociado a la *dark web* puede representarse de manera sintética a partir de tres dimensiones interdependientes: actores, flujos y tecnologías. Esta representación no pretende reducir la complejidad del fenómeno, sino ofrecer una cartografía funcional mínima que permita comprender cómo se organiza, se reproduce y se adapta el crimen digital en ausencia de jerarquías estables (tabla 4).

Tabla 4. Esquema operativo del ecosistema criminal de la *dark web*³

Dimensión	Componentes principales	Función sistémica dentro del ecosistema criminal
Actores	Desarrolladores de <i>malware</i> y <i>exploits</i> ; operadores de mercados ilícitos; proveedores de servicios <i>crime-as-a-service</i> ; intermediarios financieros y lavadores digitales; usuarios finales; actores híbridos (estatales y paraestatales)	Ejecutan funciones especializadas dentro de una red policéntrica. Los roles no están fijados jerárquicamente, sino que se asignan dinámicamente según reputación, capacidades técnicas y oportunidades del entorno

Continúa en la otra página

³ El ecosistema criminal no depende de la permanencia de nodos individuales, sino de la interacción sostenida entre estas tres dimensiones. Por ello, la disrupción aislada de actores o plataformas específicas tiende a ser absorbida mediante procesos de reorganización sistémica.

Dimensión	Componentes principales	Función sistémica dentro del ecosistema criminal
Flujos	Capital financiero ilícito (criptomonedas); datos robados; <i>malware</i> y <i>exploits</i> ; servicios criminales; contenidos ideológicos y narrativas	Conectan a los actores mediante rutas múltiples y redundantes. Permiten la adaptación del sistema, su resiliencia frente a disrupciones y la recombinación funcional tras intervenciones externas
Tecnologías	Redes de anonimización (Tor, I2P); servicios ocultos y <i>bulletproof hosting</i> ; criptomonedas, mezcladores y <i>privacy coins</i> ; plataformas de mensajería cifrada; infraestructura descentralizada	Constituyen el entorno habilitador del ecosistema criminal. Reducen la trazabilidad, amplían los márgenes de impunidad y configuran tanto oportunidades como vulnerabilidades estructurales

Fuente: elaboración propia.

Una vez operacionalizado el ecosistema criminal de la *dark web* en términos de actores, flujos y tecnologías, el siguiente paso analítico consiste en dotar a este esquema de una lógica anticipatoria que permita no solo describir el fenómeno, sino advertir su evolución, mutaciones y posibles escaladas de amenaza. En este punto resulta pertinente introducir el concepto de *warning intelligence* (inteligencia de alerta temprana), una tradición analítica clásica de los estudios de inteligencia que adquiere renovada relevancia en entornos criminales complejos y adaptativos.

Desde la perspectiva clásica, la inteligencia de “alerta temprana” se define como la función de la inteligencia orientada a detectar indicios tempranos de amenazas emergentes, con el fin de proporcionar a los decisores el tiempo y el espacio necesarios para responder antes de que dichas amenazas se materialicen plenamente. Para Grabo (2010), la advertencia estratégica no se basa en la predicción exacta de eventos, sino en la identificación de patrones anómalos, cambios graduales y señales débiles que indiquen una modificación significativa en las capacidades, intenciones o comportamientos de un adversario. En términos similares, Wirtz (2017) subraya que el fracaso de la inteligencia de alerta temprana no suele obedecer a la ausencia de información, sino a la incapacidad para interpretar correctamente señales dispersas dentro de contextos complejos y ambiguos. Gentry y Gordon (2019) amplían este enfoque al señalar que la *strategic warning intelligence* resulta sobremano desafiante en escenarios donde los actores no estatales, las tecnologías emergentes y las dinámicas no lineales erosionan los supuestos clásicos de previsibilidad. En dichos contextos la advertencia no puede basarse exclusivamente en indicadores lineales o jerárquicos, sino que debe orientarse a la comprensión de sistemas dinámicos, capaces de reorganizarse con prontitud frente a la presión externa.

Esta observación resulta en particular relevante para el análisis del ecosistema delictivo digital. Como ya se argumentó, la *dark web* opera en la forma de

un complejo sistema adaptativo, caracterizado por la ausencia de control centralizado, la recombinación funcional de nodos y la resiliencia estructural frente a intervenciones represivas. En consecuencia, la utilidad de la *warning intelligence* en este entorno no reside en anticipar actos delictivos específicos, sino en detectar transformaciones sistémicas que indiquen procesos de adaptación, escalamiento o convergencia criminal. Desde esta óptica, el enfoque ecosistémico y la inteligencia de alerta temprana se refuerzan mutuamente. Mientras el primero permite mapear la estructura y las interdependencias del sistema criminal, la segunda proporciona una lógica metodológica para observar su dinámica evolutiva. En vez de centrarse en actores individuales o plataformas concretas, la advertencia estratégica se orienta hacia la vigilancia de flujos críticos, innovaciones tecnológicas, cambios en patrones de interacción y mutaciones narrativas, todos ellos indicadores tempranos de transformación del ecosistema.

A fin de traducir esta lógica en una herramienta analítica concreta, la tabla 5 presenta una matriz de identificación de puntos de intervención estratégica, diseñada desde una perspectiva de *warning intelligence* aplicada a ecosistemas criminales digitales.

Tabla 5. Matriz de *warning intelligence* para el ecosistema criminal de la dark web

Elemento del ecosistema criminal	Indicadores de alerta temprana	Valor estratégico para inteligencia y defensa
Flujos financieros ilícitos	Cambios abruptos en el uso de criptomonedas; migración hacia <i>privacy coins</i> ; aparición de nuevos mezcladores o protocolos de anonimato financiero	Señala procesos de adaptación frente a presión regulatoria o preparación de operaciones criminales de mayor escala
Infraestructura tecnológica	Incremento en el uso de nuevos servicios ocultos; <i>bulletproof hosting</i> o tecnologías emergentes de anonimización	Indica reorganización ecosistémica tras acciones de disrupción estatal o tecnológica
Mercados y foros clandestinos	Aparición de servicios integrados (<i>bundling criminal</i>); especialización funcional extrema, o consolidación de reputaciones transversales	Refleja maduración del ecosistema y aumento de eficiencia operativa
Interacciones actorales	Convergencia entre actores criminales, ideológicos y estatales en espacios compartidos	Alerta sobre procesos de hibridación entre crimen organizado, espionaje y conflicto híbrido
Narrativas y contenidos	Circulación de discursos que legitiman el crimen como resistencia, negocio o causa política	Señal temprana de normalización social del delito y expansión de bases de apoyo digitales

Fuente: elaboración propia, con base en Grabo (2010), Wirtz (2017) y Gentry y Gordon (2019).

Desde una lógica de inteligencia anticipatoria, la intervención estratégica eficaz no consiste en “desmantelar” el ecosistema criminal (un objetivo poco realista en sistemas complejos adaptativos), sino en incrementar los costos de adaptación, reducir la velocidad de recombinación funcional y generar fricciones persistentes en flujos y tecnologías críticas. Para la inteligencia y la defensa, ello implica priorizar la detección de señales débiles, identificar cuellos de botella sistémicos y anticipar trayectorias evolutivas del crimen digital, en vez de respuestas reactivas centradas exclusivamente en actores visibles. En conjunto, la integración entre el marco de sistemas complejos, la operacionalización del ecosistema criminal y la lógica de la *warning intelligence* refuerza el valor del enfoque ecosistémico como herramienta analítica, prospectiva y decisional. La *dark web* aparece así no solo como un espacio de ilegalidad, sino como un sistema dinámico de poder criminal, cuya comprensión exige enfoques capaces de articular complejidad, anticipación y estrategia en los escenarios contemporáneos de seguridad y defensa.

En definitiva, abordar la *dark web* como un ecosistema criminal digital permite a académicos y profesionales ir más allá de las nociones simplistas del “ciber-crimen como herramienta” y apreciar su naturaleza sistémica, adaptativa e integrada. Reconoce las interacciones multiescalares entre individuos, tecnologías, economías y sistemas de gobernanza que sustentan el submundo cibernético. Así como Álvarez (2017) advierte que la ausencia de autoridad estatal en los ecosistemas criminales físicos de Colombia conduce a una gobernanza basada en la ilegalidad, la ausencia de marcos jurídicos internacionales y de capacidad de aplicación de la ley en el ciberespacio abre la puerta a que actores cibernéticos no estatales ejerzan coerción, legitimidad y control sobre los territorios digitales.

Por lo tanto, el desafío para los responsables políticos de la toma de decisiones y las instituciones de seguridad y defensa no consiste en, simplemente, reprimir a actores aislados, sino en intervenir de manera estratégica en el propio ecosistema: modificando las entradas, alterando las rutas de flujo, reduciendo los incentivos sistémicos y restaurando la gobernanza del espacio digital. En resumen, la *dark web* no es un espacio monolítico de maldad ni una colección aleatoria de actos ilegales: por el contrario, es un ecosistema complejo, dinámico e interconectado (es decir, una biosfera en evolución de delincuencia, desviación y convergencia), que refleja tanto las posibilidades como los fracasos de la globalización del siglo XXI.

Delitos de conexión e inmersión: redes sociales, metacrimen y desviación digital

La constante evolución del ciberespacio ha dado lugar no solo a nuevas formas de comunicación y de comercio, sino también a nuevas modalidades de comportamiento delictivo. Entre ellas, dos destacan por su complejidad e importancia: el cibercrimen en plataformas de redes sociales y la emergente categoría de *metacrímenes* en entornos digitales inmersivos como el metaverso. Ambos fenómenos trascienden los marcos criminológicos tradicionales, y plantean desafíos únicos para la regulación, la aplicación de la ley y la comprensión conceptual.

El cibercrimen en las plataformas de redes sociales se ha desarrollado a la par con la proliferación de estas plataformas, al igual que el contenido generado por los usuarios. Como argumentan Babu y Siddik (2022), la rápida expansión de las TIC ha creado un terreno fértil para la innovación delictiva, especialmente en ámbitos caracterizados por el anonimato, la velocidad y los flujos transfronterizos de información. Estos incluyen delitos como el robo de identidad, acoso, obscenidad digital y manipulación de datos personales. Sin embargo, como señalan Smith y Haines (2023), las categorizaciones tradicionales a menudo no toman en cuenta la naturaleza fluida y polimórfica de estos cibercrímenes: por ejemplo, muchos cibercrimitos en redes sociales abarcan simultáneamente múltiples categorías, combinando elementos de daño interpersonal, robo de propiedad y sabotaje reputacional.

Paralelamente a estos desarrollos, la aparición del metacrimen (comportamiento delictivo en entornos digitales inmersivos, persistentes y descentralizados, como el metaverso) presagia una ruptura epistemológica en la comprensión del propio delito. El metacrimen no es simplemente una extensión del cibercrimen: abarca un nuevo espectro de desafíos criminógenos, victimógenos, etiológicos y regulatorios, como lo demuestran Zhou et al. (2025). Estos delitos involucran avatares, contratos inteligentes y activos virtuales, y a menudo ocurren en zonas grises legales más allá de la jurisdicción territorial convencional. Además, el metacrimen implica nuevas dimensiones afectivas y cognitivas de victimización, debido a la naturaleza inmersiva y corporizada del metaverso.

Para fundamentar este análisis se hace necesario basarse en dos marcos teóricos complementarios. En primer lugar, la categorización de Wall (2007) del cibercrimen en delitos de contenido, delitos de integridad y delitos de engaño/robo proporciona una tipología útil para analizar el cibercrimen en las redes sociales. En segundo lugar, para el metacrimen adopto la perspectiva conceptual de Tiwari

et al. (2025), quienes argumentan que el delito en el metaverso debe evaluarse a través de las dimensiones criminógena, victimogénica y regulatoria. Estos marcos se emplearán a continuación para sistematizar el debate y destacar los puntos de convergencia y divergencia entre los delitos en redes sociales y el metacrimen.

Finalmente, este apartado se alinea con el modelo de los ecosistemas criminales de Álvarez y Rodríguez (2018), que conceptualizan el cibercrimen como una interacción dinámica entre actores, facilitadores y mercados. Con base en este modelo, la red oscura y las comunicaciones cifradas, al igual que las plataformas descentralizadas, funcionan como facilitadores y sustratos para la evolución de organizaciones criminales. Adicionalmente, las nuevas actividades de ciberdelincuencia, como el acoso en redes sociales o las estafas descentralizadas de *tokens* no fungibles (en inglés, NFT, por las iniciales de *Non-Fungible Tokens*), vienen reflejando la lógica de dicho ecosistema, caracterizado por su modularidad, su adaptabilidad y su alcance transnacional. Como se procura demostrar, tanto la delincuencia en redes sociales como el metacrimen ocupan zonas diferentes, aunque cada vez más superpuestas, dentro de esta arquitectura ilícita en evolución.

Cibercrimen en redes sociales

Las plataformas de redes sociales han transformado la naturaleza de la interacción pública y privada. Como explica Salter (217), estas plataformas de redes sociales ofrecen tanto el alcance y la velocidad de la comunicación masiva como también la intimidad de la correspondencia privada, a condiciones que propician la delincuencia digital. El diseño algorítmico de plataformas como Facebook, Twitter (X), Instagram y TikTok optimiza la interacción, mas no la seguridad, lo que permite una rápida difusión de contenido dañino, desinformación y la reproducción viral de conductas delictivas (por ejemplo, discursos de odio o pornografía vengativa). A su vez, el anonimato (o *seudonimato*), la transitoriedad del contenido y la escala global de las redes sociales debilitan las respuestas legales convencionales, especialmente al abordar delitos transjurisdiccionales o cuando este tipo de plataformas digitales se resisten a las citaciones judiciales debido a preocupaciones sobre la soberanía de los datos (Singh et. al, 2023). En este contexto, el cibercrimen deja de ser una simple conducta ilícita para convertirse en una característica estructural integrada en el diseño de los sistemas de redes sociales.

A partir de las tipologías propuestas en Roy y Tripathy (2023), el cibercrimen en redes sociales puede clasificarse en cinco dominios interrelacionados: El primero está relacionado con la ciberdifamación, una forma de ciberdelito que implica la

difusión de contenido falso, engañoso o humillante para dañar la reputación de personas. A menudo manifestada mediante imágenes manipuladas, narrativas falsas o campañas de desinformación coordinadas, la difamación se vuelve especialmente perjudicial en casos que involucran a mujeres, funcionarios públicos o grupos minoritarios. La velocidad a la que se comparte este contenido puede amplificar el daño, especialmente en ataques virales masivos o troleo orquestado (Singh et. al, 2023).

El segundo ámbito de los ciberdelitos en redes sociales es el relacionado con el acoso cibernético, que incluye el seguimiento, vigilancia o intimidación persistentes a través de mensajes directos, etiquetado o publicación repetida de datos personales. Cabe señalar que las redes sociales permiten a los acosadores monitorear a sus objetivos en múltiples plataformas en tiempo real; asimismo, el acoso puede ser de género, racial o político, lo que constituye violencia digital (Salter, 2017). El tercero es el *grooming* y la explotación infantil en línea: en efecto, una de las amenazas más graves es el uso de las redes sociales para iniciar, desarrollar y agravar conductas de *grooming*, donde los adultos manipulan a los menores para que realicen actos sexuales o de explotación. Estas interacciones pueden culminar en imágenes sexuales autogeneradas, trata o, incluso, secuestro. La capacidad para suplantar identidades y explotar la ingenuidad digital de los jóvenes usuarios exacerba el riesgo de este delito cibernético (Kumari et al., 2023).

El cuarto dominio de los ciberdelitos en las redes sociales es la desinformación e interferencia electoral, ya que las redes sociales también son un vector principal de comportamientos como la desinformación política, la desinformación relacionada con la salud (propaganda antivacunas) y los medios manipulados digitalmente (*deepfakes*). Estos comportamientos son instrumentalizados cada vez más por actores estatales y no estatales que buscan erosionar la confianza en las instituciones o manipular los procesos democráticos. Finalmente, se encuentra el *doxing*, donde la exposición deliberada de información personal (dirección, lugar de trabajo, números de teléfono) con intenciones maliciosas, conocida como *doxing*, se emplea cada vez más contra periodistas, funcionarios públicos, activistas u otras figuras públicas. Esta forma de ciberdelito utiliza como arma datos disponibles públicamente, y a menudo resulta en amenazas reales, pérdida de empleo o traumas de salud mental.

Una característica del ciberdelito en las redes sociales es su papel facilitador de la arquitectura de las mismas plataformas. Características de diseño como las funciones de retuitear/compartir, los “me gusta” y los comentarios, la difusión

algorítmica de contenido y una mínima configuración de privacidad predeterminada facilitan, a su vez, la viralidad del contenido dañino. Además, muchas plataformas monetizan los datos y la interacción de los usuarios, lo que crea incentivos perversos para retener durante más tiempo contenido controvertido o sensacionalista. Por ello, las plataformas de redes sociales no son intermediarios pasivos en la ciberdelincuencia: más bien, funcionan como facilitadores sociotécnicos que moldean, sostienen y, en ocasiones, amplifican la conducta delictiva en línea (Roy & Choudhary, 2023).

Salter (2017) profundiza esta crítica argumentando que la lógica económica y de diseño de las plataformas, impulsada por la mercantilización del contenido generado por los usuarios, genera lo que él denomina “daño predecible”. Es decir, el abuso en línea, que incluye el acoso, las amenazas y la distribución no consensuada de imágenes no es una aberración, sino un resultado estructural de las posibilidades de la plataforma. Es más, Salter (2017) sitúa esto dentro de una teoría crítica del abuso en línea, al señalar que estos daños rara vez son priorizados por los moderadores o las fuerzas del orden, especialmente cuando las víctimas son mujeres o usuarios marginados.

Pero a pesar de la creciente evidencia que vincula la arquitectura de redes sociales con algunos ciberdelitos, los marcos legales siguen siendo reactivos y fragmentados. Roy y Choudhary (2023) critican la insuficiencia de las leyes nacionales actuales señalando que la mayoría de los marcos (incluida la Ley de Tecnologías de la Información de la India y leyes comparables en el Sur Global), carecen de fuerza para su aplicación, debido a la escasez de recursos en las unidades policiales y a la insuficiente capacitación digital. Además, en jurisdicciones como la de Estados Unidos, el artículo 230 de la Ley de Decencia en las Comunicaciones ha protegido históricamente a las plataformas de redes sociales de la responsabilidad por el contenido de terceros. Aunque fue modificada por FOSTA-SESTA, en 2018, para permitir el enjuiciamiento civil y penal de los sitios web involucrados en la trata de personas con fines de explotación sexual, la ley sigue siendo controvertida y de alcance limitado.

A nivel internacional, la coordinación regulatoria también sigue siendo un desafío. Si bien la Convención de Budapest representa, hasta el momento, el principal tratado internacional sobre ciberdelincuencia, Estados clave, como la Federación de Rusia y la República Popular de China no son signatarios, y ello dificulta su aplicación a nivel mundial. Hayes y Luther (2018) destacan las disparidades jurisdiccionales que surgen cuando los perpetradores, las plataformas y las víctimas

operan en diferentes territorios legales, lo que conduce a una aplicación inconsistente de la ley y a una reparación deficiente para las víctimas.

Esta disyuntiva socio-legal se hace visible en estudios de caso de alto perfil. El incidente de “Bois Locker Room”, en la India (2020), reveló cómo los chats grupales de Instagram pueden servir de repositorios de contenido misógino, que superan tanto a los sistemas disciplinarios escolares como a los moderadores de la plataforma. De igual manera, la campaña #Gamergate (2014-presente) utilizó como arma las posibilidades de la plataforma, como las etiquetas y el anonimato, para coordinar el abuso contra las mujeres en los videojuegos, lo cual vino a revelar los puntos ciegos sistémicos en los algoritmos de moderación de Twitter y Reddit. Finalmente, el Disturbio del Capitolio en los Estados Unidos del 6 de enero de 2021 ejemplificó la transición de la incitación digital a la violencia física, propiciada por las cámaras de resonancia de las plataformas y la incapacidad de la moderación algorítmica para anticipar la movilización a gran escala.

Metacrimen: criminalidad inmersiva en el metaverso

El término “metacrimen” se refiere a los actos ilícitos cometidos en entornos virtuales inmersivos, persistentes y tridimensionales, como, por ejemplo, el metaverso. A diferencia del cibercrimen convencional, que ocurre en contextos bidimensionales mediados por pantallas, el metacrimen surge de las interacciones corpóreas basadas en avatares en espacios digitales diseñados para imitar y extender la realidad física (Tiwari et al., 2025). Estos ciberdelitos son posibles gracias a tecnologías como la realidad virtual (RV), la realidad aumentada (RA), la cadena de bloques (*blockchain*), la inteligencia artificial (IA) y los contratos inteligentes, por lo que desafían la jurisprudencia convencional, debido a su indeterminación espacial, ambigüedad jurisdiccional e intensidad psicológica. Tiwari et al. (2025) argumentan que el metacrimen presentaría al menos cinco dimensiones que lo distinguen del cibercrimen: 1) criminógeno (nuevas oportunidades), 2) victimógeno (vulnerabilidades únicas), 3) etiológico (causas distintas), 4) ético (daño inmersivo) y 5) regulatorio (fallos de las fuerzas del orden).

En este orden de ideas, el metaverso no sería tan solo una nueva plataforma para el cibercrimen existente, sino un novedoso terreno criminológico que reconfigura las relaciones entre el espacio, la identidad, el delito y la justicia. Interpol (2024) ha descrito recientemente siete categorías principales de metacrimen: los delitos de identidad, los delitos financieros, los delitos contra la propiedad intelectual, los delitos contra la propiedad, los delitos sexuales, los delitos contra menores

y el cibercrimen generalizado. Estos se comprenden mejor si se analizan a través de unas modalidades específicas:

1. Violencia sexual basada en avatares y acoso inmersivo: uno de los aspectos más controvertidos del metacrimen se refiere a la agresión y el acoso sexual que sufren los avatares en entornos de RV. Aunque no hay contacto físico, el realismo perceptual de los trajes hápticos, audio espacializado e interfaces corpóreas crea sensaciones intensas que las víctimas experimentan como profundamente violentas. Zhou et al. (2025) enfatizan que el impacto psicológico de una agresión virtual inmersiva puede rivalizar con el trauma psicológico del mundo real, lo que dificulta la distinción entre daño simbólico y daño material.
2. Estafas de NFT, *Rug Pulls* y comercio de lavado: los metaversos basados en la infraestructura *blockchain* admiten NFT y activos digitales como terrenos, *wearables* o avatares. Estos ecosistemas *tokenizados* han generado variadas estafas como *Rug Pulls* (abandono de un proyecto tras recaudar fondos de inversores), comercio de lavado (transacciones simuladas para inflar precios) y mercados falsos de NFT (Annison, 2022). Además, la falta de protección a los inversores, los protocolos KYC/AML deficientes y los mecanismos de intercambio descentralizados facilitan estos fraudes (Tiwari et al., 2025).
3. Blanqueo de capitales y financiación del terrorismo: los delincuentes explotan la fluidez de los criptoactivos para blanquear ganancias ilícitas, y evadir así a las instituciones financieras tradicionales. Como detallan Tiwari et al. (2025), las plataformas de metaverso permiten a los delincuentes convertir fondos ilícitos en monedas digitales, comprar terrenos virtuales o avatares y luego venderlos a monederos limpios. Estos rastros de dinero virtual son difíciles de rastrear y se complican aún más por el anonimato de los identificadores descentralizados.
4. Suplantación de avatar y robo de identidad *deepfake*: la suplantación de un avatar permite a los actores engañar, manipular o defraudar a otros actores en entornos persistentes. Con renderizado en tiempo real, además de retroalimentación biométrica y herramientas de IA generativa, los avatares pueden imitar convincentemente a personas reales. Estas suplantaciones pueden utilizarse en esquemas de *phishing*, captación de usuarios, extorsión y campañas de desinformación (Zhou et al., 2025). Es importante destacar que el realismo psicológico de las interacciones de los avatares intensifica el impacto del engaño.

5. Explosiones de contratos inteligentes y robo de activos virtuales: los contratos inteligentes automatizan las transferencias de activos, pero son altamente sensibles a las vulnerabilidades a nivel de código. Tiwari et al. (2025) documentan cómo los atacantes han manipulado contratos inteligentes para vaciar billeteras, falsificar *tokens* dentro de la plataforma y crear versiones falsas de activos digitales legítimos. Un ejemplo de ello fue la falsificación de Robux, en Roblox, donde las transacciones no autorizadas minaron la confianza en la plataforma.
6. Delitos internos-internos y entre reinos: Seo et al. (2023) clasifican los metadelitos en cuatro categorías: 1) internos-internos (p. ej., robo completamente dentro del metaverso), 2) internos-externos (el delito ocurre en el metaverso, pero sus efectos se presentan en el mundo real), 3) externos-internos (delitos en el mundo real facilitados a través del metaverso) y 4) multifacéticos (delitos de doble contexto con evidencia en ambos ámbitos). Esta tipología enfatiza la naturaleza híbrida y difusa del metacrimen.

Por otro lado, una característica muy importante del metacrimen es el realismo de la victimización. Tiwari et al. (2025) argumentan que las cualidades inmersivas de los entornos de RV reducen la distancia psicológica entre la simulación y la realidad, ya que las víctimas internalizan el daño del avatar como daño personal. Por ejemplo, el acoso, el manoseo o la agresión en RV pueden desencadenar disociación, trastorno de estrés postraumático (TEPT) o ansiedad similar a la del trauma del mundo real. Además, los avatares actúan como gemelos digitales: prototipos mejorados biométricamente que imitan la postura corporal, la voz, las expresiones faciales y las señales fisiológicas. Esta continuidad encarnada hace que la victimización en el metaverso sea plausible y personal, lo que complica las distinciones legales entre avatar y usuario (Gehl, 2018; Tiwari et al., 2025).

Con base en lo anterior, la regulación del metacrimen se enfrenta a tres desafíos principales. El primer desafío es una falta de coherencia jurisdiccional, ya que ningún organismo soberano gobierna el metaverso. Tiwari et al. (2025) argumentan que esas lagunas jurisdiccionales permiten a los delincuentes operar con impunidad a través de las fronteras, por lo que estas empresas del metaverso se constituyen en jurisdicciones favorables, limitan el alcance de la persecución penal y complican la aplicación transnacional de la ley.

El segundo desafío son los derechos de propiedad intelectual poco claros, ya que la propiedad de los NFT, avatares y territorios digitales a menudo carece de una

definición legal sólida. Según Tiwari et al. (2025), los contratos inteligentes automatizan la transferencia de propiedad, pero no resuelven las disputas sobre el código fuente, los derechos de autor o la replicación no autorizada. Esto crea zonas grises legales en torno al robo de activos, la suplantación de marca y la falsificación.

El tercer desafío es la ambigüedad de la responsabilidad de los avatares: o sea, ¿quién es responsable cuando un avatar comete un delito? Tiwari et al. (2025) afirman que los avatares pueden servir como extensiones psicológicas de los usuarios, pero también son entidades legalmente distintas. Ello plantea interrogantes sobre la atribución de agencia y culpabilidad, especialmente en casos de los *deepfakes*, perfiles pirateados o avatares generados por IA.

Análisis comparativo e integración del ecosistema

Si bien el cibercrimen en redes sociales y el metacrimen difieren en la complejidad de sus plataformas, sus lógicas delictivas subyacentes muestran una superposición sustancial. Los puntos de convergencia son los siguientes:

1. El cibercrimen en las redes sociales y el metacrimen están tecnológicamente habilitados: Se basan en infraestructuras digitales (algoritmos de redes sociales o plataformas inmersivas) diseñadas principalmente para la conectividad y la monetización, y no para la seguridad del usuario ni el cumplimiento legal.
2. El cibercrimen en las redes sociales y el metacrimen son impulsados por el anonimato: Los delincuentes explotan las posibilidades de seudónimos de los nombres de usuario en redes sociales o avatares del metaverso para ofuscar la identidad, reducir la trazabilidad y ampliar el alcance operativo.
3. El cibercrimen en las redes sociales y el metacrimen son jurisdiccionalmente evasivos: Ambos tipos de ciberdelito dejan en evidencia la incapacidad de las geografías legales para regular espacios digitales sin fronteras. Un acosador que opera desde un país o un estafador que blanquea NFT de otro a menudo quedan atrapados en la nada (zona gris).
4. El cibercrimen en las redes sociales y el metacrimen buscan la explotación de datos: Ya sea mediante la recopilación de datos personales en Facebook o el rastreo de datos biométricos mediante trajes hápticos en el metaverso, estos ciberdelitos se basan en la asimetría informativa entre las arquitecturas de las plataformas y los usuarios (Roy & Tripathy, 2023; Tiwari et al., 2025).

Estas similitudes apuntan a una arquitectura criminógena compartida, que Álvarez y Rodríguez (2018) describen como las "condiciones del sustrato" de los ecosistemas criminales: ausencia de supervisión, densidad de oportunidades, incentivos de mercado y flujos de recursos que propician la conducta ilícita. Sin embargo, el metacrimen no es una extensión del cibercrimen, sino, por el contrario, una ruptura paradigmática, ya que es un salto criminológico hacia la desviación pospantalla, integrada espacialmente. Por eso, y a pesar de su solapamiento, el metacrimen puede entenderse como una frontera cualitativamente nueva. Los puntos de divergencia con relación con el cibercrimen en redes sociales son las siguientes:

1. Daño inmersivo: En redes sociales la victimización se basa en la pantalla y es principalmente textual o visual. En el metacrimen las víctimas experimentan sensaciones físicas y violaciones encarnadas a través de avatares, lo cual hace que el daño se acerque psicológicamente a la agresión física (Tiwari et al., 2025).
2. Ambigüedad ontológica: Los usuarios de las redes sociales son claramente humanos. En el metaverso los avatares pueden ser controlados por el usuario, operados por *bots* o generados por IA, lo que difumina las fronteras entre agencia y responsabilidad.
3. Complejidad de activos: Los delitos en las redes sociales rara vez involucran propiedad tokenizada. En contraste, el metacrimen gira en torno a tierras digitales, NFT y propiedad mediada por contratos inteligentes, lo que complica la restitución y la valoración.
4. Dispersión probatoria: El metacrimen puede abarcar plataformas y ámbitos (por ejemplo, un incidente de acoso en realidad virtual con evidencia en Discord y *blockchain*), lo que dificulta exponencialmente la reconstrucción forense (Tiwari et al., 2025).

En el contexto descrito, el modelo de ecosistema criminal es en especial relevante para sintetizar estos dominios. Por lo tanto, el modelo define los ecosistemas criminales como constelaciones dinámicas de (Álvarez & Rodríguez, 2018): 1) actores (individuos, grupos e intermediarios); 2) tecnologías (plataformas, cifrado, contratos inteligentes); 3) territorios (espacios virtuales o físicos de control o influencia); 4) flujos (de dinero, datos, poder, contenido), y 5) reglas (normas implícitas, códigos o estructuras formales).

Los delitos en redes sociales funcionan dentro de un ecosistema con alta densidad de actores, difusión algorítmica de contenido (flujo) y reglas formales débiles

(por ejemplo, ausencia de jurisprudencia robusta en la materia). Sus facilitadores incluyen el anonimato, la viralidad y la baja rendición de cuentas de la plataforma. El metacrimen, en cambio, opera en un ecosistema descentralizado que se caracteriza por territorios inmersivos (mundos de realidad virtual), flujos mediados por *blockchain* (criptomonedas, NFT), así como reglas ambiguas (por ejemplo, responsabilidades poco claras de los avatares). Sus facilitadores incluyen la presencia espacial, las posibilidades de los avatares y los contratos inteligentes. En ambos casos es válida la idea de Álvarez y Rodríguez (2018) de que la delincuencia prospera donde las instituciones formales se retiran o no se adaptan; al igual que en su análisis original de los ecosistemas criminales urbanos colombianos, los análogos digitales observados aquí muestran un repliegue institucional y una ilegalidad adaptativa.

Además, tanto el cibercrimen en las redes sociales como el metacrimen presentan zonas de convergencia horizontal, donde se interceptan distintas economías criminales. Por ejemplo, una campaña de *doxing* en X (un actor) puede extenderse al metaverso, donde el avatar de un usuario es el objetivo. Una estafa de NFT (delito basado en activos) puede financiar una campaña de acoso en Discord o Instagram. Un evento de acoso en VRChat puede dar pie a un chantaje en el mundo real a través de Telegram. Estos puntos de convergencia sugieren que la delincuencia digital del presente no debe analizarse de forma aislada, sino como sistemas ecológicos superpuestos que interactúan a través de flujos de capital, información y violencia simbólica. También es necesario señalar que los ecosistemas criminales son inherentemente adaptativos. Tal como lo señalan Álvarez y Rodríguez (2018), cuando se aplica presión a un nodo (por ejemplo, las fuerzas del orden interrumpen Silk Road) el sistema se regenera en otro (nuevos mercados, como Hydra o AlphaBay). La misma lógica se aplica ahora a plataformas descentralizadas que resisten la intervención estatal, generadores de avatares impulsados por IA que logran ocultar la identidad y sindicatos multiplataforma que integran redes sociales con realidad virtual y criptomonedas para generar sinergias operativas.

Por consiguiente, y de cara al futuro, la convergencia de la Web 3.0, la tecnología inmersiva y las finanzas descentralizadas (DeFi) parece sugerir una nueva generación de "ecologías híbridas" ciberdelictivas, marcadas por identidades estratificadas, la agencia de la IA y dilemas de gobernanza postterritorial. En este futuro el llamado de Álvarez y Rodríguez (2018) a mapear, intervenir e interrumpir las rutas de flujo de los ecosistemas criminales se convierte en un imperativo estratégico, no solo para los Estados, sino también para las instituciones multilaterales, las plataformas privadas y las coaliciones de la sociedad civil.

En resumen, el surgimiento del cibercrimen en redes sociales y del metacrimen reflejan una profunda transformación en la naturaleza, el alcance y la arquitectura de la delincuencia digital. No se trata simplemente de nuevos delitos en nuevas plataformas: representan la formación de nuevos entornos criminógenos, caracterizados por la presencia inmersiva, la gobernanza algorítmica, las finanzas descentralizadas y la convergencia del anonimato con una interacción de alto impacto. Este capítulo ha procurado demostrar cómo estas formas de ilegalidad digital interactúan con el diseño de plataformas, el comportamiento social, la ambigüedad legal y la complejidad tecnológica.

Sin embargo, para comprender plenamente las implicaciones de estos desarrollos, es necesario considerar el papel de la desviación digital como puente conceptual entre la violación de las normas en línea y la delincuencia estructurada. Como argumentan Graham y Smith (2024), la desviación digital incluye el troleo, la resistencia subcultural, el "acoso gamificado" y los actos performativos que difuminan la legalidad y la moralidad. Estos comportamientos funcionan como iniciadores culturales socializando a los actores en redes, lenguajes y lógicas que facilitan o, incluso, normalizan la entrada a los ecosistemas cibercriminales. La desviación digital no es periférica, sino fundamental. Constituye el sustrato a partir del que puede crecer el crimen organizado, y por lo tanto sirve como puerta de entrada cultural, técnica y social a estructuras criminales más formalizadas. La progresión desde la participación desviada en campañas de desinformación o suplantación de avatares hasta la plena participación en esquemas de *ransomware* o fraudes con NFT se ve facilitada por las porosas fronteras morales y la validación subcultural presentes en muchas comunidades en línea.

El cibercrimen en redes sociales y el metacrimen funcionan como subsistemas adaptativos dentro de un ecosistema criminal policéntrico más amplio, caracterizado por la autoorganización, la modularidad y los flujos transnacionales de datos, capital y daños. El énfasis de Álvarez y Rodríguez (2018) en los flujos, los nodos y los facilitadores ayuda para aclarar cómo las economías ilícitas se distribuyen entre plataformas, cómo los actores se especializan o coordinan, y cómo estos sistemas evolucionan bajo la presión de las fuerzas del orden o el escrutinio público. Para afrontar tan complejas realidades, las intervenciones políticas deben evolucionar más allá de la aplicación reactiva de la ley. Deben incluir:

1. Reforma de la gobernanza de las plataformas, con transparencia exigible, rendición de cuentas algorítmica y sólidos estándares de protección del usuario.

2. Innovación legal capaz de abordar los daños específicos del metaverso, incluyendo la responsabilidad por avatares, el consentimiento inmersivo y la regulación descentralizada de activos.
3. Programas de educación y alfabetización digital que desmitifiquen las prácticas desviadas en redes sociales y doten a los usuarios, especialmente a los jóvenes, de herramientas cruciales para gestionar el riesgo y resistir la normalización del daño en línea.
4. Cooperación transnacional en ciberseguridad, especialmente en el análisis forense, la criptorregulación y la investigación interjurisdiccional de delitos cometidos en mundos virtuales inmersivos.
5. Investigación sociotécnica que integre criminología, interacción humano-computador, psicología del comportamiento y antropología digital para adaptar continuamente los modelos de amenazas a la innovación de las plataformas.

En consecuencia, el estudio de las nuevas actividades de ciberdelincuencia en redes sociales y entornos metaversales debe basarse no solo en la tecnología o el derecho, sino también en la desviación cultural, la evolución del comportamiento y la teoría de sistemas. Solo vinculando la desviación digital con los ecosistemas criminales podremos empezar a comprender, y eventualmente desmantelar, las arquitecturas de daño que ahora están arraigadas en nuestros espacios digitales más avanzados.

Conclusiones

Este capítulo abordó la pregunta central: ¿Cómo operan y evolucionan las redes ciberdelictivas organizadas dentro de los ecosistemas de la *dark web*, y cuáles son las dinámicas estructurales, tecnológicas y criminológicas que sustentan estas economías ilícitas? Pues bien, a lo largo del presente análisis se logró el objetivo de identificar las estructuras, funciones y dinámicas operativas de la ciberdelincuencia organizada en la *dark web* articulando perspectivas criminológicas, sociotécnicas y estratégicas, para revelar la complejidad y resiliencia del ecosistema criminal digital.

En efecto, las redes ciberdelictivas organizadas no son entes aislados, sino subsistemas interdependientes que interactúan dentro de una arquitectura más amplia que integra anonimato, especialización funcional, mercados

descentralizados y lógica empresarial. Al igual que sus contrapartes en el mundo físico, estas redes aprovechan vacíos regulatorios, fallas de gobernanza tecnológica y subculturas digitales desviadas para sostener una cadena de valor delictiva transnacional, sostenida por criptomonedas, plataformas de anonimización y entornos digitales inmersivos.

La evolución de la ciberdelincuencia organizada en la era digital de la actualidad refleja la convergencia de las motivaciones delictivas tradicionales con las nuevas posibilidades tecnológicas. En efecto, la ciberdelincuencia ha pasado de ser solo *exploits* de *hacking* aislados a operaciones estructuradas y orientadas a servicios, integradas en los mercados ilícitos globales. Esta transformación se caracteriza por la profesionalización de los ciberdelincuentes, la proliferación de modelos de crimen como servicio (CaaS) y el uso estratégico de tecnologías de anonimización como las VPN, las criptomonedas y la red Tor.

No obstante, una perspectiva clave es la naturaleza cada vez más ecosistémica de la delincuencia digital, ya que las organizaciones ciberdelincuenciales no operan de forma aislada: por el contrario, forman parte de una red interconectada de servicios, intermediarios, plataformas y actores que facilitan todo, desde el diseño y la distribución de *malware* hasta el blanqueo de capitales ilícitos y la facilitación del mercado ilegal. Dentro de dicha estructura, la desviación digital cumple una función vital, aunque a menudo subestimada. Como argumentan Graham y Smith (2024), la desviación digital abarca una gama de prácticas subculturales, posturas ideológicas y comportamientos que traspasan los límites de la legalidad y la legitimidad. Estos incluyen el troleo, el *doxing*, la piratería y el vigilantismo digital. Prácticas que no siempre pueden clasificarse como delitos, pero, sin embargo, desafían las normas sociales y erosionan las fronteras entre la legalidad y la ilegalidad.

Es importante destacar que la desviación digital actúa como precursor cultural y conductual de formas más organizadas de ciberdelincuencia. Las comunidades desviadas normalizan la conducta transgresora en línea proporcionando bases de reclutamiento, justificaciones morales y habilidades técnicas que alimentan organizaciones delictivas más formalizadas. Además, la visibilidad y la proliferación de comportamientos desviados contribuyen a un ambiente cultural más amplio, donde la legalidad se vuelve negociable, la aplicación de la ley se dificulta y la ciberdelincuencia se camufla ideológicamente.

Por lo tanto, la ciberdelincuencia organizada no solo debe entenderse en términos técnicos o económicos, sino también como parte de un continuo socio digital más amplio, en el que la desviación, la subcultura y la innovación criminal

coevolucionan. Por ende, las futuras investigaciones y respuestas políticas al ciber-crimen deberían adoptar una perspectiva multidisciplinaria (integrando la criminología, la sociología, la ciberseguridad y los estudios culturales digitales), para comprender la arquitectura completa de las operaciones cibercriminales en el siglo XXI.

Este capítulo demuestra que tanto la ciberdelincuencia organizada en la *dark web* como los delitos emergentes en redes sociales y metaverso constituyen expresiones diferenciadas, pero convergentes, de un ecosistema criminal digital en evolución. Este ecosistema se caracteriza por su modularidad, descentralización y adaptabilidad, lo que dificulta el uso de marcos legales tradicionales y herramientas de seguridad unidimensionales. La desviación digital, además, emerge como un factor cultural y conductual clave: normaliza el comportamiento transgresor y facilita la transición hacia formas más estructuradas de criminalidad. Desde una perspectiva de los estudios en seguridad y defensa, y considerando la especificidad del entorno colombiano, se proponen las siguientes líneas de acción:

1. Fortalecer la inteligencia cibernética estructural. La ciberdelincuencia organizada del presente no puede enfrentarse solo con “ciberpatrullajes” o respuestas tácticas. Se requiere un modelo de inteligencia estratégica del ecosistema criminal digital, que identifique nodos, flujos, roles funcionales y convergencias entre mercados, plataformas y actores ilícitos.
2. Crear un Centro Nacional de Estudios Criminológicos Digitales. Colombia necesita un espacio interdisciplinario que articule criminología, ciberseguridad, sociología digital y ciencia de datos para comprender y anticipar la evolución del crimen en entornos virtuales. Este centro debe formar parte del Sistema Nacional de Inteligencia y Contrainteligencia.
3. Actualizar el marco jurídico penal y procesal para tipificar ciberdelitos asociados a: 1) la inmersión digital y los avatares (metacrímenes); 2) la participación en economías ilícitas digitales; 3) el desarrollo y comercialización de herramientas delictivas (*malware*, *exploits*), y 4) la complicidad algorítmica y negligencia de plataformas.
4. Impulsar un esquema robusto de cooperación interagencial y con el sector privado, articulando a: 1) Ministerio de Defensa y Policía Nacional (Dirección de Investigación Criminal e Interpol); 2) MinTIC y Ministerio de Justicia; 3) Superintendencia Financiera y la Unidad de Información y Análisis Financiero (UIAF) (por criptoactivos), y 4) Grupo de Respuestas a Emergencias Cibernéticas de Colombia (ColCERT) y sector académico en ciberseguridad.

5. Establecer mecanismos de gobernanza algorítmica, y además, exigir a plataformas que operan en Colombia: 1) protocolos de moderación más transparentes; 2) mecanismos rápidos de remoción de contenido criminal, y 3) colaboración con autoridades judiciales, sin invocar sistemáticamente el “puerto seguro” de la neutralidad tecnológica.
6. Diseñar una estrategia nacional de prevención de la desviación digital, con énfasis en: 1) alfabetización crítica para los jóvenes en las redes sociales y plataformas inmersivas; 2) intervenciones tempranas en las comunidades digitales de alto riesgo, y 3) visibilización de las consecuencias psicológicas del metacrimen y el acoso virtual.
7. Integrar el concepto de los ecosistemas criminales a la estrategia colombiana de ciberseguridad reconociendo que: 1) el ciberespacio debe ser concebido como un entorno operativo fluido y estratégico; 2) las intervenciones deben ser sistémicas, y no aisladas, y 3) las políticas deben orientarse a modificar las condiciones del entorno, y no solo a capturar individuos.

En suma, comprender la *dark web*, el metacrimen y el crimen en redes sociales desde una lógica de ecosistemas criminales digitales permite avanzar hacia un modelo de seguridad predictivo, adaptativo y multidimensional. Colombia, como potencia regional emergente en ciberseguridad, debe liderar en la región de América Latina la transición hacia un paradigma de gobernanza estratégica del ciberespacio, que combine tanto la soberanía tecnológica como la disuasión jurídica, la alfabetización cultural y la cooperación internacional inteligente.

Referencias

- Alexandrou, A. (2021). *Cybercrime and information technology: Theory and practice - The computer network infrastructure and computer security, cybersecurity laws, internet of things (IoT), and mobile devices*. CRC Press.
- Álvarez, C. (2017). Ocupación de los espacios vacíos: una condición sine qua non para la seguridad multidimensional en Colombia. En Álvarez, C. (ed.), *Escenarios y desafíos para la seguridad multidimensional en Colombia* (pp. 307-386). Sello Editorial ESDEG.
- Álvarez, C. y Zambrano, J. (2017). Globalización desviada: plataforma de convergencia criminal. En Álvarez, C. (Ed.), *Escenarios y desafíos para la seguridad multidimensional en Colombia* (pp. 249-306). Sello Editorial ESDEG.
- Álvarez, C. y Rodríguez, C. (2018). Criminal ecosystems: Habitats for convergence and deviant globalization. *Revista Científica General José María Córdova*, 16(24), 1-30.
- Akhgar, B.; Gercke, M.; Vrochidis, S. y Gibson, H. (Eds.). (2021). *Dark web investigation*. Springer.
- Annisson, T. (2022). *The Future of Financial Crime in the Metaverse: Fighting Crypto-Crime in Web 3.0*. Elliptic.
- Bandler, J. y Merzon, A. (2020). *Cybercrime investigations: A comprehensive resource for everyone*. CRC Press.
- Brenner, S. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. UPNE.
- Brewer, R.; de Vel-Palumbo, M.; Hutchings, A.; Holt, T.; Goldsmith, A. y Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. Palgrave Macmillan.
- Chaka, J. y Marimuthu, M. (2018). Curtailing the threats to cloud computing in the fourth industrial revolution. En Fields, Z. (Ed.), *Handbook of research on information and cyber security in the fourth industrial revolution* (pp. 112-141). IGI Global.
- Check Point Software Technologies (2025). *2025 Cyber Security Report: Understanding Cybercrime Trends and Threat Vectors in a Post-RaaS Era*. <https://www.checkpoint.com/downloads/cyber-security-report-2025.pdf>
- Choi, K.; Lee, C. y Louderback, E. (2020). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. En Holt, T. y Bossler, A. (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 27-43). Palgrave Macmillan.
- Clough, J. (2012). The council of Europe convention on cybercrime: Defining 'crime' in a digital world. *Criminal Law Forum*, 23, 363-391.
- Clough, J. (2015). *Principles of cybercrime (2nd ed.)*. Cambridge University Press.
- Daras, N. (Ed.). (2019). *Cyber-security and information warfare*. Nova Science Publishers.
- Donalds, C., Barclay, C. y Osei-Bryson, K. (2022). *Cybercrime and cybersecurity in the Global South: Concepts, strategies and frameworks for greater resilience*. CRC Press.
- East, C. (2017). Demystifying the Dark Web. *ITNOW*, 59(1), 16-17.
- Friedrichs, D. (2009). *Trusted criminals (4th ed.)*. Cengage.

- Gehl, R. W. (2018). *Weaving the Dark Web: Legitimacy on freenet, Tor, and I2P*. MIT Press.
- Gentry, J. y Gordon, J. (2019). *Strategic Warning Intelligence: History, Challenges, and Prospects*. Georgetown University Press.
- Grabo, C. (2010). *Handbook of Warning Intelligence: Assessing the Threat to National Security*. Scarecrow Press.
- Graham, R. y Smith, S. (2024). *Cybercrime and digital deviance (2nd ed.)*. Routledge.
- Hannigan, K. (2021). Vygotsky and Internet Grooming: The Darker Side of ZPD and Scaffolding. En Owen, T. y Marshall, J. (Eds.), *Rethinking Cybercrime: Critical Debates* (pp. 23-40). Palgrave Macmillan.
- Hayes, R. y Luther, K. (2018). *#Crime: Social Media, Crime, and the Criminal Legal System*. Palgrave Macmillan.
- Hollinger, R. y Lanza-Kaduce, L. (1988). The process of criminalization: The case of computer crime laws. *Criminology*, 26, 101-126.
- Holt, T.; Bossler, A. y Seigfried-Spellar, K. (2022). *Cybercrime and digital forensics: An introduction (3rd ed.)*. Routledge.
- INTERPOL (2024). *Metaverse a Law Enforcement Perspective: Use Cases, Crime, Forensics, Investigation, and Governance*. INTERPOL
- Jenkinson, A. (2022). *Ransomware and cybercrime*. CRC Press.
- Kardya, M. y Mitrou, L. (2007). *Internet forensics: Legal and technical issues. Second international workshop on digital forensics and incident analysis*. WDFIA.
- Kremling, J. y Sharp Parker, A. (2017). *Cyberspace, cybersecurity, and cybercrime*. SAGE Publications.
- Krone, T. (2005). *Concepts and terms: High Tech Crime Brief*. Australian Institute of Criminology.
- Kumari, K.; Singh, J. y Suman, S. (2023). Analysis and Detection of Cyberbullying in Reddit Discussions. En Roy, P. y Tripathy, A. (Eds.). *Cybercrime in Social Media: Theory and Solutions* (pp. 107-120). CRC Press.
- Lastowka, F. y Hunter, D. (2004). The laws of the virtual worlds. *California Law Review*, 92, 1-73.
- Lavorgna, A. (2020). Organized Crime and Cybercrime. En Holt, T. y Bossler, A. (Eds.). *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 117-134). Palgrave Macmillan.
- Leukfeldt, E.; Lavorgna, A. y Kleemans, E. (2017). Organised cybercrime or cybercrime that is organised? *European Journal of Criminology*, 14(1), 100-119.
- Liggett, R.; Lee, J.; Roddy, A. y Wallin, M. (2020). The Dark Web as a Platform for Crime: An Exploration of Illicit Drug, Firearm, CSAM, and Cybercrime Markets. En Holt, T. y Bossler, A. (Eds.). *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 91-116). Palgrave Macmillan.
- Luo, X. y Liao, Q. (2009). Ransomware: A new cyber hijacking threat to enterprises. En Gupta, J. y Sharma, S. (Eds.), *Handbook of research on information security and assurance* (pp. 1-6). IGI global.

- Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press.
- McGuire, M. (2012). *Organized crime in the digital age*. John Grieve Centre for Policing and Security and BAE Systems Detica.
- Mansfield-Devine, S. (2016). *Ransomware: Taking businesses hostage*. Network Security, 10, 8-17.
- Nearchou, N. (2023). *Combating crime on the dark web: Learn how to access the dark web safely and not fall victim to cybercrime*. Packt Publishing.
- Neto, J. (2017). Social Network Analysis and Organized Crime Investigation: Adequacy to Networks, Organized Cybercrime, Portuguese Framework. En Viano, E. (Ed.), *Cybercrime, organized crime, and societal responses: International approaches* (pp. 179-200). Springer.
- Noble, W.; Owen, T. y Speed, F. (2017). *New perspectives on cybercrime*. Palgrave Macmillan.
- Owen, T. (2021). CyberTerrorism: Some Insights from Owen's Genetic-Social Framework. En Owen, T. y Marshall, J. (Eds.), *Rethinking Cybercrime: Critical Debates* (pp. 3-22). Palgrave Macmillan.
- Ozkaya, E. e Islam, R. (2019). *Inside the dark web*. CRC Press.
- Parker, D. (1976). *Crime by computer*. Scribner.
- Payne, B. (2020). Defining Cybercrime. En Holt, T. y Bossler, A. (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 3-26). Palgrave Macmillan.
- Roy, P. y Choudhary, J. (2023). Emotions Detection from Social Media Text Using Machine Learning. (2023). En Roy, P. y Tripathy, A. (Eds.), *Cybercrime in Social Media: Theory and Solutions* (pp. 41-66). CRC Press.
- Roy, P. y Tripathy, A. (Eds.) (2023). *Cybercrime in Social Media: Theory and Solutions* (pp. 1-22). CRC Press.
- Sabell, E.; Manaf, A. e Ismail, Z. (2012). Development of Malaysian digital forensics investigator competency identification methods. En Hassanien, A.; Salem, A.; Ramadan, R. y Kim, T. (Eds.), *Advanced machine learning technologies and applications* (pp. 554-565). Springer.
- Salter, M. (2017). *Crime, Justice and Social Media*. Routledge.
- Schwab, K. (2016). *The fourth industrial revolution*. Crown Business.
- Seo, S.; Seok, B. y Lee, C. (2023). Digital Forensic Investigation Framework for the Metaverse. *The Journal of Supercomputing*, 79(14), 9467-9485.
- Singh, B.; Kumar, A.; Adhikari, D.; Pradhan, J.; Singh, D. y Mishra, D. (2023). Fundamental Theories Behind the Detection of Fake News and Rumors. En Roy, P. y Tripathy, A. (Eds.), *Cybercrime in Social Media: Theory and Solutions* (pp. 1-22). CRC Press.
- Smith, T. y Haines, K. (2023). A Doubled- Edged Sword Called Cyberspace: Introducing the Concept of Cybercrime. En Roy, P. y Tripathy, A. (Eds.), *Cybercrime in Social Media: Theory and Solutions* (pp. 121-142). CRC Press.

- Symanovich, S. (2019). *How to safely access the deep and dark webs*. Norton.
- Thurner, S.; Hanel, R. y Klimek, P. (2018). *Introduction to the Theory of Complex Systems*. Oxford University Press.
- Tiwari, M.; Zhou, Y.; Gilmour, P. y Bernot, A. (2025). Confronting metacrime: complexities, enforcement challenges and regulatory pathways. *Law, Innovation and Technology*, 17(1), 159-176.
- UNODC. (2004). *United Nations Convention against Transnational Organized Crime (Palermo Convention)*. Organización de las Naciones Unidas.
- UNODC. (2022). *Compendio de Ciberdelincuencia Organizada*. Organización de las Naciones Unidas. Organización de las Naciones Unidas.
- Viano, E. (2017). Cybercrime: Definition, Typology, and Criminalization. En Viano, E. (Ed.), *Cybercrime, organized crime, and societal responses: International approaches* (pp. 3-22). Springer.
- Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity.
- Wang, Z. (2012). *Method for providing terminals of IMS network firewall and firewall system*. U.S. Patent Application.
- Watters, P. (2024). *Cybercrime and cybersecurity*. Routledge.
- Willems, E. (2019). *Cyberdanger: Understanding and guarding against cybercrime*. Springer.
- Wirtz, J. (2017). *Understanding Intelligence Failure: Warning, response and deterrence*. Routledge.

Capítulo 4

El auge de la ciberguerra en guerras de quinta generación: estrategias, herramientas y amenazas*

DOI: <https://doi.org/10.25062/9786287818705.04>

Carlos Enrique Álvarez Calderón

Rafael Enrique Niño Zea

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo explora el impacto transformador de la ciberguerra en el marco de la Guerra de Quinta Generación (G5G), pero centrándose en sus implicaciones estratégicas, operativas y políticas para la seguridad nacional de Colombia. Examina cómo la ciberguerra difumina las fronteras entre objetivos militares y civiles, amplifica las vulnerabilidades sociales y redefine el campo de batalla. Al analizar las distinciones operativas y tecnológicas entre ciberguerra, ciberdelito y ciberterrorismo, el capítulo destaca cómo los actores estatales y no estatales explotan la asimetría, el anonimato y la manipulación psicológica para lograr objetivos estratégicos ubicados por debajo del umbral de la guerra convencional. El capítulo concluye con recomendaciones estratégicas para las fuerzas militares colombianas, y abogando por la creación de un comando cibernético unificado, capacidades de inteligencia mejoradas, colaboración público-privada y alianzas regionales. Finalmente, subraya la necesidad de que Colombia integre la ciberdefensa como un pilar de su propia estrategia de seguridad nacional.

Palabras clave: ciberespacio; ciberguerra; defensa nacional; guerras de quinta generación; seguridad nacional.

* 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" y del proyecto de investigación "El pensamiento multidominio en el campo de batalla del futuro", ambos 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

Rafael Enrique Niño Zea

Oficial de Comunicaciones del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Contratación Estatal, Universidad de la Sabana, Colombia. Especialista en Gerencia Integral de las Telecomunicaciones y Administrador de Empresas en Telecomunicaciones, Escuela de Comunicaciones Militares.

<https://orcid.org/0009-0003-7814-9876> - Contacto: rafaelnin@cgfm.mil.co

Citación APA: Álvarez Calderón, C. E. & Niño Zea, R. E. (2026). El auge de la ciberguerra en guerras de quinta generación: estrategias, herramientas y amenazas. 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. 237-316). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818705.04>

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

En el cambiante entorno estratégico del siglo XXI, el ciberespacio se ha convertido en un ámbito crítico de competencia transformando el carácter y la conducción de los conflictos modernos. La ciberguerra, en el marco de las Guerras de Quinta Generación (G5G), desafía las nociones tradicionales de la guerra, al fusionar las innovaciones tecnológicas con las operaciones políticas, económicas y cognitivas. A diferencia de las guerras convencionales, las G5G se caracterizan por su carácter difuso, no lineal y multidimensional, donde las fronteras entre paz y guerra, civil y combatiente, físico y virtual se difuminan hasta hacerse irreconocibles.

En efecto, la G5G representa una de las últimas etapas en la evolución moderna de los conflictos, siguiendo los modelos previos de guerra de primera a cuarta generación (Álvarez et al., 2017). Mientras que las generaciones anteriores se centraban en la concentración de efectivos militares, la mecanización, la maniobra y la insurgencia descentralizada, la G5G se define por su énfasis en los dominios cognitivo, informativo y no cinético, donde el objetivo principal es influir en las percepciones, erosionar la voluntad y lograr objetivos estratégicos sin una confrontación militar convencional. De acuerdo con Álvarez et al. (2017), las G5G se caracterizan por actores difusos, adaptativos e interconectados (tanto estatales como no estatales), que operan en las dimensiones política, económica, social, cultural y tecnológica, a menudo sin declaraciones formales de guerra ni frentes identificables¹.

¹ En la literatura estratégica existe un debate sostenido sobre el uso del lenguaje de “generaciones de guerra”. Diversos autores advierten que estas tipologías, aunque útiles como heurísticas pedagógicas para describir cambios en el carácter del conflicto, pueden inducir lecturas teleológicas (como si la guerra evolucionara en “etapas” lineales), sobre generalizar fenómenos heterogéneos y oscurecer incluso continuidades históricas fundamentales (Gray, 2005; Freedman, 2013). En particular, se ha cuestionado que el marco generacional tiende a reetiquetar transformaciones doctrinales y tecnológicas sin resolver problemas conceptuales de fondo (por ejemplo, qué cambia realmente: el carácter, los medios, las formas de empleo o la naturaleza política

Una de las características que definen la G5G es su dependencia de la asimetría, la ambigüedad y la multidimensionalidad, lo cual incluye el uso de la manipulación mediática, la desinformación, ciberataques, guerra legal, coerción económica y otras herramientas no tradicionales, para desestabilizar o coaccionar a los adversarios manteniéndose por debajo del umbral de la acción militar abierta. A diferencia de la guerra de cuarta generación, centrada en la insurgencia y las tácticas de guerrilla, la G5G opera principalmente en el ámbito cognitivo, con el objetivo de “hackear” la confianza social, la cohesión política y la estabilidad económica.

Whyte y Mazanec (2023) destacan que la integración de la ciberguerra en la G5G es particularmente transformadora, pues el ciberespacio permite a los actores atacar las redes adversarias, interrumpir infraestructuras críticas, manipular los flujos de información e influir en la opinión pública a una escala y una velocidad previamente inimaginables. Una característica fundamental de la G5G es la difuminación de las distinciones entre guerra y paz, civil y combatiente, y los ámbitos nacional e internacional. Como señala Caruso (2024), todo ello conduce a una forma de “conflicto enredado”, donde las operaciones cibernéticas, la guerra cognitiva y las acciones cinéticas se interceptan de forma impredecible, y producen a menudo efectos que trascienden las fronteras nacionales y afectan a sociedades enteras.

En el contexto colombiano, el modelo de G5G es en particular relevante, dada la exposición del Estado colombiano a amenazas multidimensionales como las redes de narcotráfico, los grupos insurgentes armados, las tensiones geopolíticas regionales y los actores cibernéticos transnacionales. Dichos actores recurren cada vez más a estrategias de G5G, utilizando herramientas tanto cibernéticas como cognitivas para desafiar la autoridad estatal, perturbar la gobernanza y explotar las vulnerabilidades sociales. En ese orden de ideas, y según Whyte y Mazanec (2023), la ciberguerra opera en la intersección de los ámbitos político, militar y tecnológico, por lo que involucra ataques a redes informáticas y explotación y defensa en entornos internacionales complejos. Se trata de un desafío no solo técnico, sino también estratégico, que transforma el cálculo de la seguridad nacional y la proyección de poder. Como señala Caruso (2024), el ciberespacio contemporáneo ya no se limita a la recopilación de inteligencia o al robo digital:

de la guerra), y puede convertirse en un “contenedor” que absorbe dinámicas distintas bajo un mismo rótulo (Echevarría, 2005). En este capítulo se utiliza el término G5G en un sentido operacional y descriptivo, para referirse a entornos de conflicto caracterizados por hibridación, zona gris, centralidad informacional/cognitiva y empleo intensivo del ciberespacio; el examen crítico y comparado del debate tipológico se desarrolla con mayor amplitud en el Volumen II.

puede generar efectos cinéticos reales, perturbar infraestructuras críticas e influir decisivamente en los resultados de campañas políticas y militares.

Cabe señalar que el concepto de ciberguerra ha sido moldeado por múltiples perspectivas académicas, militares y políticas a lo largo de las últimas dos décadas. Una de las definiciones más influyentes, ofrecida por Clarke y Knake (2010), describe la ciberguerra como "las acciones de un Estado-nación para penetrar en los computadores o redes de otra nación con el fin de causar daños o perturbaciones" (p. 6). Según Whyte y Mazanec (2023), la ciberguerra se refiere al uso de ataques a redes informáticas, explotación de redes informáticas y defensa de redes informáticas como instrumentos de conflicto entre Estados o entre Estados y actores no estatales, llevados a cabo en un contexto estratégico y geopolítico más amplio. Eso implica operaciones destinadas a lograr objetivos políticos, militares o estratégicos mediante la manipulación, interrupción o destrucción de los sistemas de información del adversario.

De manera similar, Arquilla y Ronfeldt (2001) conceptualizan la ciberguerra como el uso organizado de las tecnologías de la información y la comunicación (TIC) para perturbar o inhabilitar las capacidades militares y las funciones sociales del oponente, lo cual la caracteriza como salto evolutivo en la forma de conducir la guerra en la era de la información. Caruso (2024) amplía esta definición enfatizando que la ciberguerra incluye no solo el espionaje digital, sino también operaciones con efectos cinéticos tangibles, como la desactivación de infraestructuras críticas como las redes eléctricas o los sistemas de transporte.

Sin embargo, el panorama de definiciones al respecto sigue dividido. Ashraf (2021) identifica tres amplios grupos intelectuales que han moldeado el debate sobre la conceptualización de la "ciberguerra": las escuelas alarmista, escéptica y realista. Esta diversidad de marcos interpretativos representados en las escuelas resalta la flexibilidad conceptual necesaria para dar cuenta de la evolución de los comportamientos, acciones y efectos estatales y no estatales en el ciberespacio, y explica por qué ha sido tan difícil alcanzar un consenso respecto a la definición y los límites de la ciberguerra, y por qué las respuestas políticas, militares y legales suelen divergir.

De acuerdo con Ashraf (2021), la escuela alarmista considera la ciberguerra una amenaza inminente y potencialmente catastrófica para la seguridad nacional e internacional. Los alarmistas enfatizan la vulnerabilidad de las infraestructuras críticas (como las redes eléctricas, los sistemas de transporte, las redes financieras y los sistemas militares de mando y control) a ciberataques capaces de causar

destrucción cinética y física o parálisis social. Quienes defienden esta perspectiva argumentan que la ciberguerra representa una transformación fundamental de la guerra, comparable a la introducción de armas nucleares o municiones guiadas de precisión, pues permite a los adversarios atacar el corazón de las interconectadas sociedades modernas, sin necesidad de cruzar las fronteras geográficas ni desplegar tropas en el terreno. Los alarmistas suelen destacar escenarios de un “ciber Pearl Harbor” o un “ciber 11-S”, y advertir que los Estados no se encuentran listos para las consecuencias en cascada de los ciberataques a gran escala. Clarke y Knake (2010) son citados a menudo como representantes de dicho grupo, pues argumentan que la ciberguerra no solo es real, sino que ya está en marcha, y que las democracias, en particular, se hallan peligrosamente expuestas a ella.

En contraste, la escuela escéptica cuestiona si la ciberguerra puede tan siquiera considerarse “guerra” en el sentido tradicional de Clausewitz. Los escépticos argumentan que, si bien el ciberespacio es un ámbito de intensa competencia, las operaciones llevadas a cabo en este (como el espionaje, el robo, el vandalismo y el sabotaje) no alcanzan el umbral de conflicto armado, tal como lo define el derecho internacional (Ashraf, 2021). Para los escépticos, la mayoría de las operaciones cibernéticas se clasifican mejor como actividades de inteligencia o delictivas, y no como actos de guerra. Señalan que, a pesar de décadas de advertencias, ningún ciberataque ha causado todavía un gran número de víctimas, ni derrocado un gobierno ni provocado una declaración formal de guerra. Los escépticos critican sobre todo los escenarios exagerados o los peores escenarios argumentando que fomentan la reacción exagerada, la militarización del ciberespacio y la erosión de las libertades civiles. Thomas Rid (2013) es una de las voces principales de la corriente escéptica. Se ha hecho famosa su afirmación de que “la ciberguerra no ocurrirá”, pues las operaciones cibernéticas hasta ahora han tenido un alcance y una eficacia limitados.

Por su parte, la escuela realista busca un pragmático punto intermedio. En efecto, los realistas aceptan que las operaciones cibernéticas están transformando la seguridad internacional, pero insisten en que la ciberguerra debe analizarse y regularse dentro de las estructuras existentes del derecho internacional y la teoría estratégica (Ashraf, 2021). Para los realistas, la ciberguerra se entiende mejor como una extensión de las dinámicas clásicas de conflicto (incluyendo la disuasión, la coerción, la escalada y la política de alianzas) al ámbito cibernético. Destacan que las categorías jurídicas de *jus ad bellum* (derecho a la guerra) y *jus in bello* (conducta en la guerra), junto con instrumentos como la Carta de las Naciones Unidas, las Convenciones de Ginebra y marcos como el Manual de Tallin, son aplicables a

las operaciones cibernéticas, incluso si requieren adaptación. Por tanto, los realistas abogan por un enfoque mesurado: fortalecer las defensas nacionales, mejorar la resiliencia, desarrollar posturas de disuasión creíbles y promover las normas internacionales, sin caer en el pánico ni en la indiferencia. Autores como Valeriano y Maness (2012) encajan en esta escuela, al centrarse en el análisis empírico de los incidentes cibernéticos y su uso restringido en el arte de gobernar.

Ante las definiciones divergentes, y a menudo controvertidas, de "ciberguerra" que se encuentran en la literatura académica y política, es necesario establecer una definición práctica para los fines del presente capítulo. Como ya se señaló, los académicos han debatido si la ciberguerra constituye una transformación sin precedentes del conflicto (Clarke & Knake, 2010; Arquilla & Ronfeldt, 1993), si debe considerarse con mayor cautela dentro de los límites de los marcos legales y estratégicos existentes (Ashraf, 2021) o si sus efectos son exagerados, en comparación con las formas convencionales de guerra (Rid, 2013). Esta pluralidad de definiciones refleja la complejidad del fenómeno, que abarca los ámbitos técnico, militar, político y social.

Por ende, y a efectos de este capítulo, sus autores definen la "ciberguerra" como el uso deliberado de ataques a redes informáticas, explotación de redes informáticas y defensa de redes informáticas por parte de actores estatales o patrocinados por ellos, diseñados para lograr objetivos políticos, militares o estratégicos mediante la disrupción, degradación o destrucción de la infraestructura digital, informativa y física del adversario. Opera dentro del umbral de un conflicto armado convencional, y a menudo por debajo de él, difuminando las fronteras entre la guerra y la paz, lo civil y lo militar y lo nacional y lo internacional.

Esta definición se basa en una comprensión realista de la ciberguerra situándola en el continuo de conflictos históricos, al tiempo que reconoce sus características novedosas: anonimato, negación plausible, asimetría y capacidad para moldear el orden global sin el uso visible de la fuerza. En definitiva, la ciberguerra representa la evolución del conflicto hacia la era de la información, donde el dominio de los datos, las redes y los dominios cognitivos se vuelve tan decisivo como el control del territorio o la potencia de fuego. Esta base conceptual guiará el análisis desarrollado a lo largo del capítulo.

Asimismo, es fundamental distinguir la "ciberguerra" de fenómenos relacionados como "ciberterrorismo" y "ciberdelito", ya que difieren en aspectos clave. Por ejemplo, el ciberterrorismo implica el uso o la amenaza de ciberataques por parte de actores no estatales, generalmente motivados por objetivos ideológicos, religiosos o políticos, para infundir miedo, coaccionar a gobiernos o influir en la opinión pública (Whyte & Mazanec, 2023). Por ende, a diferencia de la ciberguerra,

la cual suele involucrar a actores estatales que persiguen objetivos estratégicos, el ciberterrorismo suele atacar a la población civil, infraestructuras críticas o activos simbólicos con el objetivo principal de generar disrupción psicológica en vez de obtener una real ventaja militar. En contraste, el cibercrimen abarca actividades con fines de lucro, como el fraude financiero, el robo de identidad, las campañas de *ransomware* y las filtraciones de datos, a menudo llevadas a cabo por individuos o grupos delictivos organizados (Mehan, 2008). Si bien el cibercrimen a veces puede solaparse con la seguridad nacional (por ejemplo, cuando los Estados toleran o colaboran con los ciberdelincuentes para obtener ventajas políticas), su principal motivación sigue siendo el lucro económico (Whyte y Mazanec, 2023).

Comprender estas distinciones es clave, especialmente para Estados como Colombia, donde los desafíos de seguridad multidimensional exigen enfoques hechos a la medida de cada una de las amenazas existentes. Como lo señalan Álvarez et. al (2017), Colombia enfrenta amenazas híbridas que incluyen operaciones cibernéticas patrocinadas por el Estado, campañas ciberterroristas de actores no estatales y redes criminales impulsadas por el ciberespacio, cada una de las cuales requiere respuestas políticas, legales y de defensa específicas.

Con base en lo anterior, y dada la creciente importancia de la ciberguerra dentro del panorama más amplio de los conflictos de G5G, este capítulo es guiado por la pregunta central de investigación: ¿Cómo ha transformado la ciberguerra la dinámica estratégica, operativa y política de las G5G, y qué implicaciones tiene esta transformación para la postura de seguridad nacional de Colombia? Para explorar en busca de respuestas, el análisis abordará tres preguntas secundarias: 1) ¿Cuáles son las características operativas y tecnológicas que definen la ciberguerra del cibercrimen y el ciberterrorismo? 2) ¿Cómo explotan los actores estatales y no estatales la asimetría, el anonimato y los efectos psicológicos de la ciberguerra para lograr objetivos políticos y estratégicos por debajo del umbral de la guerra convencional? Y 3) ¿Qué vulnerabilidades específicas y brechas institucionales dentro de la arquitectura de ciberseguridad de Colombia aumentan su exposición a las amenazas de la ciberguerra?

Al abordar estas preguntas, el capítulo trabaja con tres hipótesis clave: que la integración de la ciberguerra ha desdibujado los límites entre los objetivos militares y civiles, y aumentado, en cambio, la vulnerabilidad social; que los países con capacidades limitadas de ciberdefensa, como Colombia, enfrentan riesgos estratégicos desproporcionados por parte de actores asimétricos, y que la ausencia de marcos jurídicos internacionales sólidos que regulen las operaciones cibernéticas fomenta la escalada y la normalización de las prácticas de ciberguerra.

En conjunto, estas preguntas e hipótesis proporcionan la base conceptual para un análisis multidimensional que integra tendencias globales, características técnicas e implicaciones a nivel nacional. Por consiguiente, el propósito de este capítulo es doble: en primer lugar, hacer un análisis exhaustivo de la naturaleza, las herramientas, los actores y las doctrinas de la ciberguerra en la era de la G5G. En segundo lugar, evaluar las implicaciones para la seguridad nacional y el pensamiento estratégico de Colombia. Basándose en estudios de caso globales, doctrinas comparativas y perspectivas técnicas, el capítulo ofrece una base teórica y recomendaciones prácticas.

En la primera sección del capítulo se examinan la naturaleza y las características de la ciberguerra, incluyendo la asimetría, el anonimato y su integración en operaciones híbridas y de zona gris. El análisis se centra en las armas y tácticas cibernéticas abordando herramientas clave como *malware*, *ransomware*, ataques DDoS, APT y la Cyber Kill Chain. A continuación, se presenta una visión global que analiza las estrategias de importantes actores estatales, como Rusia, China, Corea del Norte e Irán. Para fundamentar esas ideas en la práctica, el capítulo presenta casos de estudio emblemáticos, como Stuxnet o las campañas cibernéticas de Ucrania. Posteriormente, se aborda el contexto colombiano evaluando el panorama de ciberseguridad del país, sus marcos institucionales y las amenazas regionales.

El capítulo aborda, además, los desafíos legales, éticos y estratégicos del caso analizando el derecho internacional, los dilemas de atribución y la ética de las operaciones ofensivas. De cara al futuro, explora las tendencias futuras, y en particular, el impacto de la inteligencia artificial (IA), la computación cuántica y las vulnerabilidades del Internet de las Cosas (IoT). Finalmente, el capítulo concluye sintetizando los hallazgos clave y buscando ofrecer recomendaciones estratégicas para el Estado colombiano. Se aspira a que al finalizar el capítulo el lector haya obtenido una comprensión integral de la importancia estratégica de la ciberguerra en el marco de la G5G, así como los pasos que Colombia debe considerar para afrontar este entorno de amenazas, cada vez más complejo.

Naturaleza y características de la ciberguerra

La ciberguerra se ha vuelto un rasgo distintivo de los conflictos del siglo XXI, en especial dentro del paradigma de la G5G. En esta forma de la guerra, caracterizada por amenazas híbridas, ambigüedad y difuminación entre paz y conflicto, las ciberoperaciones ejemplifican muchas de las dinámicas centrales de la era del siglo

XXI. A diferencia de las batallas convencionales, restringidas al ámbito físico, la ciberguerra se desarrolla en el ámbito digital, donde actores tanto estatales como no estatales pueden enfrentarse a sus adversarios a la velocidad de la luz y, a menudo, por debajo del umbral de un ataque armado tradicional (Clark & Knake, 2010).

La Ventaja asimétrica en el ciberespacio

Una de las características más destacadas de la ciberguerra es su asimetría: la forma como empodera a actores más pequeños o con menos recursos, para desafiar incluso a los Estados más poderosos. En el ciberespacio la ofensiva suele tener ventaja, y un puñado de hábiles individuos o un Estado más débil pueden infligir un daño desproporcionado a los intereses de una gran potencia. Clarke y Knake (2010) definieron la ciberguerra como acciones de un Estado nación para penetrar en los computadores o redes de otro Estado a fin de causar daños o interrupciones. Advirtieron también que los ciberataques podrían devastar infraestructuras críticas “a la velocidad de la luz”, lo que representa una amenaza en especial grave para Estados altamente interconectados, como Estados Unidos. En su opinión, la ciberguerra no era un escenario futuro, sino una realidad en desarrollo, una en la que incluso Estados como Corea del Norte o Irán (con un poderío convencional limitado) podrían desarrollar capacidades cibernéticas capaces de causar daños similares a los causados por los japoneses en Pearl Harbor, en 1941, a un adversario más avanzado.

Por consiguiente, la naturaleza asimétrica de la ciberguerra representa una de sus implicaciones estratégicas más profundas en el contexto del conflicto contemporáneo. La teoría clásica del conflicto asimétrico, descrita por académicos como Andrew Mack (1975) e Ivan Arreguín-Toft (2001), enfatiza que los actores más débiles pueden prevalecer contra adversarios materialmente superiores explotando las vulnerabilidades de su oponente, manteniendo una resistencia prolongada y aprovechando los costos políticos, sociales o económicos de la escalada. En el ciberespacio, estas dinámicas se amplifican: la ofensiva a menudo ostenta una ventaja estructural, y los actores pequeños y con recursos limitados pueden causar una disrupción desproporcionada en los Estados tecnológicamente avanzados (Clarke & Knake, 2010; Oakley, 2019).

Como argumentó Mack (1975), la asimetría surge no solo de las diferencias en capacidades materiales, sino también de las diferencias en la voluntad política, la adaptabilidad y la capacidad para imponer costos. En el ámbito cibernético, el bajo costo de entrada, el alcance global y la iniciativa del atacante magnifican esa

asimetría y permiten que Estados más débiles y los actores no estatales desafíen la hegemonía militar y económica de las grandes potencias sin enfrentarlas en una batalla convencional (Sanger, 2018; Oakley, 2019). Por ejemplo, el ataque de Corea del Norte a Sony Pictures en 2014 ilustró cómo un régimen aislado del sistema internacional podía lograr coerción económica a un adversario mediante el empleo de medios cibernéticos a un mínimo costo (Sanger, 2018). En efecto, la ubicuidad de vulnerabilidades cibernéticas, en combinación con el anonimato que ofrece el dominio ciberespacial, permite a diversos actores explotar la iniciativa estratégica (la capacidad para elegir el momento, el lugar y el modo de ataque), que Arreguín-Toft (2001) identifica como una fuente clave de ventaja asimétrica. Por lo tanto, la ciberguerra no solo democratiza el poder ofensivo, sino que también desafía en lo fundamental los supuestos de las jerarquías de seguridad en las relaciones internacionales, lo que obliga a las grandes potencias a enfrentar un complejo panorama operativo donde el dominio material no ofrece ni garantiza protección (Clarke & Knake, 2010; Oakley, 2019; Mack, 1975; Arreguín-Toft, 2001).

Varios factores subyacen al potencial asimétrico de la ciberguerra. En primer lugar, la baja barrera de entrada al dominio ciberespacial es decisiva: el acceso a equipos informáticos y vulnerabilidades de *software* es mucho más económico que adquirir armas tradicionales. El ex subsecretario de Defensa estadounidense, William J. Lynn III, observó que un rival no necesita bombarderos furtivos ni portaaviones para amenazar al ejército de una superpotencia: "Una docena de programadores informáticos decididos pueden, si encuentran una vulnerabilidad que explotar, amenazar la red logística global de Estados Unidos, robar sus planes operativos, cegar sus capacidades de inteligencia o dificultar su capacidad para lanzar armas contra objetivos" (Lynn III, 2010, pp. 98-99).

En otras palabras, un equipo con conocimientos tecnológicos puede amenazar sistemas militares críticos con unas pocas líneas de código malicioso. Esta diferencia de costes anula algunas ventajas de los ejércitos más poderosos, ya que un arsenal convencional multimillonario ofrece poca protección si los adversarios pueden paralizar las redes o la infraestructura de mando y control mediante ciberataques que cuestan solo una fracción de esa suma. De hecho, en un conflicto cibernético, el defensor a menudo debe invertir mucho más en seguridad y redundancia que el atacante en el desarrollo de la herramienta ofensiva. En tal sentido, los estudios comparan la ciberagresión con la insurgencia o la guerra de guerrillas. Es decir, el insurgente (atacante) puede atacar en cualquier lugar y a bajo costo, mientras que el contrainsurgente (defensor) debe protegerlo todo a un alto costo (Aucsmith, 2018).

Otro aspecto de la asimetría es el alcance global. Esto, debido a que el ciberespacio no es limitado por la geografía, pues un actor puede proyectar poder a través de las redes desde prácticamente cualquier ubicación en el mundo. Eso significa que actores relativamente menores pueden lograr efectos que antes solo eran posibles para aquellos con fuerzas militares expedicionarias. Como argumenta Aucsmith (2018), los “actores relativamente menores pueden luchar dentro del ciberespacio y tener alcance global. La guerra irregular en el ciberespacio puede anular la riqueza y la ventaja tecnológica de los Estados occidentales” (p. 350). En la práctica, un grupo de *hackers* talentosos en un país menos desarrollado pueden infiltrarse en sistemas de otro continente, e interrumpir servicios públicos o robar secretos de Estado sin siquiera salir de su propia base. Esta ubicuidad de objetivos y el anonimato del acceso amplifican la amenaza asimétrica: los sistemas críticos gubernamentales y civiles en Estados avanzados presentan una amplia superficie de ataque que adversarios decididos provenientes de Estados más débiles (o grupos no estatales) pueden explotar a distancia.

La asimetría en el ciberespacio también se deriva de la iniciativa que reside en el atacante. El atacante puede elegir el momento, el método y el objetivo del ataque, a menudo disfrutando de una casi total libertad de movimiento, mientras que el defensor se ve en la obligación de monitorear y proteger los objetivos potenciales en todo momento. Esta dinámica refleja la ventaja de la sorpresa del insurgente; los ciberatacantes pueden lanzar una ráfaga de pequeños ataques continuos, en vez de un golpe decisivo, y que, acumulativamente, erosionan los recursos y la voluntad de un oponente más fuerte; como lo expresó Galula (2006), “El insurgente ataca repentinamente, socava la fuerza del enemigo, logra la sorpresa, se desvincula, se retira, se dispersa y vuelve a atacar” (p. xii). Con el tiempo este acoso persistente mediante repetidas filtraciones de datos, ataques DDoS o incidentes de *ransomware*, y puede imponer costos significativos a una potencia superior, hasta obligarla a invertir enormes esfuerzos en defensa y respuesta a incidentes.

La existencia de actores no estatales agrava aún más el panorama asimétrico, ya que, si bien las fuerzas armadas estatales dominan en la guerra convencional, en el ciberespacio los Estados no son los únicos actores en los conflictos cibernéticos. Es innegable que individuos, colectivos hacktivistas o grupos criminales pueden llevar a cabo ciber operaciones de forma independiente con efectos estratégicos. Por ejemplo, el grupo de *hackers* Anonymous ha atacado sitios web gubernamentales y corporativos para promover causas políticas, y bandas de *ransomware* con motivaciones económicas han saboteado hospitales

y oleoductos. Dichos actores operan al margen de las estructuras de poder tradicionales, pero sus acciones pueden influir en la seguridad nacional de los Estados. La difusión de las capacidades cibernéticas implica que una gran potencia podría acabar defendiéndose no solo de Estados antagónicos, sino también de grupos improvisados o ciudadanos particulares que utilizan técnicas asimétricas.

En resumen, el carácter asimétrico de la ciberguerra permite a los actores más débiles desafiar a las potencias más fuertes de formas sin precedentes. Las herramientas ofensivas de bajo coste, el alcance global, la iniciativa del atacante y la participación de agentes o aliados no estatales influyen en la balanza. A medida que el entorno de la G5G difumina los roles de los combatientes, un insurgente o un Estado menor con poder tecnológico puede poner en riesgo los activos de un enemigo mucho más poderoso sin enfrentarse a él en un campo de batalla tradicional. Esta democratización de la capacidad ofensiva en el entorno ciberespacial obliga a los Estados dominantes a replantearse la seguridad: ya no pueden asumir que un poder económico o militar superior los protegerá del daño en el ciberespacio. Como se explorará en secciones posteriores, esta asimetría impulsa muchos de los cálculos estratégicos en ciberdefensa, disuasión y normas internacionales.

Anonimato y negación plausible: el desafío de la atribución en el ciberespacio

Una lógica operativa definitoria de la ciberguerra es el anonimato que ofrece a los atacantes. A diferencia de un ataque convencional con misiles o un movimiento de tropas, una ciberintrusión puede ser difícil de rastrear hasta su origen, y ello permite a los perpetradores ocultar su identidad. Esto genera una negación plausible: es decir, los atacantes pueden negar su participación o culpar a otros explotando la incertidumbre inherente a la atribución en el ciberespacio. En el contexto de la G5G y de los conflictos híbridos esta ambigüedad es una característica, y no un defecto: permite que la agresión ocurra en la "zona gris", por debajo del umbral de la guerra abierta, mientras las víctimas tienen dificultades para atribuir con total seguridad y confianza los ataques a un actor específico (Poznansky, 2022).

La arquitectura técnica de internet y las tácticas de los operadores cibernéticos dificultan notablemente la atribución. Esto, en razón de que los ataques digitales pueden dirigirse a través de numerosos países empleando computadores secuestrados (*botnets*) propiedad de civiles involuntarios o utilizando herramientas de *malware* compartidas en foros clandestinos. Como resultado, determinar el origen, la identidad y la intención de un atacante en el ciberespacio es en extremo

difícil (Whyte & Mazanec, 2023). Los atacantes en el ciberespacio suelen enmascarar su ubicación rebotando señales a través de redes anónimas y sistemas comprometidos en todo el mundo, y pueden dejar en el código pistas engañosas, o “falsas banderas”, para desviar las sospechas hacia otra parte. Incluso cuando los analistas forenses rastrean una intrusión a un servidor o dirección IP en particular, eso por sí solo no indica necesariamente quién fue el atacante o si actuó con apoyo estatal (Poznansky, 2022). En consecuencia, un alto grado de incertidumbre suele envolver los incidentes cibernéticos.

Este problema de atribución no es solo teórico, pues se ha presentado en numerosos casos reales. De acuerdo con (Poznansky, 2022), cuando los sitios web del Gobierno de Estonia se vieron colapsados por una masiva ciberdisrupción en 2007, muchos señalaron a Rusia (indignada esta última por la retirada de un monumento de guerra soviético). De igual forma, ciberataques afectaron a Georgia durante su guerra de 2008 con Rusia, y partes de la infraestructura de Ucrania sufrieron cibersabotaje en 2013. En cada uno de los casos se sospechó del papel de Moscú, pero faltaban pruebas directas que vincularan los ataques con el Kremlin. Como era de esperarse, las autoridades rusas negaron su responsabilidad y la naturaleza descentralizada de los ciberataques (que involucraron a *hackers* patriotas y *botnets* criminales), dificultó la prueba concluyente de la orquestación estatal.

Esta negación plausible protegió a Rusia de represalias o de la condena de la Organización de las Naciones Unidas (ONU). Después de todo, sin una atribución firme, los incidentes no alcanzaban el umbral de un claro acto de guerra (Whyte & Mazanec, 2023). La incertidumbre y el carácter “inatribuible” de estas operaciones ejemplifican cómo el anonimato sirve de facilitador estratégico de la agresión en el ciberespacio. Poznansky (2022) diferencia, además, dos modelos de negación plausible: el modelo estatal, donde la negación protege al Gobierno en general para evitar una escalada o consecuencias legales, y el modelo ejecutivo, donde protege a los altos líderes a nivel nacional. Ambos modelos explotan la opacidad del ciberespacio, pero reflejan distintos cálculos y riesgos políticos.

Para los adversarios, operar bajo el anonimato resulta muy atractivo, ya que les permite emplear agresivamente las armas cibernéticas sin el mismo riesgo de represalias que conllevaría el uso abierto de la fuerza militar cinética. Como explican Egloff y Smeets (2023), un ciberatacante puede tener una expectativa razonable de eludir el castigo si la víctima no puede determinar la culpa de forma concluyente, o si al hacerlo se enfrentará al escepticismo internacional. Esto, como cabe suponer, complica la estrategia de “disuasión”: tómese el caso del ámbito nuclear,

donde identificar al atacante suele ser sencillo (por ejemplo, un radar detecta el lanzamiento de misiles balísticos desde un país), lo que permite tomar represalias.

En el ámbito cibernético, un Estado víctima puede sufrir daños graves, pero tendrá serias dificultades para atribuir la responsabilidad a tiempo para responder. Es en ese contexto donde los agresores explotan la brecha: por ejemplo, los *hackers* estatales de Corea del Norte, conocidos por operar bajo la apariencia del "Grupo Lazarus", niegan sistemáticamente sus vínculos con el régimen de Pyongyang. Cuando Estados Unidos acusó formalmente a Corea del Norte del hackeo a Sony Pictures y del posterior brote del *ransomware* WannaCry, el Gobierno norcoreano desestimó las acusaciones por infundadas, a sabiendas de que era difícil presentar pruebas definitivas públicamente.

Sin embargo, la dificultad de la atribución no es absoluta: los analistas cualificados y las agencias de inteligencia a menudo pueden identificar a los perpetradores utilizando una combinación de análisis forense técnico y fuentes humanas de inteligencia. De hecho, Rid y Buchanan (2015) argumentan que "la atribución no solo es posible, sino que se ha estado realizando con éxito durante mucho tiempo" (p. 31), y que los atacantes no pueden asumir que siempre permanecerán en el anonimato después de causar graves daños. Señalan que Estados con recursos suficientes (como la Agencia de Seguridad Nacional de Estados Unidos o el comando cibernético de China) tienen capacidades únicas para rastrear incluso operaciones sofisticadas.

Con el tiempo, se han atribuido numerosos ataques de alto perfil: la evidencia forense, por ejemplo, vinculó el gusano "Stuxnet" a una operación conjunta estadounidense-israelí, y minuciosas investigaciones identificaron a la inteligencia rusa como responsable de los ataques informáticos a las elecciones estadounidenses de 2016 y del ataque de malware "NotPetya" de 2017 (Whyte & Mazanec, 2023). Sin embargo, lograr la atribución suele requerir un tiempo considerable y un gran capital político, sobre todo si el atacante es muy sofisticado. En tal sentido, los Estados víctimas sopesan los costos y beneficios de denunciar públicamente a un adversario, ya que hacerlo puede exponer métodos de inteligencia o forzar una confrontación diplomática.

Los académicos han propuesto marcos para orientar cuándo y cómo los Estados deberían atribuir públicamente los ciberataques. Por ejemplo, Egloff y Smeets (2023) sugieren que los responsables de la toma de decisiones deben adoptar un pragmatismo estratégico y coordinado en la atribución abordándola como una decisión estratégica caso por caso, en vez de una respuesta automática.

En ese orden de ideas, el “Marco de Atribución Pública”, de Egloff y Smeets (2023) describe los factores clave que un gobierno debe evaluar antes de hacer pública una acusación: 1) Objetivo de la atribución: ¿Qué pretende lograr el Estado con la atribución? (p. ej., disuasión, condena internacional, garantías internas). Se necesita un objetivo claro y coherente. 2) Gravedad del incidente: ¿Qué tan grave es el impacto del ciber incidente? (p. ej., espionaje menor vs. destrucción de infraestructura crítica). Es decir, cuanto más grave sea el delito, más sólidos serán los argumentos para la atribución y la respuesta. 3) Contexto geopolítico: ¿Cuál es el entorno estratégico general? Las relaciones con el sospechoso, los posibles riesgos de escalada y las implicaciones para el derecho internacional son importantes. 4) Opciones posteriores a la atribución: ¿Qué respuesta o seguimiento permitirá la atribución? (p. ej., sanciones, acusaciones legales, medidas anticibernéticas, etc.). Si un Estado culpa públicamente a un adversario, debe estar preparado para actuar o al menos coordinarse con sus aliados, ya que, de lo contrario, la atribución podría sonar falsa.

Según Egloff y Smeets (2023), considerar estos factores ayuda a los gobiernos a decidir si anuncian una atribución, si la gestionan discretamente por la vía diplomática o si se abstienen de atribuirla en caso de que las pruebas sean escasas. Por ejemplo, en algunos casos, un Estado podría confrontar en privado a un adversario con pruebas (lo cual indica que conoce la responsabilidad) sin hacer una acusación pública, y mantener así cierto grado de disuasión y evitarse acorralar al adversario. En otros casos, como los de ataques atroces o descarados, la atribución pública puede generar apoyo nacional e internacional: un ejemplo es la atribución pública conjunta de Estados Unidos y el Reino Unido al Departamento Central de Inteligencia ruso (en ruso, GRU, por las iniciales de *Glávnoye Razvédyvatelnoye Upravlenie*) por el ciberataque NotPetya de 2017, para exigir responsabilidades a Moscú y demostrar unidad entre los aliados occidentales.

Desde la perspectiva de las normas y el derecho internacionales, el desafío de la atribución plantea preguntas difíciles. Si las víctimas no pueden probar fácilmente quién las atacó, ¿cómo pueden invocar la legítima defensa o buscar justicia? Esto ha dado lugar a demandas de mejoras en la ciber-ciencia forense y el intercambio de inteligencia entre aliados, e incluso, a propuestas para mecanismos internacionales de atribución. Mientras tanto, algunos Estados nación (especialmente, las democracias occidentales) han recurrido a la acusación *in absentia* contra *hackers* extranjeros, lo que en realidad implica “nombrar y avergonzar” a individuos de Estados adversarios. Por ejemplo, el Departamento de Justicia de

Estados Unidos ha acusado a miembros del Ejército Popular de Liberación de China y de la inteligencia militar rusa de ciberdelitos. Si bien dichas acciones legales son mayormente simbólicas, sirven para atribuir responsabilidades y erosionar la negación.

En resumen, el anonimato y la negación plausible en el ciberespacio permiten a los actores librar una guerra encubierta en la sombra de la ambigüedad, lo que convierte la atribución en un problema central de la ciberguerra. Esta dificultad complica la disuasión y la rendición de cuentas, pues los agresores se esconden tras un velo de incertidumbre. Sin embargo, a medida que las técnicas de atribución mejoran y los Estados coordinan sus respuestas, los adversarios deben sopesar el riesgo de ser desenmascarados. El duelo entre atacantes sigilosos e investigadores es una contienda continua en el campo de batalla de la G5G, que determina cómo se comportan (y se portan mal) los Estados en el ciberespacio.

Operaciones de bajo costo y alto impacto: el atractivo de las ciberarmas

Las ciberarmas² ofrecen una notable relación costo-impacto, sumamente atractiva desde un punto de vista estratégico. En comparación con el enorme gasto del *hardware* militar tradicional, las ciberarmas pueden a menudo desarrollarse e implementarse a un ínfimo costo, pero sus efectos pueden ser generalizados y significativos. Este potencial de bajo costo y alto impacto es una razón clave por la que la ciberguerra ha proliferado entre actores estatales y no estatales, y se relaciona directamente con su atractivo asimétrico. Especialmente en la G5G, donde los Estados buscan maneras de obtener ventajas sin involucrarse en guerras prolongadas y costosas, las ciberoperaciones ofrecen una opción tentadora.

Varios ejemplos ilustran lo atractivo de la economía de ciberguerra. De acuerdo con Whyte y Mazanec (2023), se considera que el gusano "Stuxnet" (desarrollado entre 2007-2008) fue un arma cibernética encubierta de última generación utilizada para sabotear el programa nuclear de Irán. Se estima que la creación de "Stuxnet" costó entre 5 y 25 millones de dólares, principalmente en el gasto de programadores expertos y pruebas. En ese orden de ideas, si Estados Unidos o Israel hubieran intentado lograr un efecto similar (o sea, desactivar las centrifugadoras de uranio iraníes) por medios convencionales, el coste habría sido exponencialmente

² Un arma cibernética se define como cualquier *malware* o código informático malicioso diseñado para robar datos confidenciales o causar daños a gran escala. Esto incluye virus informáticos, troyanos, *spyware* y gusanos que pueden introducir código malicioso en el *software* existente, y provocar así que un computador realice acciones o procesos no previstos por su operador.

mayor: quizás, un bombardero furtivo de 2 mil millones de dólares lanzando bombas antibúnkeres, con un enorme riesgo geopolítico. Por el contrario, “Stuxnet” logró discretamente la destrucción física sustancial de centrifugadoras iraníes, sin personal en peligro y sin confrontación directa.

Aunque desarrollar “Stuxnet” requería conocimientos avanzados (y, por lo tanto, una inversión e inteligencia significativas), una vez desarrollado, el *malware* podía replicarse y reestructurarse prácticamente sin coste. Esto lo señaló el experto en ciberseguridad Eugene Kaspersky, quien observó que el código de “Stuxnet”, ahora público, podía ser analizado y modificado por otros con bastante facilidad. Esto significa que la inversión inicial en Investigación, Desarrollo e Innovación (I+D) en una ciberarma sofisticada puede ser rentable si el código se reutiliza o sirve como modelo para futuros ataques, lo que reduce aún más el coste efectivo para los actores posteriores.

Incluso las ciberoperaciones menos sofisticadas tienen un coste insignificante en comparación con el daño potencial. Por ejemplo, un *hacker* podría dedicar varios días a crear un correo electrónico de *phishing* y una carga útil de *malware* a un costo de prácticamente cero con un computador básico. Sin embargo, si ese correo electrónico logra vulnerar la seguridad de un objetivo podría facilitar el robo de millones de dólares o provocar el cierre de las redes de una empresa durante varios días. Un caso real es el *ransomware* WannaCry, en 2017: probablemente desarrollado a partir de herramientas de espionaje filtradas, WannaCry se extendió globalmente e interrumpió el Servicio Nacional de Salud británico y muchas otras organizaciones. La inversión de los autores fue insignificante (reutilizaron código existente), pero el impacto fue de cientos de millones de dólares en daños y costes de recuperación en todo el mundo (Whyte & Mazanec, 2023). De manera similar, el *malware* “NotPetya” (atribuido a Rusia, en 2017) se hizo pasar por *ransomware*, pero era un limpiador destructivo que causó daños globales estimados en 10 mil millones de dólares (al paralizar la logística del gigante naviero Maersk y afectar a numerosas empresas multinacionales), y todo a partir de un fragmento de código malicioso probablemente mucho más barato que un solo misil de crucero (Whyte & Mazanec, 2023).

Por lo tanto, la escala y variedad de los efectos que pueden lograrse con modestas inversiones en ciberseguridad son sorprendentes. Las operaciones cibernéticas pueden robar datos confidenciales, sabotear procesos industriales, interrumpir las redes de comunicación o debilitar los sistemas financieros. Prácticamente cualquier sistema que dependa de computadores es un objetivo

potencial. Muchos de estos efectos, si se realizan de forma cinética, requerirían importantes campañas o ataques militares. Por ejemplo, provocar un apagón en la ciudad de un adversario mediante un ataque físico podría implicar el bombardeo de centrales eléctricas, un acto de guerra abierta. Pero en 2015 *hackers* rusos lograron desconectar temporalmente la red eléctrica de Ucrania mediante un ciberataque, y así cortaron el suministro eléctrico a miles de personas sin siquiera cruzar la frontera con tanques o aviones. El coste para los atacantes fue principalmente el trabajo de desarrollo y ejecución del *malware* (quizás, meses de trabajo por parte de un equipo de *hackers*), mientras que el impacto fue una pequeña muestra de parálisis de la infraestructura para la víctima.

De igual modo, perturbar los mercados financieros de un enemigo por medios convencionales sería extremadamente difícil, pero una ciberintrusión podría, teóricamente, manipular o borrar datos financieros con consecuencias económicas devastadoras, todo a través de líneas de código. Y la proliferación del conocimiento exacerba esta rentabilidad, ya que una vez se revela una nueva técnica cibernética (como ocurre cuando se expone o filtra *malware*) a menudo puede ser copiada y utilizada por otros con mucho menos esfuerzo que el creador original. La comunidad global de *hackers*, incluyendo criminales y agentes estatales, comparte y vende “exploits”³ en el mercado negro, lo cual significa que las armas cibernéticas de vanguardia y costosas de hoy pueden inspirar los kits de ataque económicos y listos para usar del mañana. Esta difusión reduce aún más los costos y empodera incluso a los actores menos capacitados.

En esencia, existe una “proliferación armamentística” de *malware* y *exploits*, pero, a diferencia de las armas nucleares o convencionales, estas pueden reproducirse infinitamente con un costo marginal cercano a cero una vez existentes (Eklund & Djup, 2021). Por ende, con el tiempo, la barrera de entrada en términos de costo y experiencia se ha reducido: lo que requería el esfuerzo de un Estado nación hace una década podría estar hoy al alcance de una banda de cibercriminales o de un pequeño ejército, gracias a las herramientas y el código disponibles.

En consecuencia, las implicaciones estratégicas del perfil de bajo costo y alto impacto de la ciberseguridad son profundas. Para Estados con restricciones económicas (por ejemplo, Corea del Norte e Irán), el ciberespacio ofrece una forma de proyectar poder internacionalmente sin arruinar sus propias finanzas. Un Estado

³ Un *exploit*, en el contexto de la ciberseguridad, es un programa o técnica que aprovecha una vulnerabilidad en un sistema para realizar acciones no autorizadas o causar un comportamiento no deseado. Estas vulnerabilidades pueden estar en *software*, *hardware* o, incluso, en la configuración del sistema. Los *exploits* pueden ser utilizados para acceder a sistemas, robar datos, instalar *malware* o interrumpir el funcionamiento de un programa.

que jamás podría permitirse una fuerza aérea o una armada modernas aún puede entrenar o contratar *hackers* y lograr influencia geopolítica. Corea del Norte, por ejemplo, invirtió fuertemente en el ciberespacio como una forma de política económica utilizándolo para robo financiero (piratería bancaria para evadir sanciones), inteligencia militar y ataques disruptivos, todos con un costo mucho menor que las operaciones militares convencionales.

Para grupos terroristas, desarrollar capacidades cibernéticas también resulta atractivo, ya que hacerlo no requiere la adquisición de armas ni municiones (aunque hasta la fecha el ciberterrorismo de alto impacto ha sido limitado). Desde la perspectiva de una gran potencia, el bajo costo para los adversarios se traduce en un alto volumen de amenaza: muchos actores pueden permitirse atacar. Esto complica la defensa, ya que una superpotencia podría enfrentarse a un ciberacoso persistente y simultáneo de decenas de fuentes (desde grupos criminales de *ransomware* hasta unidades de espionaje patrocinadas por Estados). Cada amenaza individual es económica para su creador, pero en conjunto impone un enorme coste acumulativo a la economía y la seguridad del objetivo. En términos de G5G, permite campañas prolongadas de desgaste y disrupción sin una guerra formal.

Finalmente, cabe destacar que, si bien las ciberoperaciones son económicas en relación con sus efectos, no son gratuitas: aún se necesita inversión en habilidades e infraestructura. Las operaciones verdaderamente sofisticadas (como el desarrollo de *exploits* personalizados para sistemas bien defendidos) pueden requerir una cantidad considerable de tiempo, talento y dinero. Eklund y Djup (2021) han advertido que adquirir ciberarmas de primer nivel no es trivial para los actores más débiles. Sin embargo, aunque desarrollar *exploits* de día cero o herramientas avanzadas es difícil, el uso de herramientas filtradas o comerciales existentes es fácil y económico (Whyte & Mazanec, 2023). Esto, en esencia, refleja por qué los ciberataques son un elemento básico de la G5G: ofrecen una alta rentabilidad con una inversión mínima, una combinación a la que los estrategas no se resisten.

La ciberguerra como parte de la guerra híbrida y las operaciones en la zona gris

La ciberguerra rara vez se presenta de forma aislada. Con mayor frecuencia, se emplea como una herramienta más en la guerra híbrida o en campañas en la zona gris, donde los Estados combinan medios militares y no militares, cinéticos y no cinéticos, para lograr objetivos estratégicos sin desencadenar una guerra a gran escala. En la G5G, que se nutre de la ambigüedad y la indirección, las ciberoperaciones se integran a la perfección con las operaciones psicológicas, la guerra

de la información, la coerción económica y el uso de intermediarios. El resultado es una forma de conflicto en la que la sociedad del adversario puede ser atacada persistentemente y de forma coordinada en múltiples dominios (físico, cognitivo y cibernético).

Por lo tanto, comprender la ciberguerra requiere situarla en el contexto más amplio de las estrategias híbridas y la zona gris entre la guerra y la paz. De acuerdo con Weissmann (2021), la guerra híbrida se refiere al uso sincronizado de diferentes tipos de poder como fuerza militar convencional, tácticas irregulares (insurgencia, terrorismo), ciberataques, manipulación de la información y presión diplomática, entre otras, para desestabilizar o debilitar a un oponente. El concepto cobró relevancia en los análisis de las tácticas rusas, especialmente tras la anexión de Crimea, en 2014, y el conflicto en Ucrania (Göransson, 2021). En ambos casos Rusia combinó fuerzas especiales encubiertas (*hombrecitos verdes*), milicias locales, intensa propaganda, influencia económica y ciberataques contra la infraestructura ucraniana para lograr sus objetivos negando oficialmente su participación directa.

Como lo señalan Eklund y Djup (2021), las operaciones cibernéticas rusas fueron fundamentales: por ejemplo, junto con las acciones terrestres, *hackers* vinculados a Rusia lanzaron oleadas de ataques contra las redes y medios de comunicación del Gobierno ucraniano, mientras sembraban la confusión y obstaculizaban la respuesta de Kiev. Esta convergencia de medios cinéticos y cibernéticos es exactamente lo que Clarke y Knake (2010) predijeron: que la mayoría de las guerras futuras incluirán el uso conjunto de armas cinéticas y cibernéticas. De hecho, en la actual guerra en Ucrania y en otros lugares se observa que tanto los misiles como el *malware* suelen utilizarse en conjunto, complementándose mutuamente.

Un aspecto clave de la guerra híbrida es operar en la "zona gris", una gama de actividades más agresivas que la política tradicional, pero por debajo del umbral de una guerra abierta. De acuerdo con el National Intelligence Council de los Estados Unidos (NIC), la zona gris constituye un ámbito de las relaciones internacionales situado entre la diplomacia pacífica y el conflicto armado, donde Estados y actores no estatales emplean medios coercitivos o subversivos (violentos o no violentos) para lograr objetivos políticos y de seguridad explotando vacíos normativos o actuando en ausencia de normas internacionales claramente establecidas (NIC, 2024). A diferencia de la guerra convencional, las actividades en la zona gris son deliberadamente diseñadas para permanecer por debajo del umbral del conflicto armado abierto, evitando desencadenar una respuesta militar directa y sostenida. Según el NIC, estas acciones se caracterizan por su ambigüedad intencional, el

uso de métodos indirectos, la dificultad de atribución y una lógica incremental y acumulativa, orientada a producir cambios materiales o políticos significativos en el *statu quo* sin cruzar formalmente los límites jurídicos y estratégicos de la guerra.

Desde esta óptica, la zona gris no debe entenderse como una fase transitoria entre paz y guerra, sino como un espacio funcional permanente de competencia estratégica, en el cual los actores combinan instrumentos diplomáticos, económicos, informacionales, cibernéticos y encubiertos de manera sostenida. Tal como subraya el NIC (2024), las campañas en zona gris suelen adoptar un enfoque multidominio, explotar la fragmentación institucional del adversario y aprovechar la incertidumbre normativa y política como un recurso estratégico en sí mismo. En consecuencia, la ciberguerra es ideal para las tácticas de zona gris: sus atributos permiten a los Estados lograr efectos que se considerarían actos de guerra si se realizaran abiertamente por medio de la fuerza cinética, pero en su forma cibernética complican la cuestión de si la guerra ha comenzado. Por ejemplo, inutilizar una red eléctrica mediante hackeo podría considerarse un acto de guerra, pero si la atribución es turbia y ocurre fuera de un conflicto declarado, la víctima puede dudar en si responder o no con fuerza. Esto crea una zona de maniobra para el agresor. Como afirman Eklund y Djup, (2021), “la naturaleza asimétrica de los ataques basados en internet dificulta determinar los factores motivadores y atribuir el ataque a un actor específico, lo que genera un entorno de incertidumbre y [cuestiona] si un acto específico puede considerarse un acto de guerra” (p. 149).

Esta incertidumbre es la esencia de la agresión en zona gris: los adversarios la explotan para avanzar gradualmente en sus planes (Weissmann, 2021). Los actores estatales han incorporado la ciberguerra a sus doctrinas y estrategias militares oficiales, de forma explícita, como un componente de las operaciones híbridas. En el concepto ruso de “guerra de nueva generación”, la confrontación de información (incluida la ciberguerra) es un elemento central utilizado desde el inicio de un conflicto para configurar el campo de batalla sin recurrir necesariamente a grandes despliegues de tropas (Göransson, 2021). China, por su parte, habla de “guerra informatizada” y tiene una doctrina que utiliza las ciberoperaciones para el dominio de la información en la fase inicial de cualquier conflicto (Saalman, 2021). Estos enfoques tratan las herramientas cibernéticas no de forma aislada, sino como parte de un enfoque de armas combinadas para el conflicto. Al igual que la artillería o el poder aéreo apoyan a las tropas terrestres, los ciberataques pueden apoyar y amplificar otras líneas de esfuerzo (y en ocasiones, sustituirlas).

De acuerdo con Weissmann (2021), una característica distintiva de la guerra híbrida es su ataque a la esfera civil y las instituciones del oponente para erosionar

la moral, causar problemas económicos y generar discordia interna. La ciberguerra es un poderoso facilitador en este caso, pues las sociedades modernas se hallan profundamente digitalizadas. Los atacantes pueden atacar los servicios públicos, las finanzas, las comunicaciones y los medios de comunicación para desestabilizar una sociedad desde dentro, todo ello sin una invasión formal. Por ejemplo, y según Bach (2021), durante las tensiones en el Báltico, presuntas campañas cibernéticas rusas desfiguraron sitios web gubernamentales y difundieron desinformación para exacerbar las divisiones étnicas. En 2007, cuando Estonia reubicó una estatua de la era soviética, ciberataques masivos coordinados (probablemente, con la aprobación tácita de Rusia) paralizaron durante días los bancos, las comunicaciones gubernamentales y los medios de comunicación estonios.

Posteriormente, la Organización del Tratado del Atlántico Norte (OTAN) reconoció lo anterior como una llamada de atención sobre el riesgo de que un Estado miembro pudiera verse gravemente perjudicado por medios cibernéticos en tiempos de paz (Crowther, 2021). La ciberguerra también permite operaciones de influencia a escala global, otra faceta clave de la guerra híbrida. La manipulación de redes sociales, los ataques informáticos y las filtraciones de información confidencial, al igual que las campañas de propaganda en línea. Se consideran interferencias cibernéticas en el ámbito político de un adversario. La interferencia en las elecciones estadounidenses de 2016 es un ejemplo destacado: *hackers* rusos penetraron servidores de correo electrónico y filtraron información perjudicial, mientras que un ejército de *trolls* y *bots* amplificaba contenido divisivo en redes sociales. Si bien estas acciones no causaron daños físicos, tuvieron un impacto estratégico al socavar la confianza pública y la cohesión social, y lograron con solo bytes lo que antes habría requerido agentes humanos subversivos sobre el terreno.

En cierto sentido, las técnicas cibernéticas han potenciado tácticas ancestrales como la propaganda y el espionaje permitiendo que se lleven a cabo de forma remota y a gran escala. Y la “niebla de guerra” es densa en las campañas cibernéticas híbridas, pues las víctimas a menudo se enfrentan a la confusión sobre lo que está sucediendo y quién está detrás, lo que retrasa y debilita su respuesta. Durante una ofensiva híbrida coordinada, un Estado podría experimentar cortes de energía (sabotaje cibernético), explosiones de noticias falsas (operaciones de información), protestas callejeras (quizás, impulsadas por la propaganda) e incidentes paramilitares, todo a la vez. La naturaleza interconectada de los sistemas modernos puede incluso desdibujar si un efecto fue deliberado o colateral.

Por consiguiente, defenderse de las campañas cibernéticas híbridas es un gran desafío, ya que requiere la resiliencia de toda la sociedad, y no solo de cortafuegos.

Los Estados y las alianzas militares (como la OTAN) se han adaptado mediante el desarrollo de equipos de respuesta cibernética rápida, acuerdos de intercambio de información y asociaciones público-privadas para proteger la infraestructura crítica. Según Crowther (2021), la OTAN incluso ha declarado formalmente que un ciberataque podría, en determinadas circunstancias, activar la defensa colectiva del artículo 5 del Tratado del Atlántico Norte, al reconocer que el ciberespacio forma parte del espectro bélico. Sin embargo, en la práctica, la dificultad de atribuir y la preferencia por evitar la escalada implican que las respuestas a las ciberoperaciones en la zona gris suelen ser diplomáticas o económicas (sanciones), en vez de militares. En conclusión, la ciberguerra en la 5GW rara vez se trata de un fenómeno aislado: se entrelaza con estrategias de guerra híbrida que buscan lograr objetivos estratégicos bajo el manto de la ambigüedad. Al atacar sistemas críticos, difundir desinformación y perturbar la vida cotidiana, los ciberataques complementan otras tácticas para debilitar la determinación y la capacidad de lucha del adversario.

Operaciones cibernéticas, armas y tácticas: el arsenal digital en las guerras de quinta generación

De acuerdo con Couretas (2024), una “ciberoperación” se refiere a las acciones y actividades coordinadas que se llevan a cabo en el dominio ciberespacial para lograr efectos específicos en los sistemas, redes o datos del adversario. Las ciberoperaciones pueden incluir espionaje, sabotaje, disrupción o destrucción, y son utilizadas por Estados, delincuentes, hacktivistas y otros actores para lograr objetivos políticos, militares o económicos. Ahora bien, dentro de la ciberestrategia militar, las ciberoperaciones suelen dividirse entre operaciones cibernéticas ofensivas (OCO) y operaciones cibernéticas defensivas (OCD). Estas categorías, utilizadas, por ejemplo, por el Departamento de Defensa de los Estados Unidos, capturan la doble naturaleza de la ciberguerra: es decir, la capacidad para atacar los sistemas del adversario y la capacidad para defender los propios. Por consiguiente, comprender la diferencia entre OCO y OCD, y cómo se complementan, es clave para comprender la lógica operativa de las fuerzas cibernéticas en los ejércitos modernos.

Evolución de las operaciones cibernéticas

Las operaciones cibernéticas se han vuelto un rasgo distintivo de los conflictos del siglo XXI, al transformar los paradigmas tradicionales de la guerra y la seguridad.

Su trayectoria histórica muestra una progresión desde el hackeo experimental y oportunista hasta sofisticadas campañas cibernéticas patrocinadas por Estados que combinan la innovación técnica con la estrategia geopolítica. Como señala Willett (2024), las ciberoperaciones han evolucionado a través de tres dimensiones superpuestas: la formulación doctrinal por parte de los Estados, el reconocimiento público de operaciones específicas y la atribución y denuncia de dichas campañas por parte de terceros. Estas facetas, en conjunto, subrayan la creciente integración de las capacidades cibernéticas en las arquitecturas de seguridad nacional.

Décadas de 1980-1990: experimentación temprana y hackeos

La primera fase de las ciberoperaciones se caracterizó por la experimentación, intrusiones motivadas por la curiosidad y el surgimiento del concepto de ciberseguridad. Los orígenes de las operaciones cibernéticas se remontan a finales de la década de 1980, con incidentes pioneros como el "Cuckoo's Egg" (1986), en el que *hackers* de Alemania Occidental se infiltraron en las redes de defensa estadounidenses. A ello le siguió el "Gusano Morris" (1988), que marcó el primer *malware* autorreplicante significativo que causó una disrupción generalizada, al paralizar aproximadamente el 10 % del internet global explotando contraseñas débiles y errores de *software*, lo que mostró la inesperada magnitud de las vulnerabilidades digitales (O'Leary, 2019).

La década de 1990 y los principios de la década de 2000 fueron testigos de la maduración de las operaciones cibernéticas, al pasarse de incidentes aislados a acciones coordinadas a nivel estatal. Ejemplos notables incluyen la Operación Laberinto de Luz de Luna, llevada a cabo por parte de Rusia en 1998, y que implicó un extenso espionaje contra agencias gubernamentales estadounidenses, así como la Operación Lluvia de Titanes, de China, a principios de la década de 2000, que atacó sistemáticamente a contratistas de defensa y redes gubernamentales estadounidenses (Willett, 2024). Estas campañas subrayaron la transición del cibervandalismo a intrusiones estratégicas persistentes destinadas a obtener información confidencial y erosionar las ventajas tecnológicas de los adversarios.

Década de 2000-2010: operaciones patrocinadas por Estados, ataques DoS y espionaje

En esta fase las operaciones cibernéticas pasaron de la experimentación *amateur* a campañas altamente organizadas lideradas por Estados y actores sofisticados. Un ejemplo importante es la Operación Aurora (2009-2010), una serie de ciberintrusiones presuntamente vinculadas a China, que tuvieron por objetivo importantes empresas

tecnológicas estadounidenses, como Google, Adobe y Juniper Networks. El propósito de la operación era robar propiedad intelectual y vigilar las cuentas de Gmail de activistas de derechos humanos, lo que revela cómo las cibercampañas persiguen objetivos tanto económicos como políticos (O'Leary, 2019; Couretas, 2024). Otro ejemplo son los ciberataques de 2008 contra Georgia durante el conflicto ruso-georgiano; estos ataques utilizaron campañas de denegación de servicio distribuida (DDoS) y desfiguraciones de sitios web para paralizar los medios de comunicación, el gobierno y los servicios financieros georgianos sincronizando la disrupción digital con las operaciones militares físicas (Couretas, 2024).

Pero el momento decisivo en la historia de las operaciones cibernéticas llegó con el descubrimiento de "Stuxnet", en 2010. Stuxnet, un sofisticado gusano informático, fue diseñado para sabotear el programa de enriquecimiento de uranio de Irán atacando los sistemas de control industrial de la planta nuclear de Natanz. Su precisión, sigilo y complejidad lo posicionaron como un hito en la historia de la ciberguerra (Lindsay, 2013; Aanonsen, 2025). Stuxnet representó una iniciativa conjunta estadounidense-israelí bajo el nombre en clave "Olympic Games", cuyo objetivo era retrasar las ambiciones nucleares de Irán sin recurrir a una acción militar cinética.

Técnicamente, "Stuxnet" se destacó por el uso de cuatro vulnerabilidades de día cero (fallos de *software* desconocidos explotados antes de que pudieran desarrollarse parches), junto con certificados digitales robados para ocultar su identidad. Inicialmente se propagó a través de unidades USB para conectar sistemas con aislamiento de aire, una táctica que puso de relieve el profundo conocimiento de los atacantes sobre entornos de seguridad tanto digitales como físicos (Aanonsen, 2025). Según Lindsay (2013), la carga útil de "Stuxnet" fue diseñada para alterar sutilmente la velocidad de rotación de las centrifugadoras, para provocar su degradación con el tiempo, a la vez que alimentaba datos falsos a los sistemas de monitorización, y ocultar así el sabotaje a los técnicos iraníes. Estratégicamente, "Stuxnet" planteó preguntas cruciales sobre la naturaleza y los límites de la ciberguerra. Como señala Willett (2024), si bien muchos aclamaron a "Stuxnet" como el inicio de una nueva era en los ciberconflictos, otros advirtieron que su éxito fue puramente táctico y no impidió que la República Islámica de Irán prosiguiera con su programa nuclear. De hecho, para 2013 Irán había ampliado significativamente su capacidad de centrifugación, lo cual sugiere que el impacto de "Stuxnet" fue más una interrupción temporal que una victoria decisiva.

Además, las consecuencias de "Stuxnet" impulsaron un replanteamiento de la estrategia cibernética a nivel global. Lindsay (2013) argumenta que la exposición del gusano terminó desencadenando, por parte de los Estados, una carrera

armamentista en el desarrollo de capacidades cibernéticas ofensivas, ya que estos reconocieron tanto el potencial como las limitaciones del ciber sabotaje. "Stuxnet" también desdibujó la línea entre espionaje y guerra, al desafiar los marcos legales y éticos existentes que rigen el comportamiento estatal en el ciberespacio. Además de su impacto operativo, "Stuxnet" sirvió como herramienta de diplomacia secreta. Lindsay (2025) sugiere que el gusano buscaba tanto ganar tiempo para las negociaciones diplomáticas como sabotaje físico. La naturaleza encubierta de la operación permitió a Estados Unidos e Israel presionar a Irán, y evitar, al mismo tiempo, consecuencias internacionales que podrían acompañar los ataques militares cinéticos. En este sentido, el caso de "Stuxnet" personifica la convergencia de las operaciones cibernéticas con una política geopolítica más amplia.

Década de 2010-presente: integración cibernética, ransomware y explotación de big data

El legado de "Stuxnet" es evidente en las campañas cibernéticas posteriores. Por ejemplo, el ataque de *malware* "NotPetya", en 2017, atribuido a actores estatales rusos, mostró técnicas similares de *malware*, pero con el objetivo de causar una perturbación económica generalizada, en vez de un sabotaje preciso. En este orden de ideas, la fase actual se define por la integración de los efectos cibernéticos y cinéticos, el auge del *ransomware* como herramienta geopolítica y la explotación a gran escala de datos personales y comerciales. Un ejemplo fue la filtración de datos personales de la Oficina de Administración de Personal (2015) por parte de actores chinos, lo que representa uno de los mayores robos de datos personales en la historia de Estados Unidos, con más de 21 millones de registros comprometidos, incluyendo formularios confidenciales de autorización de seguridad. La operación puso de manifiesto el valor estratégico de la exfiltración de datos a gran escala con fines de inteligencia (O'Leary, 2019).

Por su lado, las campañas de *ransomware* como el ataque al Oleoducto Colonial (2021) ilustran aún más la evolución de las operaciones cibernéticas hacia la disrupción económica y la coerción. Llevado a cabo por el grupo de *ransomware* "DarkSide", el ataque interrumpió el suministro de combustible en la costa este de Estados Unidos, lo que provocó declaraciones de emergencia y puso en evidencia la vulnerabilidad de las infraestructuras críticas (O'Leary, 2019). Otro caso notable fue el ataque informático al Comité Nacional Demócrata (en inglés DNC, por las iniciales de Democratic National Committee) de Estados Unidos, en 2016, por parte de la inteligencia rusa, cuando se exfiltraron y filtraron correos electrónicos para influir en las elecciones presidenciales.

Este asalto marcó un punto de inflexión en el uso de operaciones cibernéticas para la guerra política y la influencia informativa (Couretas, 2024). Los ataques a Saudi Aramco Shamoon (2012, 2016), presuntamente orquestados por actores iraníes, utilizaron *malware* destructivo de borrado de datos a fin de paralizar a la mayor compañía petrolera del mundo destruyendo decenas de miles de computadores y causando semanas de interrupción operativa. Este caso demostró la evolución de las operaciones cibernéticas hacia el sabotaje económico (O'Leary, 2019). Asimismo, el robo al banco de Bangladesh (2016), atribuido a Corea del Norte, combinó la ciberdelincuencia con objetivos estatales utilizando la red financiera SWIFT para intentar el robo de casi mil millones de dólares (de los cuales se robaron 81 millones). Esta operación ilustró cómo las herramientas cibernéticas pueden utilizarse para generar ingresos a los regímenes sancionados (Couretas, 2024).

Varias tendencias se manifiestan a lo largo de las fases de evolución de las operaciones cibernéticas. En primer lugar, se evidencia una creciente sofisticación de los ataques, desde gusanos simples hasta *malware* de alta ingeniería y campañas multivectoriales. En segundo lugar, las operaciones cibernéticas están ahora profundamente arraigadas en la doctrina militar, las operaciones de inteligencia y la estrategia diplomática (Couretas, 2024). En tercer lugar, los Estados combinan cada vez más las acciones cibernéticas con la guerra cognitiva, la coerción económica y las operaciones militares. Por último, las operaciones cibernéticas ya no son dominio exclusivo de los Estados: los actores no estatales, los grupos criminales y sus aliados desempeñan ahora un papel decisivo en dichas acciones (O'Leary, 2019).

Según Couretas (2024), esta evolución refleja la creciente sofisticación técnica, la proliferación de actores no estatales y la integración de operaciones cibernéticas en la estrategia estatal. Como se observa en la tabla 1, cada fase representa no solo un avance tecnológico, sino un cambio profundo en cómo los Estados y actores no estatales entienden y emplean el ciberespacio como campo de poder e influencia.

Tabla 1. Fases de la evolución de las operaciones cibernéticas

Fase histórica	Periodo	Características clave	Ejemplos representativos
1. Experimentación temprana	Década de 1980-década de 1990	- Hacks motivados por curiosidad o investigación - Descubrimiento de vulnerabilidades básicas - Primeros indicios de espionaje digital	<i>Morris Worm</i> (1988), <i>The Cuckoo's Egg</i> (investigación de Clifford Stoll sobre <i>hackers</i> de Alemania Oriental)
2. Operaciones estatales y espionaje	Década de 2000-2010	- Surgimiento de actores estatales - Operaciones de espionaje estratégico - Primeras operaciones disruptivas - Uso de ataques DoS/DDoS	Operación Aurora (China), ataques "DDoS" (a Estonia) (2007); "Stuxnet" (a Estados Unidos e Israel contra Irán); "Titan Rain" (China a Estados Unidos)
3. Integración cibernética y ransomware	2010-presente	- Combinación de ciberataques con efectos físicos y estratégicos - Auge del <i>ransomware</i> como herramienta criminal y geopolítica - Robo masivo de datos y operaciones híbridas	"NotPetya" (Rusia); ataque a Colonial Pipeline ("DarkSide"); hackeo al DNC (Rusia, 2016); "Shamoon" (Irán contra Saudi Aramco); Bangladesh Bank Heist (Corea del Norte)

Fuente: elaboración propia, con base en Couretas (2024).

En conclusión, la evolución de las operaciones cibernéticas, desde los primeros experimentos de *hacking* hasta la sofisticada campaña multicapa de "Stuxnet", subraya su creciente centralidad en los conflictos y la política moderna. Como bien observa Willett (2024), los conflictos cibernéticos actuales abarcan un amplio espectro, desde el acoso y el espionaje de bajo nivel hasta el sabotaje de alto impacto, lo que obliga a los Estados a adaptar continuamente sus doctrinas, defensas y estrategias para desenvolverse en ese ámbito complejo y en constante evolución. Como señalan Couretas (2024) y O'Leary (2019), el futuro de la ciberguerra será determinado por una mayor integración de la IA, la automatización y la coordinación ofensiva-defensiva, que convertirán el ciberespacio en un ámbito cada vez más decisivo en la política de poder global.

Operaciones cibernéticas ofensivas y operaciones cibernéticas defensivas

Las operaciones cibernéticas ofensivas (OCO) se refieren al uso de capacidades cibernéticas para proyectar poder en el ciberespacio, lograr objetivos políticos, militares o económicos, e imponer costos o moldear el comportamiento del

adversario atacando sus sistemas de información, redes o infraestructura crítica (Couretas, 2024; O'Leary, 2019). Estas operaciones implican acciones deliberadas que buscan negar el acceso, degradar capacidades, interrumpir servicios, destruir activos o manipular información dentro de los sistemas cibernéticos del adversario. Como enfatiza O'Leary (2019), las OCO marcan una transición de la defensa digital pasiva a los ataques proactivos y dirigidos, diseñados para "alterar la toma de decisiones y la efectividad operativa del adversario" (p. 52). Couretas (2024) describe de manera similar las OCO como "la convergencia de tecnología, inteligencia y arte operacional para lograr efectos no cinéticos con consecuencias a nivel cinético" (p. 11), destacando su potencial para reemplazar o complementar las operaciones militares tradicionales. Quizá, el ejemplo más conocido de OCO sea "Stuxnet", una sofisticada ciberarma estadounidense-israelí que atacó la planta de enriquecimiento de uranio de Natanz, en Irán. "Stuxnet" utilizó múltiples vulnerabilidades de día cero y una carga útil altamente especializada para sabotear centrifugadoras, a fin de retrasar el programa nuclear iraní sin un solo misil o bomba. Este caso ilustró cómo las capacidades cibernéticas pueden lograr objetivos geopolíticos y, al mismo tiempo, evitar un conflicto abierto, lo que sentó un precedente para futuras campañas cibernéticas ofensivas (Couretas, 2024; O'Leary, 2019).

A fin de comprender cómo se desarrollan las OCO, la *Cyber Kill Chain* (o cadena de ciberataque), desarrollada por Lockheed Martin, ofrece un marco conceptual ampliamente adoptado. Divide el proceso de ataque en distintas fases, cada una con sus propios desafíos técnicos y operativos (O'Leary, 2019; Couretas, 2024):

1. Reconocimiento: El atacante recopila información sobre el sistema o red objetivo, como la identificación de personal, tecnologías, vulnerabilidades y puntos de acceso. Esta fase suele basarse en inteligencia de código abierto (en inglés, OSINT, por las iniciales de *Open Source Intelligence*), ingeniería social y análisis técnico (O'Leary, 2019).
2. Armamentización: Se desarrolla *malware* y se combina con un *exploit* adecuado para las vulnerabilidades identificadas. Los atacantes, por ejemplo, podrían combinar un troyano de acceso remoto (en inglés, RAT, por las iniciales de *Remote Access Trojan*) personalizado con una carga útil de *phishing* selectivo (Couretas, 2024).
3. Distribución: La carga útil manipulada se transmite al entorno objetivo, a menudo a través de correos electrónicos de *phishing*, sitios web comprometidos o dispositivos USB infectados (O'Leary, 2019).
4. Explotación: Una vez dentro, el *malware* activa el *exploit*, y obtiene acceso o control no autorizado del sistema.

5. Instalación: El atacante instala una puerta trasera o un implante para mantener el acceso persistente, y asegurar así una presencia a largo plazo en la red.
6. Comando y Control (C2): El sistema comprometido establece un canal de comunicación con la infraestructura del atacante, lo que permite el control remoto y la asignación de tareas (Couretas, 2024).
7. Acciones según los objetivos: El atacante ejecuta el efecto deseado, ya sea la exfiltración de datos confidenciales, la interrupción de operaciones, la destrucción de activos o la manipulación de información (O'Leary, 2019).

Este enfoque por etapas es fundamental para el éxito operativo, y puede durar semanas o meses, sobre todo en campañas sofisticadas de amenazas persistentes avanzadas. Por ejemplo, en la Operación Lluvia de Titanes, entre 2003 y 2006, *hackers* chinos se infiltraron sistemáticamente en las redes de defensa estadounidenses, donde robaron datos militares confidenciales, planos de diseño de tecnologías militares y datos de inteligencia. Esta campaña de espionaje a gran escala demostró cómo las operaciones cibernéticas podían servir a objetivos de inteligencia estratégicos sin desencadenar un conflicto directo (Couretas, 2024). En efecto, las OCO ofrecen varias ventajas sobre la fuerza militar convencional:

1. Sigilo y negación: Las operaciones cibernéticas ofensivas pueden llevarse a cabo por debajo del umbral de la guerra, lo que dificulta la atribución y la respuesta.
2. Rentabilidad: Una inversión relativamente pequeña en herramientas o talento puede infligir un daño desproporcionado a un adversario mucho mayor.
3. Alcance global: El ciberespacio trasciende la geografía, lo que permite a los actores atacar objetivos en todo el mundo sin cruzar fronteras físicas.

Sin embargo, las OCO también conllevan riesgos. Los errores de cálculo, los daños colaterales y la escalada son peligros reales, especialmente cuando la infraestructura crítica se convierte en un objetivo predilecto. Por ejemplo, "NotPetya", originalmente dirigida contra entidades ucranianas, rápidamente se convirtió en un desastre global, que afectó a empresas como Maersk y Merck y causó más de miles millones de dólares en daños (Couretas, 2024). Empero, las OCO representan uno de los avances más transformadores en los conflictos contemporáneos: permiten a los actores estatales y no estatales imponer costos, recopilar inteligencia, moldear la percepción y degradar las capacidades del adversario sin disparar un solo tiro.

Por su parte, las operaciones cibernéticas defensivas (OCD) se refieren al conjunto de actividades, tecnologías y estrategias diseñadas para proteger los sistemas de información, las redes y los datos de ataques adversarios. Como explica Couretas (2024), el objetivo fundamental de las OCD es garantizar la confidencialidad, integridad y disponibilidad de los activos críticos ante un entorno de amenazas complejo y en rápida evolución. Mientras que las OCO buscan interrumpir o degradar a un adversario, las OCD buscan preservar la resiliencia y la funcionalidad de los propios sistemas bajo una ciberpresión persistente.

Las estrategias cibernéticas defensivas se dividen generalmente en dos grandes categorías: defensa pasiva y defensa activa. La defensa pasiva incluye las medidas básicas que protegen los sistemas por defecto, sin necesidad de una interacción activa con los adversarios. Estas medidas constituyen la primera línea de defensa, e incluyen:

1. Cortafuegos, que controlan el tráfico de red entrante y saliente.
2. *Software* antivirus y *antimalware*, que detectan y bloquean el código malicioso conocido. También, el cifrado, que protege los datos confidenciales en reposo y en tránsito.
3. Gestión de parches, que mantiene el *software* actualizado y corrige las vulnerabilidades conocidas.
4. Formación en seguridad para usuarios, con el fin de reducir los errores humanos.

Las defensas pasivas son cruciales, pero limitadas. Suelen basarse en firmas de amenazas conocidas y son menos eficaces contra ataques nuevos o sofisticados (por ejemplo, *exploits* de día cero). La defensa activa, en cambio, va más allá de la protección estática, ya que implica la monitorización, detección y respuesta en tiempo real para neutralizar las amenazas antes de que causen daños. Según O'Leary (2019), la defensa activa puede incluir:

1. Sistemas de detección de intrusiones (en inglés, IDS, por las iniciales de *Intrusion Detection System*) y sistemas de prevención de intrusiones (en inglés, IPS, por las iniciales de *Intrusion Prevention System*), que identifican y detienen la actividad sospechosa.
2. Búsqueda de amenazas, donde los analistas de seguridad buscan proactivamente amenazas ocultas en la red.
3. Segmentación y aislamiento de la red, que limitan la propagación de un ataque entre sistemas.
4. Tecnologías de engaño, como *honeypots* y *honeynets*, que atraen a los atacantes a entornos controlados, para su monitoreo.

5. *Hacking back*, o contramedidas ofensivas limitadas, aunque esto sigue siendo controvertido y legalmente restringido.

Couretas (2024) destaca que la defensa activa refleja una mentalidad de “compromiso persistente”, donde los defensores asumen el compromiso y se centran en la contención, la recuperación y la resiliencia, en vez de la prevención total. No obstante, las OCD se desarrollan en varias etapas, y conforman un ciclo de vida continuo de ciberdefensa:

1. Preparación: Establecer la arquitectura de defensa, capacitar al personal y hacer evaluaciones de riesgos.
2. Detección: Utilizar sensores, registros e inteligencia de amenazas para identificar actividad anormal.
3. Análisis: Investigar alertas, correlacionar datos y determinar si un evento es benigno o malicioso.
4. Contención: Aislar los sistemas afectados, para evitar el movimiento lateral. Erradicación y Recuperación: Eliminación de *malware*, cierre de vulnerabilidades y restauración desde copias de seguridad.
5. Revisión postincidente: Realización de ejercicios de lecciones aprendidas, para mejorar las defensas y ajustar las políticas.

Este enfoque cíclico garantiza que las organizaciones evolucionen junto con sus adversarios. La estrategia *Defend Forward*, del Comando Cibernético de los Estados Unidos, interrumpe proactivamente las operaciones adversarias antes de que lleguen a las redes estadounidenses combinando la defensa activa con las operaciones de inteligencia (Couretas, 2024). Los equipos CERT (Equipos de Respuesta a Emergencias Informáticas) de todo el mundo participan rutinariamente en operaciones defensivas, que incluyen la coordinación de vulnerabilidades, la respuesta a incidentes y la difusión de avisos de amenazas. En el sector privado, empresas como Google y Microsoft operan centros de operaciones de seguridad (en inglés, SOC, por las iniciales de *Security Operations Center*) 24/7, que monitorean miles de millones de eventos al día utilizando IA y analistas humanos para detectar y neutralizar amenazas (Couretas, 2024).

Sin embargo, y a pesar de los avances, las OCD se enfrentan a desafíos persistentes:

1. Asimetría: Los defensores deben asegurar todos los puntos, mientras que los atacantes solo necesitan un éxito.
2. Incertidumbre de atribución: Identificar con prontitud a un atacante es difícil, lo que complica las estrategias de respuesta.

3. Restricciones de recursos: Mantener personal cualificado, herramientas de última generación y cobertura 24/7 es costoso.
4. Riesgos en la cadena de suministro: El *software* y *hardware* de terceros pueden introducir vulnerabilidades ocultas.

Para abordar estas cuestiones, O'Leary (2019) enfatiza la importancia de integrar el intercambio de inteligencia sobre amenazas, la automatización y la colaboración intersectorial en las estrategias defensivas. En conclusión, las OCD constituyen la columna vertebral de la seguridad digital en el mundo moderno. Combinan resiliencia pasiva y participación activa para proteger activos críticos, garantizar la continuidad operativa y disuadir a los adversarios. Como señala Couretas (2024), la medida del éxito de la ciberdefensa no es la ausencia de ataques, sino la velocidad y la eficacia de la detección, la contención y la recuperación. A medida que los atacantes innovan, también deben hacerlo los defensores, lo que convierte a las OCD en un ámbito esencial y en constante evolución de la seguridad nacional.

La interacción entre la OCO y la OCD es compleja. Por un lado, son opuestos (atacar vs. proteger). Por otro, son interdependientes. Una ciberdefensa eficaz a menudo requiere conocimiento ofensivo. Por ejemplo, para defenderse de las armas cibernéticas de un adversario podría ser necesario comprenderlas analizando *malware* capturado, o incluso, penetrando en las unidades de *hackers* enemigas, una actividad de inteligencia ofensiva. Por el contrario, llevar a cabo una ofensiva de forma segura puede requerir medidas defensivas (como el sigilo y la cobertura para proteger las propias herramientas e infraestructura de la detección o el contraataque).

En la doctrina militar, una capacidad cibernética plenamente desarrollada implica que tanto la OCO como la OCD trabajen en conjunto. Estados Unidos, por ejemplo, creó Fuerzas de Misión Cibernética que incluyen Equipos Nacionales de Misión Cibernética (con un mandato principalmente defensivo, y que protegen la infraestructura crítica cibernética del país), Equipos de Misión de Combate (equipos ofensivos que apoyan a los comandos combatientes para llevar a cabo OCO) y Equipos de Protección Cibernética (principalmente, equipos defensivos que protegen las redes del Departamento de Defensa). Cabe señalar que la existencia de equipos separados subraya que las habilidades ofensivas (explotación de sistemas) y defensivas (fortalecimiento de sistemas y detección de intrusiones) son disciplinas relacionadas, pero distintas.

Los operadores suelen especializarse, aunque existe una superposición, pues la línea entre ataque y defensa puede difuminarse en el ciberespacio. Una acción defensiva podría implicar “contraatacar” la red de un adversario para detener un

ataque. ¿Se trata de ataque o defensa? Algunos argumentan que es una forma de defensa activa o "contraataque cibernético". Asimismo, infiltrarse en una red enemiga para neutralizar preventivamente *malware* dirigido contra uno podría considerarse una defensa avanzada, aunque utilice técnicas ofensivas. Esta ambigüedad se refleja en la doctrina en evolución (que se analiza en la siguiente sección, sobre "defensa avanzada").

Otro matiz es la diferencia en las restricciones legales y políticas. Las OCO, especialmente las que causan daños o interrupciones, a menudo requieren una autorización de alto nivel, ya que pueden equipararse al uso de la fuerza según el derecho internacional. En tiempos de paz, una OCO militar contra otra nación podría violar la soberanía o considerarse un acto de guerra. Por lo tanto, las OCO suelen ser muy controladas, y en ocasiones, encubiertas. Las OCD, en cambio, suelen ser continuas y se consideran parte de la seguridad normal: se espera (y se permite) que cada Estado fortalezca sus propias redes.

Sin embargo, la defensa activa que se extiende a redes externas plantea cuestiones legales. Actualmente, los Estados lidian con las normas sobre qué medidas defensivas son aceptables fuera de su propio territorio (por ejemplo, ¿pueden hackearse los servidores delictivos en otro país para dismantelar una *botnet* que infecta sus computadores?). Dentro de la categorización del Departamento de Defensa de los Estados Unidos existe una tercera categoría distinta de las OCO y las OCD: las Operaciones de la Red de Información del Departamento de Defensa (en inglés, DoDIN, por las iniciales de Department of Defense Information Network), que se encargan, en esencia, de la gestión y protección diarias de las redes militares, una función predominantemente defensiva y administrativa (Aucsmith, 2018). Esto destaca que gran parte del trabajo de "ciberoperaciones" no consiste en elegantes duelos de *hackers*, sino en configurar sistemas, aplicar parches, supervisar registros y capacitar a los usuarios: la higiene de la ciberseguridad que previene ataques exitosos.

Esta línea de base es crucial. Sin ella, incluso las mejores capacidades ofensivas son inútiles si las redes propias se hallan expuestas a los adversarios. Para contextualizar la OCO frente a la OCD, considérese una analogía con los dominios tradicionales: la OCO es como las misiones de ataque de la Fuerza Aérea, mientras que la OCD es como un sistema integrado de defensa aérea que protege el territorio nacional. Clarísimamente, ambos son necesarios: uno proyecta poder en territorio enemigo, y el otro protege el frente interno.

Históricamente, algunos Estados se han centrado en gran medida en la construcción de una “ciberdefensa” (p. ej., cortafuegos robustos, equipos CERT), pero dudaban en desarrollar ciberdefensas ofensivas, por temor a la escalada o a la falta de capacidad. Otros, como Estados Unidos y Rusia, invirtieron en ambas. Asimismo, Israel es conocido por su gran capacidad ofensiva, combinada con una defensa activa. Estados como Irán, inicialmente víctima de ciberataques, construyeron rápidamente unidades ofensivas (p. ej., el comando cibernético del CGRI), pero también reforzaron sus redes tras el ataque con “Stuxnet”.

Desde una perspectiva operativa, la eficacia de las OCO y las OCD puede medirse de forma diferente. En el ámbito cibernético, la ofensiva suele ser más fácil de ejecutar que la defensa. Es un dicho común que el atacante solo necesita encontrar una vulnerabilidad, mientras el defensor debe asegurarlas todas. De hecho, la ofensiva disfruta de la iniciativa y la sorpresa. Sin embargo, un intento ofensivo fallido puede pasar desapercibido (si fracasa discretamente), mientras que una defensa fallida es obvia (se produce una brecha). Por otro lado, en operaciones sostenidas el defensor puede adaptarse y contener el daño, mientras que el atacante, una vez descubierto, puede perder su posición. Esta dinámica del gato y el ratón es continua.

Tabla 2. Operaciones cibernéticas ofensivas vs. defensivas

Categoría	Operaciones Cibernéticas Ofensivas (OCO; en inglés, <i>Offensive Cyber Operations</i>)	Operaciones Cibernéticas Defensivas (OCD; en inglés, <i>DCO</i> , por las iniciales de <i>Defensive Cyber Operations</i>)
Definición	Acciones deliberadas para proyectar poder y lograr objetivos políticos, militares o económicos mediante la degradación, negación, interrupción, destrucción o manipulación de sistemas e información del adversario (Courteas, 2024; O'Leary, 2019)	Acciones destinadas a detectar, proteger y responder frente a amenazas cibernéticas, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de los sistemas (Courteas, 2024; O'Leary, 2019)
Objetivo principal	Lograr una ventaja estratégica o táctica sobre los adversarios; imponer costos o moldear su comportamiento	Garantizar la protección continua de las redes propias; prevenir y mitigar ataques, y recuperarse de estos
Acciones típicas	• Robo de datos (espionaje) • Interrupción de sistemas (ataques DDoS) • Sabotaje a infraestructuras (ej., Stuxnet) • Campañas de desinformación	• Firewalls; IDS/IPS; antivirus • Monitoreo y detección de amenazas • Gestión de parches y vulnerabilidades • Respuesta y recuperación ante incidentes
Fases/tácticas	Reconocimiento → Armado → Entrega → Explotación → Instalación → Comando y Control (C2) → Acciones sobre el objetivo (Courteas, 2024; O'Leary, 2019).	Inteligencia de amenazas → Evaluación de riesgos → Fortalecimiento de defensas → Monitoreo continuo → Detección de incidentes → Contención → Recuperación (O'Leary, 2019)

Continúa en la otra página

Categoría	Operaciones Cibernéticas Ofensivas (OCO; en inglés, <i>Offensive Cyber Operations</i>)	Operaciones Cibernéticas Defensivas (OCD; en inglés, <i>DCO</i> , por las iniciales de <i>Defensive Cyber Operations</i>)
Ejemplos	• Ciberataques de Rusia a Ucrania • Operación Titan Rain, de China • Campañas de <i>ransomware</i> de Corea del Norte (ej., "WannaCry") • Uso de herramientas cibernéticas por ISIS	• Defensa de redes del Comando Cibernético de los Estados Unidos • Respuesta de CERT a ataques de <i>ransomware</i> • Defensa corporativa contra <i>phishing</i> y <i>malware</i> (Courteas, 2024; O'Leary, 2019)
Actores clave	• Actores estatales; comandos cibernéticos; grupos APT; hacktivistas; sindicatos criminales	• CERT nacionales; unidades militares de ciberdefensa; centros de operaciones de seguridad (SOC) del sector privado
Contexto legal/ético	Suele operar en zonas grises legales; plantea preguntas sobre soberanía, proporcionalidad y efectos colaterales	Generalmente amparado en leyes nacionales e internacionales; enfocado en la protección legítima de activos

Fuente: elaboración propia, con base en Couretas (2024) y O'Leary (2019).

Como lo muestra la tabla 2, la comparación entre las OCO y las OCD destaca la naturaleza dual del ciberconflicto moderno. Las OCO buscan proyectar poder e imponer costos a los rivales mediante ataques deliberados, mientras que las OCD buscan proteger los sistemas críticos mediante la detección, prevención y mitigación de amenazas. Y mientras las OCO aprovechan tácticas como la implementación de *malware*, el robo de datos y la interrupción del sistema, las OCD se basan en defensas estratificadas, monitoreo continuo y respuesta a incidentes para garantizar la resiliencia. En conclusión, las OCO y las OCD son dos caras de la ciberguerra: unas están centradas en atacar a los adversarios a través del ciberespacio, y las otras, en proteger y responder a los ataques. Como afirman Couretas (2024) y O'Leary (2019), ambos dominios son componentes clave de la estrategia cibernética nacional, lo que refleja una interacción dinámica entre ataque y defensa en un entorno digital global y altamente contestado. En consecuencia, los comandos cibernéticos modernos las consideran misiones complementarias.

Ciberarmas, tácticas y preparación para operaciones

Las ciberoperaciones abarcan un conjunto diverso y sofisticado de actividades que combinan armas, tácticas y preparación operativa para lograr objetivos estratégicos y tácticos. En lo referente a las ciberarmas, estas abarcan desde *malware* hasta herramientas sofisticadas, como bombas lógicas, gusanos, *exploits* de día cero y *ransomware*. Por consiguiente, las ciberarmas están diseñadas para violar, degradar, interrumpir o manipular los sistemas del adversario (Couretas, 2024).

El *malware* (*software* malicioso) es un término general que se refiere a cualquier *software* diseñado intencionalmente para dañar computadores, redes o usuarios. Incluye una amplia gama de códigos maliciosos, como virus, gusanos, troyanos, *ransomware* y *spyware*. El *malware* generalmente viola los sistemas para robar datos, espiar a los usuarios, interrumpir los servicios o establecer un control no autorizado (Couretas, 2024). Por ejemplo, el virus "ILOVEYOU" (2000) se propagó globalmente por correo electrónico, sobrescribió archivos y causó miles de millones de dólares en daños.

Una bomba lógica es un fragmento de código malicioso incrustado en *software* o sistemas legítimos que se activa solo cuando se cumplen condiciones específicas, como una fecha determinada, la eliminación de un archivo o la acción del usuario. Una vez activada, una bomba lógica puede eliminar archivos, bloquear sistemas o deshabilitar funciones críticas. Por ejemplo, en 2006 un contratista informático descontento con una aseguradora instaló una bomba lógica en los sistemas de la empresa, lo que causó daños por 3 millones de dólares, al eliminar archivos críticos tras su renuncia.

A diferencia de los virus, los gusanos son programas autorreplicantes que se propagan por redes sin necesidad de un archivo *host* ni de la intervención humana. Los gusanos explotan vulnerabilidades en sistemas o *software* para moverse de forma autónoma, lo que a menudo causa interrupciones generalizadas y consume ancho de banda. Por ejemplo, el gusano "Conficker" (2008) infectó millones de computadores en todo el mundo creando una enorme *botnet*.

Por su parte, un *exploit* de "día cero" busca atacar una vulnerabilidad de *software* previamente desconocida que los desarrolladores no han tenido tiempo de parchear. Estos *exploits* son muy valiosos tanto para los ciberdelincuentes como para los Estados nación, ya que permiten a los atacantes vulnerar los sistemas sin ser detectados. Los *exploits* de "día cero" suelen combinarse con *malware* o distribuirse mediante campañas de *phishing*. El gusano "Stuxnet" utilizó múltiples vulnerabilidades de "día cero" para propagarse y dañar las centrifugadoras nucleares de Irán, por lo cual se convirtió en la primera ciberarma conocida con efectos físicos y cinéticos (Couretas, 2024).

El *ransomware* cifra los datos de la víctima o la bloquea de sus sistemas, y exige un pago (generalmente, en criptomonedas) por las claves de descifrado o la restauración del acceso. Se ha convertido en una de las formas de ciberdelincuencia más lucrativas y disruptivas, utilizada tanto por grupos criminales como, en ocasiones, por actores alineados con los Estados. El brote de *ransomware*

"WannaCry" (2017) afectó a más de 200.000 sistemas en 150 países paralizando hospitales, empresas y organismos gubernamentales. El ataque se atribuyó posteriormente a actores norcoreanos.

Una preocupación clave es el desafío de evitar daños colaterales. A diferencia de otras formas de armamento, las armas cibernéticas no son intrínsecamente indiscriminadas, ya que pueden diseñarse para objetivos altamente específicos si se respaldan con suficiente inteligencia y rigor técnico. Por ejemplo, "Stuxnet" demostró la posibilidad de operaciones cibernéticas con objetivos específicos, centrándose en centrifugadoras iraníes y minimizando los efectos no deseados (Bellovin et al., 2018). Sin embargo, el riesgo de proliferación es considerable, ya que una vez es desplegada un arma cibernética, los adversarios o terceros pueden estudiarla, aplicarle ingeniería inversa y reutilizarla. Esto aumenta la importancia de que diseñadores y legisladores consideren medidas de no proliferación junto con los objetivos operacionales.

Y a diferencia de los campos de batalla tradicionales (tierra, mar, aire), el dominio ciberespacial está fuertemente privatizado, con infraestructuras, plataformas y servicios críticos en gran medida en manos comerciales. Los actores privados no solo se enfrentan a ataques, sino que también poseen capacidades ofensivas. Esto plantea complejos debates legales y éticos en torno al "contraataque", en el que las empresas toman represalias contra los atacantes, lo cual difumina en ocasiones la línea entre defensa y ataque (Kello, 2018).

Tabla 3. Principales armas y tácticas cibernéticas

Categoría	Arma/táctica	Descripción	Ejemplo conocido
Malware	Virus	Código malicioso que se adjunta a archivos ejecutables y se propaga al activarse	"ILOVEYOU" (2000); "Melissa" (1999)
	Gusanos (worms)	Programas autónomos que se replican a través de redes sin intervención humana	"Morris Worm" (1988); "Conficker" (2008)
	Troyanos	Programas que se disfrazan de software legítimo para instalar <i>malware</i> u obtener acceso no autorizado	"Zeus"; "Emotet"
	Ransomware	<i>Malware</i> que cifra archivos del sistema de la víctima y exige un rescate para liberarlos	"WannaCry" (2017); "Petya/NotPetya" (2017)
	Wipers	<i>Malware</i> diseñado para destruir datos y sistemas, y no para obtener beneficios financieros	"Shamoon" (2012, 2016); "StoneDrill"

Continúa en la otra página

Categoría	Arma/táctica	Descripción	Ejemplo conocido
Ataques a redes	DDoS (<i>Distributed Denial of Service</i>)	Sobrecarga de servidores o redes mediante tráfico masivo, para causar interrupciones	Ataque DDoS a Estonia (2007); "Dyn DNS" (2016)
Explotación de vulnerabilidades	Zero-Day Exploits	Ataques que aprovechan vulnerabilidades desconocidas para los desarrolladores, antes de que exista un parche	"Stuxnet"; "EternalBlue" (utilizado en "WannaCry")
Ataques a la cadena de suministro	Supply chain attacks	Compromiso de software, hardware o servicios de terceros para penetrar en el objetivo final.	SolarWinds (2020)
Herramientas de espionaje	Keyloggers	Software que registra pulsaciones del teclado para robar credenciales o datos sensibles	Agent Tesla, FormBook
	Sniffers	Herramientas que capturan tráfico de red para obtener datos no cifrados.	"Wireshark" (en contextos maliciosos)
	Phishing	Correos electrónicos o mensajes falsos que engañan al usuario para revelar datos o descargar <i>malware</i>	Campañas contra bancos o agencias gubernamentales
	Spear phishing	Variante dirigida de <i>phishing</i> , personalizada para un individuo o institución en concreto	Hackeo al DNC (2016)
	Baiting	Ofrecer algo atractivo (USB infectados, enlaces) para atraer víctimas a ejecutar <i>malware</i>	USB infectados abandonados en espacios públicos
Tácticas avanzadas	APT (<i>Advanced Persistent Threats</i>)	Grupos altamente organizados y persistentes, normalmente estatales, que infiltran redes durante largos periodos para espionaje o sabotaje	"APT28" (Rusia); "APT29" (Rusia); "APT10" (China)
	Living off the land (LotL)	Uso de herramientas legítimas del sistema (como PowerShell) para moverse lateralmente y evitar la detección	Uso de PsExec, WMIC o PowerShell en ataques APT
Ataques híbridos	Ciber-psicológicos/desinformación	Uso de redes sociales, <i>bots</i> y contenido falso para influir en la opinión pública o desestabilizar sociedades	Interferencia rusa en las elecciones (Estados Unidos, 2016)

Fuente: elaboración propia.

La tabla 3 resume las armas y tácticas más relevantes utilizadas en conflictos cibernéticos contemporáneos. Como destaca Couretas (2024), su combinación (por ejemplo, *malware* más ingeniería social o ataques DDoS coordinados con campañas de desinformación) refleja el carácter híbrido, estratégico y adaptativo de la guerra cibernética actual. Tácticamente, los actores utilizan la ingeniería social (p. ej., *phishing*), ataques a la cadenas de suministro, *botnets* y amenazas persistentes avanzadas (en inglés, APT, por las iniciales de *Advanced Persistent*

Threat) para infiltrarse en redes, establecer persistencia y mantener el control durante largos periodos (Oakley, 2019). La ingeniería social consiste en manipular el comportamiento humano para obtener acceso no autorizado a información o sistemas. Una de sus formas más comunes es el *phishing*, en el que los atacantes envían correos electrónicos o mensajes engañosos que parecen provenir de fuentes confiables. El objetivo es engañar a los destinatarios para que revelen información confidencial (como contraseñas) o hagan clic en enlaces maliciosos que implementan *malware* (Oakley, 2019). Por ejemplo, en el ataque al Comité Nacional Demócrata (en inglés, DNC, por las iniciales de Democratic National Committee), de Estados Unidos, en 2016, agentes rusos utilizaron correos electrónicos de *phishing* selectivo para obtener credenciales de figuras políticas clave, lo que finalmente influyó en unas elecciones mediante filtraciones de datos.

Por su parte, los ataques a la cadena de suministro, o *supply-chain attacks*, se dirigen a proveedores externos, proveedores de servicios o proveedores de *software* que tienen acceso a la red de la víctima final. Al comprometer a un proveedor confiable, los atacantes pueden infiltrarse en múltiples sistemas secundarios con un riesgo mínimo de detección. El ataque "SolarWinds" (2020) comprometió una actualización rutinaria de software de la plataforma SolarWinds Orion, lo que permitió a grupos rusos de Amenazas Persistentes Avanzadas (en inglés, APA, por las iniciales de *Advanced Persistent Threat*) vulnerar las redes gubernamentales y privadas de Estados Unidos en diversos sectores. Ese ataque ilustró cómo las interdependencias en los ecosistemas digitales pueden utilizarse como arma para lograr objetivos de alto valor (Oakley, 2019).

Las *botnets* son redes de computadores comprometidas (llamadas *bots* o *zombies*), controladas a distancia por un atacante. Estas redes pueden incluir millones de dispositivos infectados en todo el mundo, lo que permite a los agresores realizar ataques de denegación de servicio distribuido (DDoS), enviar *spam* o propagar *malware* a gran escala. Por ejemplo, la *botnet* "Mirai" (2016) aprovechó dispositivos inseguros del IoT para lanzar ataques DDoS de récord contra proveedores de DNS como Dyn interrumpiendo el acceso a importantes sitios web como Twitter, Netflix y Airbnb.

Las APA son adversarios sofisticados, patrocinados por Estados o con abundantes recursos, que se infiltran en las redes y mantienen un acceso encubierto a largo plazo. Las APA utilizan una combinación de ingeniería social, *malware*, *exploits* de "día cero" y movimiento lateral a través de las redes, para recopilar inteligencia discretamente, exfiltrar datos o preparar sistemas para sabotajes.

Por ejemplo, “APA28” (“Fancy Bear”), una unidad de inteligencia militar rusa, ha sido vinculada a campañas de ciberespionaje contra la OTAN, Ucrania y el Comité Nacional Demócrata de los Estados Unidos. Las APA son conocidas por su persistencia, ya que a menudo permanecen sin ser detectadas en las redes durante meses o, incluso, años, ajustando sus tácticas a medida que los defensores mejoran la seguridad (Oakley, 2019).

Cada una de estas tácticas desempeña un papel decisivo en el panorama general de las ciberamenazas. La ingeniería social explota la confianza humana, los ataques a la cadena de suministro eluden las defensas directas, las *botnets* proporcionan escala y potencia, y las APA ofrecen persistencia y alcance estratégico. Juntos, permiten a los atacantes no solo infiltrarse en las redes, sino también establecer un control duradero, adaptarse a las defensas y lograr objetivos operativos a largo plazo, razón por la cual son clave para el estudio de la ciberguerra. Como destaca Richards (2014), las cibertácticas difuminan cada vez más las fronteras entre espionaje, sabotaje y guerra cognitiva, lo que pone de relieve la necesidad de una planificación integrada en los ámbitos político, militar y de inteligencia.

Tras describir la gama de armas y tácticas cibernéticas disponibles para actores estatales y no estatales resulta evidente que su uso exitoso raramente es espontáneo. En cambio, las OCO exigen una preparación técnica y operativa meticulosa. Sin la crucial base de la recopilación de inteligencia, el análisis de objetivos y la configuración del entorno, incluso las herramientas cibernéticas más sofisticadas corren el riesgo de fallar o, peor aún, ser detectadas. Por lo tanto, comprender la fase preparatoria es esencial para comprender cómo las operaciones cibernéticas logran precisión e impacto.

La inteligencia, vigilancia y reconocimiento (IVR) en el ámbito cibernético se refiere a la recopilación, el análisis y la difusión sistemáticos de información sobre redes, sistemas y personal del adversario. A diferencia de la IVR tradicional, basada en satélites, sensores o informantes humanos, la IVR cibernética aprovecha medios digitales para mapear topologías de red, identificar vulnerabilidades del sistema, comprender patrones de comunicación y recopilar metadatos o credenciales (Inglis, 2018). Esta fase es decisiva para el éxito de las operaciones cibernéticas, ya que permite a los atacantes adaptar sus herramientas y estrategias a las características específicas del entorno objetivo. Por ejemplo, sin saber qué sistemas operativos se utilizan, qué protecciones antivirus están instaladas o quién administra las redes, los atacantes se arriesgan a ser detectados o a sufrir un fallo.

Por consiguiente, una IVR cibernética eficaz ayuda a los atacantes a identificar puntos débiles, priorizar objetivos y evaluar el posible impacto de sus acciones.

Antes del ataque “Stuxnet” a la central nuclear iraní de Natanz, se cree que los atacantes realizaron una exhaustiva investigación de seguridad (IVR), que incluyó la recopilación de detalles sobre los controladores PLC de Siemens, las configuraciones de las centrífugas, e incluso, la cadena de suministro utilizada para instalar los equipos. Esta meticulosa recolección de datos de inteligencia permitió a los atacantes diseñar *malware* con efectos destructivos precisos, en vez de causar daños indiscriminados (Inglis, 2018).

La Preparación Operativa del Entorno (POE) es la fase en la que los atacantes pasan de la recopilación de inteligencia a la preparación del campo de batalla para las operaciones reales. Esto implica acciones encubiertas realizadas dentro del entorno objetivo para posicionar activos, establecer puntos de apoyo y configurar las condiciones para futuros ataques, sin activar la detección. Las actividades de OPE pueden incluir (Inglis, 2018):

1. Obtener acceso inicial (mediante *phishing*, ataques a la cadena de suministro o explotación de vulnerabilidades).
2. Instalar puertas traseras o *shells web* para permitir el acceso persistente.
3. Preposicionar *malware* que permanece inactivo hasta su activación; establecimiento de canales de Comando y Control (C2) para la gestión remota de sistemas infectados.
4. Mapeo de redes internas, para facilitar el movimiento lateral una vez iniciada la fase de ataque.

El objetivo de la OPE es sentar las bases para una acción rápida y eficaz durante la fase de explotación o ataque minimizando el riesgo operativo y maximizando el impacto. Por ejemplo, antes del ataque ruso “NotPetya”, en 2017, se cree que los atacantes se infiltraron en el *software* de contabilidad ucraniano y prepararon la distribución de *malware* destructivo de borrado a través de canales de actualización confiables. Esta fase de preparación discreta les permitió detonar el ataque a gran escala, interrumpir la infraestructura crítica ucraniana e impactar inadvertidamente a empresas multinacionales de todo el mundo. Con base en lo anterior, las actividades de IVR y POE son indispensables en las operaciones cibernéticas modernas. Sin inteligencia precisa, los atacantes corren el riesgo de desperdiciar recursos o ser detectados prematuramente. Sin una preparación exhaustiva, incluso los ataques bien planificados pueden fracasar o no lograr los objetivos

estratégicos. Como destaca Inglis (2018), la integración perfecta de IVR y POE se ha convertido en un sello distintivo de los actores cibernéticos sofisticados, al permitir operaciones que van desde disrupciones tácticas hasta decisiones políticas estratégicas.

Pero si bien la preparación técnica sienta las bases para la acción, el verdadero poder de las operaciones cibernéticas reside en los efectos que generan a nivel tanto estratégico como táctico. Ya sea que busquen paralizar la infraestructura nacional o deshabilitar una red en el campo de batalla, las campañas cibernéticas están diseñadas no solo para penetrar sistemas, sino para producir resultados mensurables alineados con objetivos políticos, militares o económicos. Examinar estos efectos nos permite evaluar cómo las capacidades cibernéticas moldean el comportamiento de los adversarios e influyen en el curso de conflictos más amplios.

Las operaciones cibernéticas ejercen influencia en múltiples niveles de conflicto configurando tanto las condiciones inmediatas del campo de batalla como la dinámica geopolítica a largo plazo. Según señalan académicos como Couretas (2024) y Sanger (2018), la flexibilidad y escalabilidad de las herramientas cibernéticas les permiten producir efectos que abarcan desde disrupciones tácticas hasta estrategias de gobierno. Para comprender de manera sistemática cómo las operaciones cibernéticas producen efectos diferenciados en los conflictos contemporáneos resulta útil conceptualizarlas a través de un esquema de escalamiento que distinga entre niveles táctico, operacional y estratégico (tabla 4). Esta diferenciación no implica compartimentos estancos, sino un continuo dinámico en el cual acciones técnicas de bajo nivel pueden acumularse, coordinarse y amplificarse hasta generar consecuencias políticas, económicas o militares de alto impacto. El ciberespacio, por su flexibilidad, ambigüedad y bajo costo de entrada, facilita especialmente esta progresión escalonada de efectos.

Tabla 4. Escalamiento cibernético por niveles de guerra (táctico-operacional-estratégico)⁴

Nivel	Finalidad	Forma típica	Alcance	Indicadores de efecto	Ejemplos
Táctico	Ventaja inmediata/disrupción específica	DDoS; intrusión limitada; degradación local; engaño técnico	Unidad/objetivo específico	Interrupción breve; confusión local; ventaja momentánea	DDoS y defacement en Georgia (2008); efectos específicos contra comunicaciones
Operacional (campana)	Degradar capacidades y condicionar operaciones en el tiempo	APT; sabotaje persistente; preposición; manipulación de datos; coerción digital sostenida	Sector/teatro /función crítica	funcional prolongada; presión institucional; sincronización con otras líneas (info/cinético)	"NotPetya" (2017) como disrupción de campana; "Shamoon" (2012/2016)
Estratégico	Logro de objetivos políticos mayores (coacción, disuasión, deslegitimación)	Ataques a infraestructura crítica; interferencia política; campañas híbridas integradas	Sistema nacional /orden político	Crisis nacional; erosión de legitimidad; impacto geopolítico	ataques a red eléctrica ucraniana (2015/2016); interferencia electoral (2016)

Fuente: elaboración propia, con base en Couretas (2024), Sanger (2018), Farrell y Glaser (2018).

El esquema de escalamiento mostrado en la tabla 4 permite entender por qué las operaciones cibernéticas son especialmente funcionales en las guerras G5G: su capacidad para operar de forma incremental, ambigua y acumulativa permite a los actores modular la intensidad del conflicto, permanecer por debajo del umbral de la guerra convencional y, al mismo tiempo, producir efectos estratégicos significativos. En este sentido, el ciberespacio no solo amplía el repertorio táctico de los actores, sino que redefine la relación entre medios, niveles de conflicto y objetivos políticos. Desde la lógica de la zona gris, la ciberguerra obra como un mecanismo privilegiado de escalamiento controlado, en el cual acciones en apariencia tácticas pueden adquirir relevancia operacional, o incluso estratégica, mediante su acumulación, sincronización y persistencia en el tiempo. Esta dinámica de escalamiento gradual (sintetizada en la tabla 4) explica por qué las operaciones cibernéticas resultan especialmente funcionales para la coerción, la disuasión ambigua y la presión política sostenida sin recurrir a la violencia armada abierta.

⁴ El escalamiento se define por finalidad político-militar, alcance sistémico y duración del efecto (y no por complejidad técnica).

A partir de esta lógica de escalamiento controlado, resulta analíticamente útil distinguir entre efectos cibernéticos estratégicos y efectos cibernéticos táctico-operacionales, no como categorías cerradas o mutuamente excluyentes, sino como niveles funcionales de impacto dentro de un mismo continuo de conflicto. En el ciberespacio (y particularmente, en escenarios de zona gris), una misma acción puede adquirir significados distintos según su alcance temporal, su acumulación, su articulación con otras herramientas de poder y su incidencia sobre los procesos de decisión del adversario. Esta distinción permite clarificar cómo las operaciones cibernéticas contribuyen tanto a lograr objetivos inmediatos en el campo de batalla como a la configuración gradual del entorno estratégico.

Los efectos cibernéticos estratégicos se refieren a operaciones destinadas a lograr resultados a largo plazo y de alto nivel, a menudo con trascendencia política, económica o militar más allá del objetivo inmediato. Estos incluyen:

1. Alterar la infraestructura nacional (p. ej., redes eléctricas, sistemas bancarios, redes de transporte).
2. Socavar la estabilidad política (p. ej., sembrar desconfianza pública en las instituciones gubernamentales).
3. Lograr influencia geopolítica (p. ej., coaccionar a adversarios o cambiar alianzas).

Por ejemplo, los ataques rusos a las redes energéticas ucranianas (en particular, los ataques “BlackEnergy” e “Industroyer”, de 2015 y 2016) demostraron la capacidad de las operaciones cibernéticas para dejar paralizadas infraestructuras críticas generando apagones y agitación económica (Sanger, 2018). De igual manera, la interferencia rusa en las elecciones estadounidenses y europeas mediante hackeos, filtraciones y campañas de desinformación refleja el uso de las operaciones cibernéticas como instrumentos de guerra política, con el objetivo de erosionar la confianza pública, exacerbar las divisiones sociales y debilitar la legitimidad de las instituciones democráticas (Couretas, 2024). Es importante destacar que la naturaleza estratégica de dichas operaciones cibernéticas a menudo implica que sus efectos son indirectos, acumulativos y están diseñados para moldear el comportamiento del adversario a lo largo del tiempo, en vez de asestar un golpe decisivo.

A nivel táctico u operativo, las operaciones cibernéticas están diseñadas para lograr objetivos militares más inmediatos, a menudo en apoyo directo de operaciones de combate o misiones de inteligencia en curso. Los ciberefectos tácticos pueden incluir:

1. Negar o degradar las comunicaciones de un adversario en el campo de batalla.
2. Desactivar los sistemas de mando y control (C2).
3. Interrumpir las plataformas logísticas o de armas.
4. Realizar operaciones psicológicas contra las fuerzas de primera línea.

Un ejemplo clave es la Operación *Glowing Symphony* (2016), de Estados Unidos, cuyo objetivo era la infraestructura mediática del Estado Islámico (ISIS), incluyendo sitios web, cuentas de redes sociales y plataformas de comunicación. En este sentido, al degradar la maquinaria de propaganda de ISIS, la operación complementó los esfuerzos militares convencionales y disminuyó la capacidad del grupo para reclutar, coordinar y difundir su mensaje globalmente (Sanger, 2018; Couretas, 2024). Otro caso ilustrativo es la Operación *Orchard* (2007), de Israel, donde, según se informa, las fuerzas israelíes utilizaron herramientas cibernéticas para desactivar los radares de defensa aérea sirios, lo que permitió a los aviones de combate destruir un presunto reactor nuclear sin ser detectados. Esta operación demostró cómo los ciberefectos pueden generar ventajas tácticas temporales permitiendo acciones cinéticas precisas sin escalar hacia un conflicto más amplio.

Las operaciones cibernéticas estratégicas y tácticas suelen estar interconectadas. Una disrupción táctica exitosa (p. ej., la desactivación de las defensas aéreas o las redes de medios) puede tener un efecto dominó estratégico, e influir, por lo tanto, en la toma de decisiones del adversario o socavar su estrategia de disuasión. Por el contrario, las campañas estratégicas (p. ej., la interferencia electoral), pueden basarse en una serie de acciones tácticas coordinadas (como ataques de *phishing*, filtraciones de datos, operaciones de influencia). Como destacan Farrell y Glaser (2018), esta naturaleza multidimensional de las operaciones cibernéticas desafía las distinciones tradicionales entre guerra y paz, frentes y retaguardia, así como de los ámbitos militares y civiles.

Entonces, comprender las dimensiones estratégicas y tácticas de las operaciones cibernéticas es clave para evaluar su papel en la competencia de seguridad contemporánea. Las armas cibernéticas no son meras herramientas técnicas: son instrumentos de poder que configuran el orden global, la resiliencia nacional y los resultados en el campo de batalla por igual. Por consiguiente, los encargados de formular políticas y los planificadores militares deben abordar las operaciones cibernéticas no solo como desafíos técnicos, sino como elementos centrales de la estrategia moderna.

En general, las operaciones cibernéticas representan una interacción en constante evolución entre innovación tecnológica, ingenio táctico y ambición estratégica. Al combinar las armas cibernéticas, la inteligencia, la seguridad y la operación operativa con objetivos estratégicos y tácticos claros, tanto los actores estatales como los no estatales están transformando la naturaleza de los conflictos en el siglo XXI. Como advierte Richards (2014), la continua integración de capacidades cibernéticas en las estrategias de seguridad nacional genera oportunidades y profundos desafíos éticos, legales y de estabilidad. Se hace evidente que la integración de las capacidades cibernéticas en las estrategias de seguridad nacional plantea no solo desafíos operativos, sino también profundas preguntas sobre la estabilidad internacional, la ética y el futuro de la guerra.

Actores estatales globales en la ciberguerra

La ciberguerra patrocinada por los Estados se ha vuelto un componente central de la estrategia moderna de seguridad internacional. Las principales potencias participan cada vez más en operaciones cibernéticas que tienen como objetivo tanto los sistemas tecnológicos como la dimensión humana del ciberespacio. El ciberespacio es un “entorno intangible donde los individuos [...] interactúan para satisfacer diferentes intereses” (Jones-Chaljub, 2022, p. 12). Por lo tanto, la ciberguerra parece abarcar las vulnerabilidades técnicas y la influencia psicológica, ya que, en última instancia, “el usuario final en el ciberespacio será una persona de carne y hueso” (p. 11).

Las principales potencias cibernéticas (Estados Unidos, Rusia, China, Corea del Norte e Irán) tienen doctrinas y objetivos distintos en ese ámbito. Sus operaciones abarcan desde ataques disruptivos a infraestructura crítica hasta el espionaje cibernético y campañas de influencia. Estados como Colombia, menos estudiados en el contexto global, también están formulando estrategias de ciberseguridad y ciberdefensa para proteger sus intereses nacionales (ESDEG, 2020), pues a medida que se expande la infraestructura digital de Colombia también crece su exposición a las ciberamenazas, desde redes criminales transnacionales hasta actores estatales hostiles.

La rápida evolución de las TIC ha obligado a los Estados a replantear los modelos tradicionales de defensa y seguridad, por lo que la ciberdoctrina se ha vuelto un componente crucial de la política de seguridad nacional encapsulando principios y estrategias que guían las acciones de los Estados en el ciberespacio. Como

explican Colarik y Janczewski (2019), la ciberdoctrina integra principios políticos, legales y militares para formular respuestas coherentes a los desafíos que plantean las operaciones en el ciberespacio. Mientras que la doctrina ambiental se centra en las características únicas de los sistemas de información, las redes informáticas y las infraestructuras físicas, la doctrina organizativa se centra en la adaptación de las estructuras militares a las operaciones en el ciberespacio.

Uno de los principales desafíos en el desarrollo de una doctrina cibernética es definir la frontera entre guerra cibernética y guerra tradicional, ya que sin una distinción clara resulta difícil determinar cuándo y cómo aplicar respuestas justificadas, racionales y proporcionales a los ciberataques (Colarik & Janczewski, 2019). El desarrollo de una doctrina cibernética también exige un enfoque sistémico que integre componentes civiles y militares. Como señalan Colarik y Janczewski (2019), los esfuerzos actuales suelen estar fragmentados, con los sectores civil y militar trabajando en paralelo, pero sin una integración suficiente. Por lo tanto, una doctrina cibernética integral debe abordar los principios de autodefensa nacional, proteger la infraestructura civil y militar, guiar las operaciones militares y proporcionar un marco para las relaciones internacionales y la disuasión cibernética. En otras palabras, la doctrina cibernética es indispensable para la política de seguridad contemporánea, pues a medida que las ciberamenazas aumentan en complejidad e impacto, los actores estatales deberán invertir en el desarrollo de doctrinas resilientes, adaptables y alineadas con sus objetivos estratégicos más amplios.

Doctrinas cibernéticas en evolución: de la defensa pasiva a la defensa avanzada

La llegada del ciberespacio como ámbito decisivo de conflicto ha transformado las concepciones tradicionales del poder y la doctrina en asuntos militares. El ciberpoder (a menudo definido como la capacidad para aprovechar el ciberespacio para generar ventajas nacionales e influir en los acontecimientos globales) se ha vuelto fundamental en los paradigmas de seguridad (Bebber, 2017). Asimismo, Realpe (2025) sitúa el ciber poder en el marco más amplio de la competencia geopolítica, y señala que su naturaleza intangible oculta sus consecuencias tangibles para la seguridad, la economía y la soberanía del Estado. En ese orden de ideas, Bebber (2017) profundiza en el ciberpoder proponiendo un marco de doble nivel: el "ciberpoder potencial" y la "cibereficacia". El ciberpoder potencial se basa en los recursos humanos y materiales de un Estado (infraestructura tecnológica, personal cualificado y capacidad institucional), mientras que la cibereficacia es la

capacidad para traducir dichos recursos en resultados prácticos en el ciberespacio. Esta distinción refleja la máxima militar tradicional de que el poder material debe organizarse y emplearse eficazmente para obtener ganancias estratégicas.

Un componente crucial de la cibereficacia es la integración del ciberpoder en las doctrinas estratégicas, operativas y tácticas más amplias de un Estado nación. Según Ormrod y Turnbull (2016), la doctrina militar no es un simple conjunto de reglas, sino un marco conceptual que vincula los objetivos estratégicos con las realidades operativas, y garantiza así la coherencia en todos los niveles de intervención. La ciberdoctrina, en particular, debe abordar la naturaleza dinámica e ilimitada del ciberespacio distinguiéndolo de los ámbitos de la guerra convencional, como la tierra, el mar y el aire (Ormrod & Turnbull, 2016). En ese sentido, la doctrina desempeña una doble función en las ciberoperaciones. En primer lugar, estandariza los procedimientos y las tácticas de defensa y ataque, para garantizar que las fuerzas militares puedan responder de forma cohesionada a los incidentes cibernéticos. En segundo lugar, proporciona una perspectiva conceptual a través de la cual se comprenden y anticipan los conflictos cibernéticos. Como señalan Ormrod y Turnbull (2016), la doctrina fundamenta las decisiones sobre si el ciberespacio se trata como un ámbito distinto o como parte de operaciones de información más amplias, con implicaciones para la estructura de la fuerza y la planificación operativa.

Bebber (2017) subraya que una doctrina cibernética eficaz debe integrar atributos clave: capacidad de respuesta (adaptabilidad a amenazas en constante evolución), habilidad (competencia técnica de las fuerzas cibernéticas), calidad (infraestructura y herramientas), integración (alineación de políticas, estrategias y tácticas) y reputación (percepción de la capacidad cibernética por parte de los adversarios). Dichos factores, en conjunto, determinan la cibereficacia de un Estado y su capacidad para disuadir a los adversarios o lograr objetivos estratégicos.

Un ejemplo ilustrativo es el Comando Cibernético de los Estados Unidos, que reconoció formalmente el ciberespacio como un dominio bélico similar a la tierra, el mar y el aire. Sin embargo, el desarrollo de la doctrina cibernética militar está plagado de desafíos. Ormrod y Turnbull (2016) señalan discrepancias en la conceptualización de la ciberguerra por parte de diferentes Estados. Por ejemplo, mientras la OTAN enfatiza la defensa colectiva y la resiliencia a través de su Centro de Excelencia Cooperativo de Ciberdefensa (en inglés, CCDCOE, por las iniciales de Cooperative Cyber Defence Centre of Excellence), países como China y Rusia consideran las cibercapacidades como parte integral de sus estrategias más amplias de guerra

de la información, combinando ciberataques con campañas psicológicas y de propaganda (Ormrod & Turnbull, 2016). Una idea central de Ormrod y Turnbull (2016) es que la doctrina militar debe ser adaptativa y reflejar los imperativos políticos nacionales, ya que la doctrina estática o adoptada en su totalidad de otros Estados corre el riesgo de volverse irrelevante ante la rápida evolución de las amenazas. Ello se hizo evidente a principios de la década de 2000, cuando varios Estados tuvieron dificultades para incorporar las ciberamenazas en su planificación militar, lo que generó vulnerabilidades que los adversarios explotaron rápidamente.

En este orden de ideas, la trayectoria de las doctrinas cibernéticas en las últimas dos décadas muestra una marcada evolución desde un enfoque inicial en la defensa pasiva y reactiva hacia estrategias más asertivas e integradas, ejemplificadas por la “defensa avanzada”. En los inicios de la ciberestrategia muchos Estados trataban el ciberespacio como un dominio para proteger, haciendo hincapié en los cortafuegos, los antivirus y la respuesta a incidentes (defendiéndose dentro de las propias redes). Según Buchanan (2020), los comandos cibernéticos estatales, cuando existían, solían operar con restricciones, y la ciberdefensa ofensiva se mantenía en secreto y se utilizaba con moderación. Sin embargo, a medida que las ciberamenazas se multiplicaban y se entrelazaban con la seguridad nacional, las doctrinas se adaptaron.

La doctrina estadounidense en ciberdefensa, replicada de forma similar por otros Estados occidentales, aboga por operaciones preventivas y continuas para enfrentar las amenazas lo más lejos posible de su propia infraestructura cibernética. Ese cambio, de una postura de moderación a una de defensa avanzada y participación activa, pone de relieve las lecciones aprendidas a través de conflictos cibernéticos reales y el reconocimiento de que el ciberespacio es un campo de batalla dinámico. A principios de la década de 2000 las iniciativas nacionales en materia cibernética solían centrarse en la “garantía de la información”: proteger las redes gubernamentales y militares (instalar parches, capacitar a los usuarios, crear redundancia). Los documentos de estrategia hacían hincapié en mejorar la ciberseguridad y la resiliencia, pero poco se debatía públicamente sobre las operaciones cibernéticas ofensivas. La disuasión, si se mencionaba, se basaba en la idea de que una potencia convencional abrumadora disuadiría los ciberataques importantes. Se trataba de una disuasión pasiva y poco creíble para una agresión de menor nivel.

A nivel internacional, incluso se debatía si la “ciberguerra” era un concepto distinto o, simplemente, una extensión de la guerra electrónica/espionaje. Por

ejemplo, Rid (2012) argumentó que los ciberataques eran básicamente sabotaje o espionaje, sin llegar a la categoría de "guerra", por cuanto este tipo de acciones no habían causado la muerte directa de nadie. Dicha perspectiva académica restaba importancia a la necesidad de doctrinas bélicas en el ámbito cibernético. Empero, a medida que se acumulaban los incidentes (Estonia en 2007, Georgia en 2008, "Stuxnet" en 2010, el virus "Shamoon" que afectó a Saudi Aramco en 2012, los ataques a la red eléctrica en Ucrania en 2015-2016, etc.), se hizo evidente que la simple defensa pasiva era insuficiente, y que las operaciones cibernéticas podían tener efectos estratégicos.

Los ejércitos comenzaron a incorporar la ciberdefensa de forma más abierta. Para 2010 se creó el Comando Cibernético de los Estados Unidos y la OTAN declaró la ciberdefensa como parte de sus tareas principales (Harrop & Matteson, 2019). Aun así, la doctrina inicial para muchos Estados seguía siendo defensiva: proteger la infraestructura crítica, responder a los incidentes cibernéticos y mejorar la conciencia situacional. En otras palabras, el ciberespacio a menudo se consideraba un escenario transversal a los dominios físicos de la guerra, y en consecuencia se asumía una función de apoyo a las operaciones cinéticas (p. ej., usar el ciberespacio para desactivar los radares enemigos antes de un ataque aéreo).

No obstante, el punto de inflexión en la doctrina llegó a mediados de la década de 2010, impulsado por las audaces acciones de los adversarios. El descubrimiento de que unidades cibernéticas del Ejército Popular de Liberación de China (EPL) habían logrado penetrar numerosas corporaciones y bases de datos del Gobierno de Estados Unidos llevó a acusaciones contra oficiales del EPL en 2014 y a impulsar una iniciativa de disuasión (Moulton et al., 2019). De igual manera, las actividades rusas indicaron que en cualquier conflicto futuro los ciberataques a las redes de comando y la infraestructura civil serían características tempranas. Por lo tanto, los militares empezaron a tratar el ciberespacio como un dominio de guerra constante, y no solo como un dominio de apoyo.

Esta nueva doctrina también implicó elevar el rol de la ciberseguridad ofensiva. Anteriormente, la ciberseguridad ofensiva se mantenía en gran medida como una reserva estratégica, el equivalente digital de las fuerzas especiales, utilizada solo en operaciones encubiertas selectas (como "Stuxnet") o como una amenaza disuasoria. Bajo la estrategia de defensa avanzada las herramientas cibernéticas ofensivas se utilizarían de forma más rutinaria para interrumpir las operaciones de los adversarios. Se trataba, entonces, de un cambio significativo en el pensamiento estratégico: es decir, de considerar las ciberarmas como bazas a usarlas

como herramientas cotidianas del arte de gobernar. De acuerdo con Moulton et al. (2019), un reflejo de esto fue la decisión estadounidense, en 2018, de flexibilizar algunas normas para que el Comando Cibernético realizara operaciones fuera de las zonas de guerra tradicionales. Ese cambio burocrático indicó la alineación de la política con la nueva doctrina de vanguardia.

Y los aliados de Estados Unidos han reflejado dicha evolución. Por ejemplo, el Reino Unido, en su Revisión Integrada de 2021, anunció una Fuerza Cibernética Nacional que combina ataque y defensa, e insinuó una postura cibernética más proactiva. Francia publicó en 2019 una doctrina que reconoce la ciberseguridad ofensiva como parte de las operaciones militares. La OTAN actualizó su política para permitir las contribuciones de los Estados miembros a la ciberseguridad ofensiva en sus misiones (mientras que la OTAN se centra en la defensa, los aliados individuales pueden realizar ciberseguridad ofensiva en apoyo). De acuerdo con Buchanan (2020), estos resultados muestran una tendencia: las capacidades cibernéticas se están integrando en la planificación militar, no están siendo restringidas.

Otro aspecto de la evolución doctrinal ha sido organizativo, pues al principio las unidades cibernéticas solían ser pequeñas y compartimentadas (quizás, bajo agencias de inteligencia o unidades de comunicaciones). En contraste, las Fuerzas Militares están actualmente integrando la ciberseguridad a nivel estratégico y operativo, hasta el punto de que los ejercicios y simulacros de guerra incluyen rutinariamente juegos de ciberguerra (Smith III et. al, 2023). Esta integración en la doctrina conjunta es una maduración del pensamiento: de ver las ciberoperaciones como una especialidad de nicho a tratarla al mismo nivel de las operaciones aéreas, terrestres, marítimas y espaciales.

Finalmente, las doctrinas en evolución enfatizan la colaboración y los esfuerzos de todo el Estado nación. La defensa avanzada no es solo una responsabilidad militar: a menudo implica trabajar con otras organizaciones jurídicas, agencias de inteligencia, fuerzas policiales (para dismantelar infraestructura criminal), aliados estatales, e incluso, empresas tecnológicas. Por ejemplo, Microsoft y otros actores de la industria han actuado en ocasiones para dismantelar *botnets* o exponer *hackers* colaborando eficazmente en los esfuerzos de defensa avanzada de los Estados (Kello, 2018). Reconociendo dicha realidad, las doctrinas ciberespaciales de los Estados han evolucionado para fomentar las colaboraciones público-privadas y el intercambio de inteligencia, hasta el punto de que la línea divisoria entre los roles militares y civiles en la ciberdefensa es cada vez más difusa que en cualquier otro dominio de guerra, y las doctrinas reflejan cada vez más que la ciberseguridad es un esfuerzo colectivo.

En resumen, la transición de la doctrina ciberespacial de la defensa pasiva a la defensa avanzada resume cómo los Estados se adaptaron a las presiones persistentes de la ciberguerra en el siglo XXI. La moderación inicial y las posturas reactivas dieron paso a operaciones asertivas y anticipatorias a medida que las naciones comprendían que esperar para absorber un impacto era demasiado peligroso en el ciberespacio. Al impulsar la lucha hacia las redes adversarias y enfrentar las amenazas continuamente, la doctrina actual busca tomar la iniciativa. Como resultado, los planificadores militares y los legisladores han integrado las consideraciones cibernéticas en el corazón de la estrategia de seguridad nacional. La articulación de Estados Unidos de un compromiso de "interacción persistente" es un ejemplo destacado de esa evolución y representa un cambio más amplio en nuestra concepción del conflicto en la era digital: implacable, interconectado y combatido tanto con paquetes y código como con tanques y misiles.

Estados Unidos, ciberdisuasión y la estrategia de la "interacción persistente"

Los conceptos tradicionales de la disuasión, desarrollados particularmente en el contexto de la Guerra Fría y el conflicto nuclear, se enfrentan a distintos desafíos en el reino ciberespacial. Según Álvarez et al. (2018), la disuasión consiste en prevenir la acción del adversario mediante la amenaza de un castigo inaceptable (disuasión por castigo) o negándole el beneficio esperado (disuasión por negación). En la ciberguerra ambas formas de disuasión han resultado difíciles de lograr. El problema de la atribución (ya discutido) debilita la disuasión por castigo, ya que si el agredido no puede estar seguro de quién lo atacó, no puede amenazar con represalias de forma creíble. Asimismo, la ventaja ofensiva inherente y las innumerables vulnerabilidades de los sistemas digitales complejos hacen que la disuasión por negación sea difícil de alcanzar, por cuanto ninguna organización puede estar perfectamente protegida contra todas las intrusiones cibernéticas.

Estos factores contribuyeron a la sensación, a mediados de la década de 2010, de que se necesitaba un nuevo enfoque, lo cual llevó al Comando Cibernético de los Estados Unidos y a otros a adoptar el concepto de "combate persistente" y "defensa avanzada". Dicha estrategia marca un cambio de una postura reactiva y disuasoria a una campaña más proactiva y continua para contrarrestar e imponer costos a los adversarios en el ciberespacio. En primer lugar, es importante explicar por qué la disuasión clásica ha fallado en el ciberespacio. Durante la Guerra Fría, la disuasión dependía de la certeza de identificar un lanzamiento nuclear y

responder de la misma forma (Destrucción Mutua Asegurada). En el ciberespacio, como ya se ha mencionado, los atacantes operan en la sombra. Un adversario podría calcular que, incluso si una víctima descubre el ataque, podría no responder con contundencia, debido a la incertidumbre o la falta de opciones de respuesta proporcionales. Además, muchos incidentes cibernéticos no alcanzan los umbrales de una guerra: ¿lanzaría un Estado misiles en respuesta a una brecha de red o a un corte de energía temporal? Es muy improbable. Los adversarios aprovechan esto manteniendo las operaciones en la zona gris, donde no existen líneas rojas disuasorias claras.

Este ritmo constante de ciberactividad sub-bélica (robo de propiedad intelectual, intromisión electoral, sondeo de infraestructura crítica) no se detenía por el temor a represalias estadounidenses. Durante años la política declarativa de Estados Unidos fue reservarse el derecho a responder a los ciberataques con cualquier medio (incluido el cinético), pero en la práctica las respuestas fueron moderadas (por ejemplo, acusaciones, sanciones, protestas diplomáticas), lo que no pareció disuadir la continua ciberagresión de los rivales. Para 2018 el Comando Cibernético de Estados Unidos (en inglés, USCYBERCOM, por las iniciales de United States Cyber Command) articuló una nueva visión estratégica que reconocía que la disuasión por sí sola era insuficiente. La declaración de visión del Comando de 2018, "lograr y mantener la superioridad en el ciberespacio", enfatizó la necesidad de un compromiso continuo con los adversarios. Afirmaba, además, que "los adversarios han explotado la velocidad y el volumen de datos y eventos en el ciberespacio para volver el dominio más hostil... necesitamos un nuevo enfoque" (Smeets & Lin, 2018, p. 85).

Este nuevo enfoque, denominado "compromiso persistente", exigía que las fuerzas cibernéticas estadounidenses estuvieran en la primera "línea de fuego" digital todos los días, frustrando a los oponentes mediante presión constante, en vez de esperar para reaccionar solo ante un ataque. En efecto, esto significó pasar de una postura de disuasión por castigo (amenazando con represalias tras ser atacado) a una postura de disuasión por negación e iniciativa operativa: o sea, tomar las medidas necesarias para detener o interrumpir las operaciones del adversario antes de que puedan atacar imponiéndole "fricción" continuamente (Scherkeller et al., 2022).

De acuerdo con Scherkeller et al. (2022), en vez de permanecer inmóvil en tiempos de paz y actuar únicamente en situaciones de crisis, el Comando Cibernético se comprometió con operaciones persistentes, que incluían acciones como la

búsqueda de *hackers* enemigos en las redes estadounidenses y aliadas, el contra-ataque a la infraestructura adversaria utilizada para llevar a cabo operaciones y, en general, la disputa del dominio ciberespacial para crear oportunidades de ataque.

En la práctica, esto podría significar, por ejemplo, que si se descubre que un adversario está desplegando una *botnet* para atacar bancos estadounidenses, los ciberoperadores del país del norte podrían no solo bloquearla defensivamente, sino también penetrar los servidores de control y dismantelar la *botnet* o extraer información sobre los perpetradores, y así atacarlos directamente. Esta es una postura mucho más activa que la norma anterior, de proteger principalmente las propias redes y responder tras ser atacado.

Otro concepto relacionado que se introdujo en la ciberestrategia estadounidense es la "Defensa Avanzada". Este principio, destacado en la Estrategia Cibernética de 2018 del Departamento de Defensa, implica defender en el origen de la amenaza, en vez de en el objetivo. O sea, en vez de esperar a que las operaciones cibernéticas enemigas alcancen las redes estadounidenses y luego reaccionar, las fuerzas cibernéticas de Estados Unidos buscarán identificar, localizar y neutralizar las amenazas dentro de las redes o infraestructuras adversarias antes de que puedan emplearse. De acuerdo con Smeets y Lin (2018), ello autoriza efectivamente una forma de acción contraofensiva preventiva o continua en el ciberespacio extranjero con fines defensivos. Por ejemplo, si los datos de inteligencia muestran que una unidad de *hackers* extranjeros está planeando una gran operación, un enfoque de defensa avanzada podría implicar infiltrarse en las herramientas o redes de esa unidad, para frustrar la operación antes del lanzamiento. Dicho enfoque reconoce que en el ciberespacio interconectado la defensa y la ofensiva se difuminan, y a veces la mejor defensa es llevar la lucha al territorio del adversario (algo parecido a dismantelar los misiles enemigos antes de su lanzamiento).

La adopción del compromiso persistente y la defensa avanzada fue una respuesta a deficiencias específicas observadas. Durante años los adversarios llevaron a cabo, con impunidad, campañas cibernéticas que no llegaban a ser un acto de guerra abierta. Y lo que es aún más grave, las herramientas disuasorias tradicionales implementadas por los Estados para evitar ese tipo de ataques, como amenazas de sanciones económicas o acciones legales, no parecieron frenar significativamente dichas campañas. Fue entonces cuando, bajo un compromiso persistente, Estados Unidos indicó que usaría sus fuerzas cibernéticas para imponer costos en tiempo real (Scherkeller et al., 2022). Por ejemplo, durante las elecciones intermedias de 2018 el Comando Cibernético supuestamente llevó a cabo

operaciones para desconectar a la Agencia de Investigación de Internet (la granja de *trolls* rusa que interfirió en 2016) hackeando sus servidores e interrumpiendo su acceso a internet. Pero dichas acciones no se publicaron, para preservar el secreto, si bien informes posteriores indicaron que la capacidad rusa para interferir en esas elecciones se vio obstaculizada por las cibermedidas ofensivas estadounidenses. Un ejemplo clásico de "interacción persistente" para proteger de modo proactivo un proceso (Scherkeller et al., 2022).

Otra justificación fue el reconocimiento de que el contacto constante es la norma en el ciberespacio (Healey, 2018). Es decir, un actor no puede permitirse cruzarse de brazos y bloquear el acceso: sus adversarios estarán investigando las 24 horas del día y los siete días de la semana. Por consiguiente, sus fuerzas cibernéticas también deben operar las 24 horas del día los siete días de la semana. Desde la perspectiva de la teoría de la disuasión, el compromiso persistente busca redefinir los cálculos de costo-beneficio del adversario: es decir, si antes un adversario consideraba que las operaciones cibernéticas eran de bajo riesgo y alta recompensa (debido a las bajas probabilidades de represalia), ahora debe considerar que los equipos cibernéticos estadounidenses o aliados podrían estar resistiendo activamente y contraatacando, incluso fuera del conflicto abierto. Ello podría disuadir ciertas conductas al aumentar su costo o reducir la confianza en su éxito (disuasión por negación). Por ejemplo, si un Estado sabe que cualquier intento de piratear una red eléctrica estadounidense se enfrentará inmediatamente a un ataque masivo contra su propia infraestructura de piratería y a la posible exposición de sus operaciones, podría estar menos inclinada a intentarlo.

En el sentido más amplio de la G5G, la intervención persistente se alinea con la noción de competencia constante y multidominio. En vez de guerras y paz claras, existe un ecosistema de conflicto continuo, en el cual el ciberespacio es un campo de batalla donde los Estados se involucran a diario, y no solo en tiempos de guerra. El objetivo es "defenderse" para interceptar amenazas y "combatir" continuamente las actividades de los adversarios, y disuadir así mediante la acción en vez de la mera amenaza. Esta es una evolución significativa con respecto a las doctrinas anteriores, que enfatizaban la disuasión mediante la capacidad de represalia o la construcción de fortalezas defensivas y, en gran medida, la espera del fuego hasta la crisis.

En resumen, la ciberdisuasión en el sentido clásico se ha visto socavada por los problemas de atribución y el atractivo de los ataques en la zona gris. El concepto de intervención persistente surgió como respuesta: es una estrategia de confrontación activa y continua con los adversarios para limitar su libertad de

maniobra. Al operar de forma continua y ofensiva en defensa de sus propias redes e intereses, un Estado buscará imponer una forma de disuasión por negación y hacer que el ciberespacio cotidiano sea hostil para posibles atacantes (Healey, 2018). Esto representa un cambio de mentalidad profundo de cómo se entiende la ciberguerra; un cambio del ciberespacio como un ámbito estratégico donde se espera disuadir cualquier conflicto (un enfoque que resultó optimista) al ciberespacio como un espacio disputado donde se requieren operaciones constantes para asegurar ventaja y proteger los activos propios.

Rusia y China: ciberinfluencia y ciberespionaje

Rusia es ampliamente reconocida como una ciberpotencia con una doctrina que enfatiza la confrontación de la información y la disrupción asimétrica. Sus operaciones cibernéticas suelen combinar ataques técnicos con guerra psicológica, con el objetivo de explotar el terreno humano del ciberespacio. Un sello distintivo de su enfoque es el uso de campañas de ciberinfluencia, en particular la interferencia en elecciones extranjeras. Actores respaldados por el Estado ruso (como la “granja de trolls” de la Agencia de Investigación de Internet) han estado implicados en la difusión de noticias falsas para sembrar discordia y manipular la opinión pública.

Estas operaciones de influencia, a menudo coordinadas con hackeos y filtración de información robada, ejemplifican la estrategia rusa de aprovechar el ciberespacio para lograr fines geopolíticos sin una confrontación militar directa. El enfoque ruso también incluye ciberataques altamente disruptivos contra infraestructuras críticas: efectivamente, en el panorama actual de amenazas, los ciberataques ya no se limitan al ámbito virtual, sino que se han convertido en poderosas herramientas capaces de causar efectos físicos en el mundo real. Esta convergencia del ciberespacio y los sistemas físicos define lo que los investigadores denominan ataques “ciberfísicos”. Loukas (2015) conceptualiza este tipo de ataques como la explotación de componentes computacionales y de comunicación integrados en sistemas físicos para manipular o dañar sus funciones físicas. A diferencia de los ciberataques tradicionales que atacan la confidencialidad o disponibilidad de los datos, los ataques ciberfísicos buscan controlar, interrumpir o destruir activos tangibles, con consecuencias potencialmente catastróficas para la seguridad humana, la estabilidad económica y la seguridad nacional.

Una idea fundamental de Loukas (2015) es que los sistemas ciberfísicos, como los sistemas de control industrial, las redes inteligentes, los vehículos autónomos y los dispositivos médicos, son especialmente vulnerables, debido a la estrecha

interrelación entre sus componentes digitales y físicos. Cuando un atacante compromete las capas de computación o red de estos sistemas, puede influir indirectamente en procesos físicos como el flujo eléctrico, las reacciones químicas o el movimiento mecánico. Por ejemplo, los atacantes pueden explotar “actuadores” (dispositivos que realizan acciones como abrir válvulas), “controladores” (que regulan el comportamiento del sistema) o “sistemas integrados” (computadores de propósito especial en maquinaria), para causar fallas o, incluso, destrucción física.

Loukas (2015) describe cuatro tipos principales de efectos de ataques ciberfísicos: 1) actuación no autorizada, como la apertura remota de puertas cerradas en edificios inteligentes; 2) actuación incorrecta, donde la manipulación de datos de sensores provoca resultados peligrosos, como el control de crucero acelerado en vehículos; 3) actuación retardada, como los ataques de denegación de servicio (en inglés, DoS, por las iniciales de *Denial of Service*), que suprimen las advertencias de presión en gasoductos, y 4) actuación impedida, donde los sistemas se desactivan por completo, como se observa en fallas inducidas por *malware* en automóviles o dispositivos médicos. Estas interrupciones pueden ocurrir mediante técnicas cibernéticas bien conocidas, como inyecciones SQL, gusanos o rastreo de paquetes, pero su impacto se define por sus consecuencias físicas en el mundo real.

Los ejemplos históricos refuerzan estas preocupaciones. El incidente del gusano “Slammer”, de 2003, aunque no fue concebido inicialmente como un ataque ciberfísico, inutilizó indirectamente 13.000 cajeros automáticos del Bank of America e interrumpió las pantallas de seguridad de la central nuclear Davis-Besse, lo que demuestra cómo incluso los ciberataques no dirigidos pueden tener repercusiones en el ámbito físico (Loukas, 2015). Asimismo, al inicio de su invasión en 2022, las fuerzas rusas atacaron Ucrania desplegando *malware* de borrado de datos para paralizar las redes gubernamentales y energéticas ucranianas. Al usar *malware* destructivo como primer ataque, Rusia reforzó su doctrina de integrar la ciberguerra en las operaciones militares para perturbar la sociedad y las defensas del adversario desde el principio.

Un aspecto en especial alarmante, según Loukas (2015), es que los ataques ciberfísicos pueden escalar a ciberataques cinéticos: es decir, operaciones intencionales destinadas a causar daños físicos, así como víctimas humanas. Esto incluye escenarios como la desactivación de marcapasos, el sabotaje de frenos en vehículos inteligentes o la provocación de fallos catastróficos en equipos industriales. Por ejemplo, en la prueba del generador Aurora, un ciberataque destruyó físicamente un generador eléctrico mediante el envío de comandos desfasados,

lo que pone de relieve cómo el *software* puede utilizarse como arma contra sistemas de *hardware* con resultados devastadores. Además, Loukas (2015) señala la amenaza emergente de ataques híbridos complejos, donde interactúan el ciberespacio, el espacio físico, e incluso, la cognición humana. Por ejemplo, las interfaces cerebro-computador podrían llegar a ser pirateadas para influir en el comportamiento del usuario, una forma de manipulación subliminal que trasciende los límites tradicionales de la ciberseguridad. Y como ha quedado demostrado en la actual guerra ruso-ucraniana, los riesgos sistémicos que plantean este tipo de ataques se amplifican en infraestructuras críticas como las redes eléctricas, los sistemas de transporte y las redes sanitarias. Loukas (2015) enfatiza que la pérdida de disponibilidad del sistema puede tener consecuencias en cascada en todos los sectores, y crear así una disrupción social generalizada.

La doctrina cibernética rusa está profundamente arraigada en el enfoque histórico de ese Estado hacia la guerra de la información, lo que refleja una continuidad de engaño estratégico, manipulación e influencia que se remonta a la era soviética (Sweet, 2024). Desde la creación de la oficina de desinformación, en 1923, por la Unión Soviética (URSS), hasta las capacidades cibernéticas contemporáneas, la doctrina rusa considera las operaciones de información y las operaciones cibernéticas herramientas cruciales para lograr objetivos geopolíticos sin cruzar el umbral de un conflicto abierto (Couretas, 2024). Pero, a diferencia de las doctrinas occidentales, Rusia no articula públicamente su estrategia cibernética a través de publicaciones militares oficiales comparables a las de la OTAN o Estados Unidos. En cambio, se basa en los conceptos generales descritos en su Doctrina para la Seguridad de la Información de la Federación de Rusia (2000), que define las operaciones cibernéticas como instrumentos para lograr la superioridad de la información y proteger la soberanía nacional.

A nivel operativo, las fuerzas militares rusas conciben la guerra de la información como una estrategia que abarca tiempos de paz, crisis y guerra integrando la guerra electrónica, las operaciones psicológicas, la recopilación de inteligencia y las operaciones cibernéticas en un proceso continuo e ininterrumpido (Couretas, 2024). Este enfoque integrado implica que las herramientas cibernéticas se utilizan junto con las operaciones militares convencionales, para difuminar la línea entre guerra y paz. La visión rusa del "ciberpoder" se vio influenciada por la Doctrina Primakov, que posiciona a Rusia como un actor central en un mundo multipolar, desafiando el dominio estadounidense y buscando socavar la cohesión occidental mediante medios asimétricos, incluidas las operaciones cibernéticas (Couretas, 2024).

Uno de los escenarios más analizados de las operaciones cibernéticas rusas ha sido Ucrania. Según Sweet (2024), *hackers*, servicios de inteligencia y grupos criminales asociados, financiados por el Estado ruso, han atacado sistemáticamente a Ucrania desde al menos 2004, cuando Moscú intervino en la Revolución naranja mediante campañas de desinformación electoral. El panorama cibernético ucraniano se convirtió en un campo de pruebas para las armas cibernéticas rusas, lo que culminó en una serie de ataques de alto perfil. Por ejemplo, el ataque de 2015 a la red eléctrica de Ucrania, atribuido al *malware* "BlackEnergy", dejó a más de 225.000 personas sin electricidad durante el invierno, lo que marcó uno de los primeros cortes de energía cibernéticos conocidos de la historia (Sweet, 2024; Couretas, 2024).

Una característica notable de la cibercampaña rusa ha sido la participación de grupos de *hackers* con afiliación débil o semiindependientes, como KillNet, XakNet y el Ejército Cibernético del Pueblo, que a menudo se hacen pasar por patriotas al llevar a cabo ataques contra Ucrania y objetivos vinculados a la OTAN. Si bien estos grupos niegan públicamente el control directo del Kremlin, la evidencia sugiere diversos grados de coordinación, apoyo financiero o, al menos, aprobación tácita de las autoridades rusas. De acuerdo con Sweet (2024), este modelo permite una negación plausible, al tiempo que aprovecha una red global de intermediarios cibernéticos para ampliar el alcance y el impacto de las operaciones estatales.

En resumen, la doctrina cibernética de Rusia refleja una cultura profundamente arraigada de guerra asimétrica, en el que las operaciones cibernéticas se consideran multiplicadores de fuerza junto con las capacidades militares tradicionales. Ucrania ha sido un laboratorio para esta doctrina, lo que ha ofrecido lecciones no solo sobre el potencial cibernético de Rusia, sino también sobre las estrategias de resiliencia necesarias para contrarrestar este tipo de campañas.

Por su lado, las ciberoperaciones patrocinadas por el Estado chino se centran en el espionaje con el objetivo de obtener inteligencia estratégica y ventaja económica. Por ende, las actividades cibernéticas chinas se caracterizan típicamente por la infiltración persistente y a largo plazo de las redes, para extraer datos confidenciales de un objetivo. Por ello, durante las últimas décadas las agencias militares y de inteligencia chinas han participado en robos masivos de propiedad intelectual y secretos de Estado de actores antagonistas, mediante medios cibernéticos (Couretas, 2024). Esta actividad se centra en la información de defensa, la tecnología avanzada y los secretos comerciales para impulsar el desarrollo de China e impulsar su progreso tecnológico-militar.

La doctrina cibernética china se ha convertido en uno de los marcos estratégicos más sofisticados y multifacéticos del mundo, moldeado por imperativos históricos, filosóficos y militares. Un aspecto central del enfoque chino es una comprensión holística e integral de la ciberguerra que integra las dimensiones militar, política, económica e informativa. A diferencia de las doctrinas occidentales, que suelen compartimentar las operaciones cibernéticas, la doctrina china percibe las capacidades cibernéticas como parte de un continuo más amplio de poder nacional, donde las etapas de paz y conflicto están interconectadas. Un aspecto clave de la doctrina china es la incorporación de las operaciones de información, las cuales se refieren no solo a actividades de piratería informática directa, sino también a operaciones psicológicas, manipulación mediática, censura y campañas de propaganda. Según Fritz (2013), los estrategas chinos adoptan el uso del control de la información para influir en el comportamiento del adversario y la opinión pública nacional, buscando moldear el entorno estratégico antes del estallido de hostilidades abiertas.

Couretas (2024) señala que el EPL ha organizado sus actividades cibernéticas en tres ramas principales: ataque a redes informáticas, explotación de redes informáticas y defensa de redes informáticas. Dichas ramas están alineadas con los niveles de guerra (estratégico, operativo y táctico), lo que les permite difuminar las fronteras tradicionales entre objetivos civiles y militares. Davis (2021) destaca que los escritos militares chinos enfatizan el uso de estrategias de guerra asimétricas, explotando las vulnerabilidades del adversario, como la dependencia de las redes informáticas, lo que nivela el terreno de juego contra oponentes tecnológicamente superiores, como Estados Unidos.

Cheng (2017) afirma que la doctrina china incluye el concepto de “defensa activa”, un principio maoísta que justifica la acción ofensiva con fines defensivos. Este principio se materializa en el ciberespacio mediante actividades como la catalogación de *exploits* de *software*, el mantenimiento de acceso encubierto a la red y el fomento de milicias de *hackers*, que pueden movilizarse en tiempos de crisis. Por ende, estas doctrinas reflejan la perdurable influencia de Sun Zi y Mao Zedong, quienes enfatizaron el papel del engaño, la guerra indirecta y la movilización de la población. Un ejemplo contemporáneo es la vasta población china en línea, que puede utilizarse como recurso cibernético durante el conflicto. Además, la doctrina se sustenta en el concepto de “informatización”, que contempla la integración de las tecnologías de la información en todos los aspectos de las operaciones militares.

Finalmente, los fundamentos teóricos de la doctrina cibernética china se ven reforzados por obras como *Unrestricted Warfare* (1999), de Qiao Liang y Wang

Xiangsui, quienes argumentan que el campo de batalla ya no se limita al ámbito militar, sino que abarca todos los elementos del poder nacional, desde la disrupción económica hasta la guerra legal. Esta amplia conceptualización ha llevado a difuminar las fronteras entre tiempos de paz y tiempos de guerra en el pensamiento estratégico chino, y convertido las operaciones cibernéticas en un pilar del enfoque de China ante la competencia de poder contemporánea. De acuerdo con Fritz (2013), China ha construido formidables ciberdefensas y regímenes de censura (el Gran Cortafuegos), lo cual refleja que su panorama de operaciones cibernéticas es tanto ofensivo (espionaje externo) como defensivo (control estricto de la información interna). En resumen, China utiliza sus capacidades cibernéticas principalmente como herramienta de espionaje estatal y robo de propiedad intelectual, buscando obtener ganancias a largo plazo y, en general, evitando los ciberataques disruptivos al estilo ruso.

Corea del Norte y la República Islámica de Irán: ciberdelincuencia y ciberoperaciones políticamente motivadas

La doctrina cibernética norcoreana refleja el enfoque del régimen en herramientas asimétricas que le permiten sortear sus limitaciones militares y económicas. Dado su severo aislamiento internacional y las sanciones impuestas por parte de Occidente, el "reino ermitaño" ha diseñado una estrategia cibernética orientada tanto a la seguridad interna como a la disrupción externa (Chen et al., 2010). La estructura de internet de Corea del Norte es singularmente insular: solo una élite selecta tiene acceso a la internet global, mientras que la mayoría de los ciudadanos están confinados a una intranet nacional (*Kwangmyong*) (Chen et al., 2010). Este entorno insular refleja, por lo tanto, un dilema estratégico: el régimen busca los beneficios de la tecnología de la información para su desarrollo y poder militar, pero teme el flujo abierto de información que podría socavar el control autoritario. Como resultado, Corea del Norte ha adoptado una doble estrategia: fomentar la capacidad cibernética técnica de unos pocos privilegiados y, al mismo tiempo, restringir drásticamente el uso social de internet. Dicha estrategia se halla profundamente arraigada en su ideología Juche, que enfatiza la autosuficiencia, aunque, paradójicamente, depende de las operaciones cibernéticas internacionales para la supervivencia del régimen (Warf, 2015).

Según Whyte y Mazanec (2023), la doctrina norcoreana considera las operaciones cibernéticas una forma de proyectar poder manteniendo, al mismo tiempo, una negación plausible. La doctrina cibernética del Estado norcoreano no se halla formalmente codificada, pero los analistas coinciden en que la Oficina General de

Reconocimiento (OGR) actúa como centro neurálgico de las operaciones cibernéticas ofensivas empleando unidades de élite como la "Oficina 121", que, según se informa, cuenta con más de 6.000 *hackers* altamente entrenados (Baig, 2019).

Cabe destacar que las operaciones cibernéticas ofrecen a Pyongyang una vía económica y de alto impacto para obtener ganancias estratégicas, a menudo en conjunto con maniobras cinéticas o diplomáticas (Sharp, 2017). Corea del Norte es conocida por utilizar la ciberdelincuencia como fuente de ingresos para financiar sus programas nucleares y de misiles balísticos. El "Grupo Lazarus", que opera bajo la supervisión de la OGR, está a la vanguardia de dichas actividades, y una de sus tácticas distintivas consiste en hackear instituciones financieras y plataformas de intercambio de criptomonedas. En efecto, el grupo fue responsable del robo al Banco de Bangladesh, en 2016, durante el cual se robaron aproximadamente 81 millones de dólares mediante transferencias SWIFT fraudulentas (Baig, 2019). Este ataque demostró la capacidad de Corea del Norte para infiltrarse con precisión en objetivos de alto valor, lo que subraya su dependencia de la ciberdelincuencia para eludir las sanciones.

El ataque del *ransomware* "WannaCry", de 2017, ejemplifica aún más la estrategia de Pyongyang. Este ciberataque infectó más de 300.000 computadores en 150 países, donde causó interrupciones en hospitales, telecomunicaciones y logística (Baig, 2019). Y si bien el lucro fue el motivo principal, la naturaleza indiscriminada del ataque puso de manifiesto la disposición de Corea del Norte a causar disrupciones generalizadas. No obstante, el robo de criptomonedas se ha convertido en un método predilecto del gobierno norcoreano para generar ingresos ilícitos en los últimos años. Al explotar vulnerabilidades en las plataformas de intercambio de criptomonedas, los *hackers* norcoreanos han exfiltrado cientos de millones de dólares en activos digitales, lo cual ofrece una atractiva combinación de liquidez y anonimato (White, 2022). Este tipo de ciberoperaciones demuestra que la ciberdelincuencia es un componente esencial del arte de gobernar de Corea del Norte (Whyte, 2016).

Más allá del lucro, el régimen de Pyongyang emplea los ciberataques como instrumentos de coerción política y represalia. El hackeo a Sony Pictures de 2014 es un buen ejemplo: en respuesta a *The Interview*, una película satírica que retrata el asesinato de Kim Jong-un, agentes norcoreanos se infiltraron en las redes de Sony, filtraron datos confidenciales e implementaron *malware* de borrado de datos (Sharp, 2017). El ataque obligó a Sony a cancelar inicialmente el estreno de la película, lo que representa un éxito poco común en cibercoerción (Sharp, 2017; Whyte, 2016). A nivel regional, los norcoreanos atacan regularmente los medios de

comunicación, los bancos y las agencias gubernamentales surcoreanas. El ataque "Dark Seoul", de 2013, interrumpió el funcionamiento de bancos y emisoras de radiodifusión, al borrar datos de decenas de miles de computadores (Barnes & Glaser, 2019). Además, unidades de espionaje norcoreanas como Kimsuky (APT37) se centran en robar información sensible de las entidades gubernamentales y de defensa de Corea del Sur, lo que alimenta el cálculo estratégico de Pyongyang (White, 2022). Esas operaciones difuminan la línea entre la acción estatal y la actividad criminal, y ofrecen a Corea del Norte beneficios tanto materiales como políticos, a la vez que dificultan la atribución de responsabilidades (Whyte, 2016). Su doctrina ciberespacial enfatiza la ofensiva (atacar primero o tomar represalias con rapidez), como forma de coerción y disuasión, ya que al demostrar su capacidad para infligir daño (financieramente o de forma disruptiva) sin recurrir a la fuerza cinética, el régimen busca disuadir a los enemigos de amenazarlo. En resumen, la ciberestrategia norcoreana se basa en la necesidad de fortalecer su frágil economía y, al mismo tiempo, reforzar su propia seguridad mediante operaciones clandestinas que puedan negarse u ocultarse, y evitar así la confrontación militar directa.

Por su parte, la doctrina cibernética de Irán se ve determinada por su ideología revolucionaria, su rivalidad geopolítica con Estados Unidos y los países del Golfo, y una persistente sensación de que se ha montado una estrategia de cerco en torno a la proyección "natural" del poder iraní en el Medio Oriente (Serscikov, 2025). La doctrina iraní enfatiza la disuasión, la represalia y el control interno. El Consejo Supremo del Ciberespacio, establecido en 2012, institucionalizó un doble enfoque del régimen iraní en la ciberguerra externa y el control interno de la información (Serscikov, 2025). En este sentido, Teherán considera las operaciones cibernéticas una extensión de su "guerra blanda" contra adversarios ideológicos y geopolíticos (Couretas, 2024). En este caso, el Cuerpo de la Guardia Revolucionaria Islámica (CGRI) desempeña un papel central en las operaciones cibernéticas ofensivas, con grupos vinculados al Estado, como el "Ciberejército Iraní" y "APT33" llevando a cabo ciberataques en Arabia Saudí, Israel, Estados Unidos y otros países antagónicos (Serscikov, 2025).

La Operación Ababil (2012-2013), una serie de ataques DDoS contra importantes bancos estadounidenses, ejemplifica el uso de medios cibernéticos por parte de Irán como represalia. Dichos ataques, atribuidos a la "Fuerza Quds" del CGRI, interrumpieron los servicios de banca en línea y se presentaron como una venganza por las sanciones occidentales y las provocaciones antiislámicas (Couretas, 2024). El ataque del *malware* "Shamoon", de 2012, tuvo como objetivo a Saudi Aramco, borró datos de 30.000 computadores y demostró la capacidad de Irán

para realizar operaciones cibernéticas destructivas (Serscikov, 2025). Versiones posteriores de "Shamoon", en 2016 y 2018, reforzaron el compromiso de Teherán con las ciberrepresalias. Irán también utiliza herramientas cibernéticas a nivel nacional para reprimir la disidencia. Los mecanismos de vigilancia y censura monitorean a activistas y grupos de oposición, mientras que las unidades cibernéticas despliegan *software* espía y ataques de ingeniería social contra disidentes (Serscikov, 2025). Este doble uso de las capacidades cibernéticas garantiza la estabilidad del régimen y proyecta disuasión externa.

Si bien son menos centrales que en la estrategia norcoreana, Irán ha participado en actividades cibernéticas con motivación financiera. Los ataques del *ransomware* "SamSam" (2015-2018) se dirigieron a municipios y proveedores de atención médica estadounidenses, para extorsionar por millones de dólares (Whyte & Mazanec, 2023). Irán también ha explorado la minería de criptomonedas y el hackeo de plataformas de intercambio, especialmente a medida que se endurecieron las sanciones en su contra (Serscikov, 2025). Sin embargo, las operaciones de Irán con motivación financiera parecen más oportunistas y menos institucionalizadas que las de Corea del Norte, lo que refleja la base económica comparativamente más sólida de Irán y su enfoque en misiones ideológicas (Serscikov, 2025).

En resumen, tanto Corea del Norte como Irán utilizan las operaciones cibernéticas como herramientas asimétricas, lo que les permite compensar las desventajas militares y económicas convencionales. Comparten la dependencia de la negación plausible, la participación de actores indirectos y la disposición a atacar objetivos civiles y de infraestructuras críticas (Whyte, 2016; Serscikov, 2025). Sin embargo, hay diferencias clave. Las operaciones de Corea del Norte se centran en gran medida en el lucro, lo que refleja su profundo aislamiento económico y su necesidad de divisas (Whyte & Mazanec, 2023). Irán, en cambio, prioriza las represalias ideológicas y estratégicas, con un enfoque regional en Oriente Medio (Serscikov, 2025).

Otra distinción radica en la cibergobernanza nacional. El internet de Corea del Norte está casi completamente aislado y concentra su poder cibernético en el exterior, mientras que Irán mantiene un complejo aparato interno de ciberrepresión, que monitorea y controla a una gran población en línea (Chen et al., 2010; Serscikov, 2025). En conclusión, ambos Estados ilustran cómo el poder cibernético permite a las potencias pequeñas o medianas superar sus posibilidades, pero sus doctrinas reflejan prioridades diferentes: la estrategia cibernética de Corea del Norte es fundamentalmente de supervivencia y criminal, mientras que la de Irán es ideológica y estratégica, y refleja sus culturas políticas y contextos geopolíticos únicos.

El contexto cibernético colombiano: desafíos y respuestas

La rápida digitalización de Colombia ha generado oportunidades económicas, pero también ha aumentado las vulnerabilidades a la seguridad y defensa del Estado. Por ejemplo, los ciberataques a las redes financieras o los sistemas de transporte podrían perturbar la economía y poner en peligro la seguridad pública, mientras que las filtraciones de las bases de datos gubernamentales podrían exponer información confidencial. El concepto de Infraestructura Crítica Cibernética Nacional ha cobrado así relevancia. Se refiere a los activos digitales cuya inutilización tendría efectos perjudiciales para la seguridad nacional (ESDEG, 2020). Proteger estos activos es ahora una preocupación primordial para las autoridades colombianas, por lo que la comunidad de defensa en Colombia considera la seguridad del ciberespacio parte integral de la defensa nacional y el bienestar público (ESDEG, 2020).

En respuesta a esos desafíos, Colombia ha articulado un marco nacional de políticas de ciberseguridad y ciberdefensa con visión de futuro. La piedra angular de este marco ha sido la construcción de una propuesta académica de la Escuela Superior de Guerra de Colombia (ESDEG), denominada *Estrategia Nacional de Ciberdefensa y Ciberseguridad 2020-2030*, un documento estratégico integral que establece objetivos e iniciativas para la década actual (ESDEG, 2020). Esa estrategia se distingue por su enfoque holístico, ya que centra una estrategia de defensa de los intereses colombianos en el ciberespacio mediante la integración, interacción y cooperación entre el sector público y privado, a fin de comprometer todos los campos político, económico, sicosocial y militar.

En vez de tratar la ciberseguridad como un asunto puramente técnico, la estrategia la integra en el contexto más amplio de la seguridad nacional y el desarrollo. Define riesgos, amenazas y desafíos en el ciberespacio y establece objetivos para mejorar la capacidad de seguridad digital de Colombia para mediados de la década de 2020. Una prioridad es fortalecer el marco legal y judicial (actualizando las leyes contra la ciberdelincuencia y mejorando el procesamiento penal de los ciberdelinquentes), para garantizar que los infractores rindan cuentas. Otro enfoque es el desarrollo de cibercapacidades: la estrategia enfatiza establecer planes de carrera y de capacitación en cada institución para formar profesionales cualificados en ciberseguridad, y así fortalecer los mecanismos defensivos en ciberdefensa y ciberseguridad en todo el país.

En cuanto a la ciberdefensa (capacidades cibernéticas militares y de seguridad nacional), la estrategia exige integrar las operaciones cibernéticas en la planificación de la defensa y reconocer el ciberespacio como un nuevo ámbito de la guerra.

Las Fuerzas Militares colombianas priorizan tanto la "defensa activa" (mediante monitoreo continuo y respuesta rápida) como la "defensa pasiva" (mediante controles de protección y resiliencia) para resistir ciberataques (Medina, 2019). Este enfoque implica desarrollar capacidades para detectar y responder a amenazas en tiempo real, a la vez que fortalece los sistemas para que sean resilientes ante ataques. La estrategia prevé que Colombia planifique y lleve a cabo operaciones cibernéticas cuando sea necesario para apoyar la defensa nacional, y fomenta el desarrollo de herramientas cibernéticas ofensivas de forma controlada (un punto que se retomará más adelante). Cabe destacar que la estrategia también destaca la cooperación internacional como un pilar de la postura de ciberdefensa de Colombia: insta al país a promover y coordinar la cooperación nacional e internacional entre las entidades responsables de la ciberseguridad (ESDEG, 2020).

La implementación efectiva de la estrategia cibernética de Colombia depende de roles claros y de la coordinación entre diversas instituciones. En ese orden de ideas, Colombia ha establecido un sólido marco institucional a través del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), que desempeña un papel fundamental en la coordinación nacional de ciberseguridad. El ColCERT se encarga de proteger la infraestructura crítica del país, colaborar con actores públicos y privados y responder a emergencias cibernéticas bajo la dirección del Ministerio de Defensa. Además, el Comando Conjunto Cibernético (CCOC) y el Centro Cibernético Policial (CCP) fortalecen las dimensiones militares y policiales de la estrategia de ciberdefensa de Colombia, garantizando una capacidad de respuesta estratificada en todos los sectores (ESDEG, 2020).

En la práctica, el ColCERT trabaja en estrecha colaboración con los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), incluyendo los de la Policía Nacional y otras instituciones del Estado, para garantizar una respuesta unificada a las ciberamenazas. El Ministerio de Defensa desempeña un papel clave en la formulación de políticas de ciberdefensa, y bajo su dirección el Ejército, la Armada y la Fuerza Aeroespacial Colombiana han estado desarrollando sus propias unidades y doctrinas cibernéticas para abordar las amenazas en el ciberespacio: por ejemplo, la Fuerza Aeroespacial Colombiana cuenta ahora con una Doctrina Básica Aérea, Espacial y Ciberespacial (DBAEC), y cada servicio de las Fuerzas Militares cuenta con unidades dedicadas a proteger sus redes y apoyar las operaciones cibernéticas.

Desde un punto de vista estratégico, Colombia ha sido un líder regional en políticas de ciberseguridad impulsando la Política Nacional de Seguridad Digital a través de documentos CONPES como el 3701 (2011) y el 3854 (2016), que

establecieron marcos para la coordinación nacional y estándares técnicos (ESDEG, 2020). Asimismo, Colombia ha buscado alianzas en el extranjero: en 2017, por ejemplo, se convirtió en el primer socio global latinoamericano de la OTAN, lo que permitió la colaboración en las mejores prácticas de ciberdefensa con los países aliados. La Estrategia Nacional también destaca el intercambio de información sobre amenazas como acción para la detección temprana de amenazas transnacionales. Al participar en foros como el programa de ciberseguridad de la Organización de los Estados Americanos (OEA) y acuerdos bilaterales, Colombia busca contribuir y beneficiarse de los esfuerzos colectivos para proteger el ciberespacio.

Sin embargo, y a pesar de estos avances, Colombia sigue enfrentando desafíos como la fragmentación de la gobernanza institucional, la escasez de especialistas en ciberseguridad y las vulnerabilidades en sectores críticos como el financiero, el energético y la salud pública (ESDEG, 2020). La catalogación de la infraestructura crítica y la definición de responsabilidades operativas entre las unidades cibernéticas civiles y militares siguen siendo prioridades, es especial ante la evolución de las amenazas provenientes de las redes regionales de ciberdelincuencia y los adversarios estatales.

Además, la creciente economía digital de Colombia y la adopción de tecnologías disruptivas añaden complejidad a su panorama de ciberseguridad (Maldonado, 2024). La creciente digitalización de la logística, las transacciones financieras y la administración pública crea nuevos vectores para los ciberataques, lo que requiere una postura de defensa adaptativa e integrada. En este contexto, el Gobierno colombiano ha priorizado la ciberinteligencia para permitir la detección temprana de amenazas y la implementación de contramedidas proactivas, como parte de una estrategia más amplia para fomentar la autonomía tecnológica, con énfasis en la inversión en I+D en ciberseguridad nacional y el desarrollo de la fuerza laboral para reducir la dependencia de soluciones externas (ESDEG, 2020).

En Colombia el desarrollo de una sólida "cultura ciberestratégica" no es solo una aspiración, sino una necesidad urgente, ya que el país enfrenta una creciente gama de ciberamenazas que ponen en peligro su seguridad nacional, estabilidad económica y cohesión social. Como subraya Giraldo (2024), el concepto de cultura ciberestratégica debe entenderse como algo más que un conjunto de mejores prácticas o soluciones técnicas. En realidad, encarna las actitudes, valores, conocimientos y comportamientos colectivos que configuran la forma como las instituciones y las personas perciben y responden a los ciberriesgos. Giraldo (2024) identifica dos pilares para el desarrollo de dicha cultura: primero, la internalización

de la ciberseguridad como un componente central de la resiliencia organizacional y nacional. Segundo, la promoción de una postura proactiva que anticipe y mitigue las amenazas antes de que se materialicen. En el contexto colombiano estos pilares se alinean estrechamente con las políticas de ciberseguridad en evolución del país, como la Política Nacional de Seguridad Digital, que enfatiza la coordinación interinstitucional y las alianzas público-privadas. Sin embargo, como señala Giraldo (2024), dichos marcos siguen siendo insuficientes si no se acompañan de una profunda transformación cultural. Esto último requiere esfuerzos sostenidos de sensibilización, educación e institucionalización del pensamiento en ciberseguridad en todos los niveles de la sociedad, desde organismos gubernamentales hasta empresas privadas y actores de la sociedad civil.

Uno de los principales desafíos que enfrenta Colombia es superar la fragmentación de responsabilidades y conocimientos. En efecto, Giraldo (2024) afirma que, si bien algunos sectores, como el CCOC y el ColCERT, han logrado avances significativos, persiste la falta de una visión unificada y de una doctrina compartida que integre el riesgo cibernético en la perspectiva estratégica más amplia de la defensa nacional. Cerrar esta brecha es clave para que Colombia responda eficazmente a amenazas sofisticadas, como el ciberespionaje, las campañas de *ransomware* y la guerra híbrida cibernética. Además, la cultura ciberestratégica debe ser adaptativa, sobre todo ante la acelerada transformación digital de Colombia, que está introduciendo nuevas vulnerabilidades mediante la adopción de tecnologías emergentes como la IA, el IoT y *blockchain*. Esto subraya la necesidad de aprendizaje continuo y evolución doctrinal garantizando que la postura de defensa de Colombia se mantenga alineada con la dinámica cambiante del ciberespacio.

Por otro lado, la transformación digital de los conflictos ha introducido nuevas complejidades en el derecho internacional, sobre todo en lo que respecta a la ciberguerra y su regulación. El panorama de seguridad global presenta cada vez más operaciones cibernéticas que desafían las nociones tradicionales de soberanía, integridad territorial y uso de la fuerza. Una cuestión decisiva en la regulación de los conflictos cibernéticos es si el derecho internacional se aplica al ciberespacio. Delerue (2020) argumenta que el ciberespacio, si bien intangible, no se halla fuera del alcance del derecho internacional. Estableciendo paralelismos con marcos jurídicos anteriores para el espacio aéreo y el espacio ultraterrestre, Delerue (2020) afirma que el ciberespacio es un dominio global regido por los mismos principios de soberanía estatal, no intervención y prohibición del uso de la fuerza consagrados en la Carta de las Naciones Unidas. El Manual de Tallin 2.0 refuerza esta postura, afirmando que las normas jurídicas internacionales se aplican a las

operaciones cibernéticas, en particular a las que podrían constituir un uso de la fuerza o un ataque armado (Delerue, 2020; Koh, 2013).

El principio de soberanía sigue siendo fundamental en los debates sobre la ciberguerra. Los Estados tienen plena jurisdicción sobre las infraestructuras cibernéticas ubicadas en sus territorios, y cualquier penetración no autorizada en dichos sistemas, ya sea mediante la implantación de *malware* o una interrupción remota, puede constituir una violación de la soberanía territorial (Delerue, 2020). El reto surge al distinguir entre las operaciones cibernéticas que tan solo causan inconvenientes y las que traspasan los límites de los actos ilícitos en conflictos armados. Por ejemplo, los ataques distribuidos de denegación de servicio (DDoS), si bien son disruptivos, pueden no cumplir con el estándar legal de uso de la fuerza según el artículo 2 de la Carta de las Naciones Unidas, a menos que causen daños físicos o lesiones (Delerue, 2020; Schmitt & Vihul, 2017).

La soberanía en el ciberespacio es al mismo tiempo clara y controvertida. Por un lado, Estados como Colombia tienen control legal sobre las infraestructuras de información dentro de sus fronteras. Pero, por otro lado, la naturaleza transnacional del ciberespacio complica su aplicación y atribución. Koh (2013) afirma que los Estados deben respetar la soberanía de otros incluso fuera de un conflicto activo, lo cual implica que las operaciones que atacan la infraestructura en un país, pero causan efectos en otro, pueden plantear problemas de soberanía. Sin embargo, prácticas operativas como la "defensa avanzada" y el "compromiso persistente", adoptadas por el Comando Cibernético de Estados Unidos, ilustran una tendencia creciente en la que los Estados buscan neutralizar las amenazas de forma preventiva difuminando las fronteras legales tradicionales. Esta práctica en evolución ha suscitado debates sobre la necesidad de nuevos instrumentos jurídicos. Algunos académicos abogan por un tratado cibernético específico, análogo al derecho espacial o al derecho del mar, para abordar las ambigüedades jurisdiccionales y operativas (Delerue, 2020). Otros, como Koh (2013), argumentan que los marcos jurídicos existentes son suficientes siempre que los Estados adopten estrategias interpretativas que apliquen las normas tradicionales a las actuales circunstancias.

Sin embargo, aplicar la teoría de la "guerra justa" a la ciberguerra plantea importantes consideraciones éticas y jurídicas. Tradicionalmente, el *jus ad bellum* exige que los Estados participen en la guerra únicamente por una causa justa, generalmente la legítima defensa contra un ataque armado. El *jus in bello* rige la conducta durante la guerra, y hace hincapié en la proporcionalidad y la discriminación. En el ámbito cibernético estos principios se ponen a prueba mediante operaciones que pueden tener efectos retardados o indirectos, lo cual dificulta evaluar la

proporcionalidad o distinguir entre combatientes y civiles (Delerue, 2020; Cristiano, 2019). Un ejemplo de ello es la Operación Stuxnet, que atacó las instalaciones nucleares de Irán mediante un sofisticado *malware*, y así provocó la degradación física de las centrifugadoras. Si bien muchos lo aclamaron como una alternativa precisa y no cinética a los ataques militares tradicionales, los juristas debaten si constituyó un acto lícito de legítima defensa o un uso ilícito de la fuerza según el derecho internacional (Cristiano, 2019). Ejemplos como ese resaltan la necesidad de estándares normativos más claros que guíen la conducta de los Estados.

De manera parecida, las normas diplomáticas desempeñan un papel cada vez más importante en la cibergobernanza, ya que ante la falta de tratados vinculantes los Estados han buscado generar consenso mediante medidas de fomento de la confianza y marcos normativos. El Grupo de Expertos Gubernamentales de las Naciones Unidas (en inglés, UNGGE, por las iniciales de United Nations Group of Governmental Experts on Information Security) ha sido fundamental en el establecimiento de normas no vinculantes, como la abstención de atacar infraestructuras críticas en tiempos de paz y la cooperación para atribuir actividades maliciosas (Cristiano, 2019; Delerue, 2020). Sin embargo, como señala Delerue (2020), dichos instrumentos de derecho indicativo enfrentan desafíos en cuanto a su aplicación y universalidad. La fragmentación es un riesgo, ya que los Estados poderosos pueden interpretar o aplicar las normas de forma selectiva. Los acuerdos bilaterales entre Estados Unidos y China (por ejemplo, el Acuerdo Xi-Obama, de 2015) y las iniciativas regionales subrayan el valor de la diplomacia, pero también revelan la dificultad de forjar estándares universales.

Para fortalecer su postura cibernética, Colombia debe profundizar su compromiso legal y diplomático en la materia. Como sugiere Cristiano (2019), la integración de las normas cibernéticas en las alianzas bilaterales y multilaterales puede mejorar la resiliencia. Además, Colombia debería promover marcos regionales que aborden el panorama de amenazas específico de América Latina garantizando que las normas internacionales reflejen las realidades locales. En este sentido y desde una perspectiva política, surgen varias recomendaciones:

1. Adaptación legal: Colombia debería clarificar sus marcos legales para definir los umbrales de incidentes cibernéticos que justifiquen la respuesta estatal alineando el derecho interno con las normas internacionales (Delerue, 2020; Cristiano, 2019).
2. Fortalecimiento de capacidades: La inversión en experiencia técnica y legal es imprescindible para mejorar las capacidades de atribución, un factor clave para exigir responsabilidades a los adversarios (Cristiano, 2019; Medina, 2019).

3. Participación internacional: Colombia debería seguir participando en diálogos globales, incluyendo la UNGGE y los foros regionales de ciberdefensa, para definir normas y fortalecer alianzas (Ministerio de Defensa Nacional, 2020).
4. Medidas de resiliencia: Fortalecer la colaboración entre los sectores público y privado garantizará una protección robusta de la infraestructura crítica, una prioridad identificada en la estrategia nacional de Colombia (ESDEG, 2020).

En resumen, la ciberguerra desafía los principios fundamentales del derecho internacional, en particular la soberanía, el uso de la fuerza y la no intervención. Si bien los marcos jurídicos existentes se aplican al ciberespacio, su interpretación y aplicación siguen siendo controvertidas, lo que subraya la necesidad de estrategias adaptativas. Para Colombia, integrar la precisión jurídica, la capacidad técnica y la colaboración diplomática es esencial para afrontar el cambiante panorama de las ciberamenazas. Pero construir una cultura ciberestratégica resiliente en Colombia requiere más que preparación técnica: exige un cambio cultural de carácter sistémico que integre la ciberseguridad en el ADN estratégico del país. Como enfatiza Giraldo (2024), solo mediante un enfoque holístico, en el que se combinen educación, reforma institucional y gobernanza proactiva, Colombia puede asegurar su futuro digital y salvaguardar su soberanía en el cada vez más disputado ciberespacio. La alineación estratégica entre defensa, gobernanza e innovación será decisiva para asegurar la soberanía digital de Colombia en la próxima década.

Conclusiones

Este capítulo ha ilustrado la profunda transformación que ha generado la ciberguerra en la arquitectura de las G5G ofreciendo un análisis crítico de cómo el ámbito digital ha transformado la dinámica estratégica, operativa y política del conflicto. Se ha analizado desde la perspectiva de las características operativas, la explotación asimétrica y las vulnerabilidades nacionales la pregunta central de investigación: ¿Cómo la ciberguerra altera esta dinámica, y qué implicaciones tiene para la seguridad nacional de Colombia?

En primer lugar, el análisis hecho en el presente documento muestra, de forma inequívoca, que la ciberguerra disuelve las fronteras tradicionales entre objetivos civiles y militares, y convierte así la ionósfera nacional en un campo de batalla expandido y persistente. A diferencia de la guerra convencional, las operaciones cibernéticas se infiltran en infraestructuras críticas, erosionan la confianza pública

y manipulan los espacios cognitivos, y ello confirma la hipótesis de que la vulnerabilidad social se ha intensificado drásticamente. Para Colombia eso implica un cambio doctrinal urgente: las estrategias de defensa deben priorizar ahora no solo la seguridad física, sino también la soberanía digital y la resiliencia de los ecosistemas de información.

En segundo lugar, el estudio confirma la potencia asimétrica de la ciberguerra. Tanto los actores estatales como los no estatales aprovechan el anonimato, la asimetría y las operaciones psicológicas para asegurar resultados políticos y estratégicos sin desencadenar respuestas militares convencionales. Ello refleja una lección clave: adversarios con un poderío convencional limitado, como Corea del Norte e Irán, han demostrado su capacidad para infligir daño estratégico mediante sofisticadas campañas cibernéticas. Para Colombia, cuyas capacidades de ciberdefensa siguen en proceso de desarrollo, el riesgo de exposición es mayor, lo que subraya la necesidad de invertir en capacidades de respuesta rápida y medidas de defensa anticipadas.

En tercer lugar, el capítulo destaca las lagunas legales y normativas en la gobernanza de la ciberguerra. Si bien marcos como el Manual de Tallin proporcionan un andamiaje interpretativo, la falta de instrumentos jurídicos internacionales vinculantes facilita la impunidad y la erosión de las normas (Cristiano, 2019; Delerue, 2020). La alineación de Colombia con las normas jurídicas internacionales y su participación activa en los procesos de elaboración de normas son vitales para reforzar su postura de seguridad global, y así garantizar una voz en la evolución de la gobernanza cibernética.

Para afrontar estos desafíos las Fuerzas Militares de Colombia deben emprender un proceso de transformación que integre la ciberdefensa en el núcleo de la doctrina de seguridad nacional. Las siguientes recomendaciones estratégicas son fundamentales:

1. Fortalecer el Conjunto de Operaciones Cibernéticas. Un CCOC debe integrar las capacidades cibernéticas del Ejército, la Armada y la Fuerza Aeroespacial Colombiana garantizando un C-2 unificado sobre las operaciones cibernéticas defensivas y ofensivas. Esto abordaría la fragmentación institucional actual y proporcionaría una dirección estratégica clara.
2. Mejorar la inteligencia cibernética y las capacidades de IVR. Las Fuerzas Militares deben priorizar la inversión en IVR específicas para el ámbito cibernético. Esto incluye el desarrollo de unidades de inteligencia contra cibermenazas capaces de monitorear, analizar y prevenir actividades cibernéticas adversarias, en consonancia con las mejores prácticas globales.

3. Avanzar en las capacidades cibernéticas ofensivas. Para lograr una disuasión creíble, Colombia debe ir más allá de una simple postura defensiva. La integración legal y ética de herramientas cibernéticas ofensivas, como implantes de *malware* y capacidades de disrupción de precisión, debe buscarse en el marco del Derecho Internacional Humanitario (DIH) y la legislación nacional.
4. Integrar las operaciones cibernéticas en ejercicios conjuntos. Los ejercicios militares conjuntos regulares que simulan escenarios complejos de ciberataques son clave para la preparación operativa. Estos ejercicios deben involucrar a agencias civiles y operadores de infraestructura crítica para evaluar la coordinación y la resiliencia.
5. Institucionalizar la capacitación en derecho cibernético. Para garantizar el cumplimiento de las normas internacionales, todo el personal militar involucrado en operaciones cibernéticas debe recibir capacitación obligatoria sobre derecho, ética y derecho de los conflictos armados aplicados al ciberespacio. Esto reforzará la adhesión a los principios del DIH de distinción, proporcionalidad y necesidad.
6. Fortalecer alianzas público-privadas. Dado que gran parte de la infraestructura crítica de Colombia es de propiedad privada, las Fuerzas Militares de Colombia deben establecer protocolos de enlace sólidos con sectores clave como la energía, telecomunicaciones y las finanzas, a fin de garantizar el intercambio rápido de información y una defensa coordinada en situaciones de crisis.
7. Fomentar el talento y la innovación. Las Fuerzas Militares colombianas deben colaborar con universidades e institutos tecnológicos para crear canteras de talento cibernético ofreciendo becas y subvenciones de investigación para formar una nueva generación de cibersoldados.

En resumen, la integración de la ciberguerra en la G5G marca un cambio profundo en el cálculo estratégico de la defensa nacional. Para Colombia, las implicaciones son claras: la resiliencia en el espacio de batalla digital exige una transformación holística de la doctrina, la infraestructura y los marcos legales. Las Fuerzas Militares de Colombia deben evolucionar hacia una fuerza híbrida, capaz de defender no solo la integridad territorial, sino también la soberanía digital, y adherir al mismo tiempo a las normas jurídicas internacionales que salvaguardan a la humanidad incluso en los rincones más oscuros del ciberespacio. A medida que se expande el espacio de batalla, también debe hacerlo la visión colombiana de seguridad, basada en la resiliencia, la adaptabilidad y la solidaridad internacional.

Referencias

- Aanonsen, C. (2025). Stuxnet, revisited (again): producing the strategic relevance of cyber operations. *Journal of Cyber Policy*, 10(1), 68-84.
- Álvarez, C.; Santafé, J. y Urbano, Ó. (2017). Metamorphosis Bellum: ¿Mutando a guerras de quinta generación? En Álvarez, C. (Ed.), *Escenarios y desafíos de la seguridad multidimensional en Colombia* (pp. 145-223). Sello Editorial ESDEG.
- Álvarez, C., Barón, P. y Monroy, V. (2018). Poder astuto: Estrategia del Empleo del Poder en el Siglo XXI. En Álvarez, C. y Fernández, A. (Eds.), *Hacia una Gran Estrategia en Colombia: construcción de política pública en seguridad y defensa* (pp. 171-268). Sello Editorial ESMIC.
- Arquilla, J. y Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. RAND Corporation.
- Arreguín-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. *International Security*, 26(1), 93-128.
- Ashraf, C. (2021). Defining cyberwar: Towards a definitional framework. *Defense & Security Analysis*, 37(3), 274-294.
- Aucsmith, D. (2018). Disintermediation, counterinsurgency, and cyber defense. En Lin, H. y Zegart, A. (Eds.), *Bytes, bombs, and spies* (pp. 343-355). Brookings Institution Press.
- Bach, D. (2021). Hybrid warfare in the Baltics. En Weissmann, M.; Nilsson, N.; Palmertz, B. y Thunholm, P. (Eds.), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 195-213). Bloomsbury Publishing.
- Baig, M. (2019). An analysis of North Korean cyber warfare capabilities and impact on USFK and USINDOPACOM. *Journal of Cyber Security Technology*, 3(4), 219-248.
- Bebber, R. (2017). Cyber power and cyber effectiveness: An analytic framework. *Comparative Strategy*, 36(5), 426-436.
- Bellovin, S.; Landau, S. y Lin, H. (2018). Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications. En Lin, H. y Zegart, A. (Eds.), *Bytes, bombs, and spies* (pp. 265-288). Brookings Institution Press.
- Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.
- Caruso, J. (2024). Inside cyber warfare: Mapping the cyber underworld. O'Reilly Media.
- Chen, C.; Ko, K. y Lee, J. (2010). North Korea's Internet strategy and its political implications. *The Pacific Review*, 23(5), 649-670.
- Cheng, D. (2017). *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*. Praeger.
- Clarke, R. y Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it*. Ecco.

- Colarik, A. y Janczewski, L. (2019). Establishing Cyber Warfare Doctrine. En Lemieux, F. (Ed.), *Current and Emerging Trends in Cyber Operations: Policy, Strategy, and Practice* (pp. 37-50). Palgrave Macmillan.
- Conway, M. (2003). What is cyberterrorism? The story so far. *Journal of Information Warfare*, 2(2), 33-42.
- Couretas, J. (2024). *Cyber Operations: A Case Study Approach*. Wiley.
- Cristiano, F. (2019). Internet access as a human right: A dystopian critique. In Blouin-Genest, M; Doran, C. y Paquerot, S. (Eds.), *Human Rights as Battlefields: Changing Practices and Contestations* (pp. 249-266). Palgrave Macmillan.
- Crowther, A. (2021). NATO and hybrid warfare: Seeking a concept to describe the challenge from Russia. En Weissmann, M.; Nilsson, N.; Palmertz, B. y Thunholm, P. (Eds.), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 21-35). Bloomsbury Publishing.
- Davis, E. (2021). *Shadow Warfare: Cyberwar Policy in the United States, Russia, and China*. Rowman & Littlefield.
- Delerue, F. (2020). *Cyber operations and international law*. Cambridge University Press.
- Echevarria II, A. (2005). *Fourth-Generation War and Other Myths*. Strategic Studies Institute, U.S. Army War College.
- Egloff, F. y Smeets, M. (2023). Publicly Attributing Cyber Attacks: A Framework. *Journal of Strategic Studies*, 46(3), 502-533.
- Eklund, Ay y Djup, A. (2021). Cyberwarfare and the internet: The implications of a more digitalized world. En Weissmann, M.; Nilsson, N.; Palmertz, B. y Thunholm, P. (Eds.), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 145-156). Bloomsbury Publishing.
- ESDEG (2020). *Estrategia Nacional de Ciberdefensa y Ciberseguridad 2020-2030*. Sello Editorial ESDEG.
- Farrell, H. y Glaser, C. (2018). How Effects, Saliencies, and Norms Should Influence U.S. Cyberwar Doctrine. En Lin, H. y Zegart, A. (Eds.), *Bytes, bombs, and spies* (pp. 45-80). Brookings Institution Press.
- Galula, D. (2006). *Counterinsurgency Warfare: Theory and Practice*. Praeger.
- Giraldo, L. (2024) Definición e impacto en la transformación digital y la ciberseguridad. En Realpe, M. y González, A. (Eds.), *Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio* (pp. 15-46). Sello Editorial ESDEG
- Göransson, M. (2021). Understanding Russian thinking on gibrdnaya voyna. En Weissmann, M.; Nilsson, N.; Palmertz, B. y Thunholm, P. (Eds.). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 83-95). Bloomsbury Publishing.
- Harrop, W. y Matteson, A. (2019). Cyber Resilience: A Review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK and USA. En Lemieux, F. (Ed.), *Current and Emerging Trends in Cyber Operations: Policy, Strategy, and Practice* (pp. 149-166). Palgrave Macmillan.

- Healey, J. (2018). The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities. En Lin, H. y Zegart, A. (Eds.), *Bytes, bombs, and spies* (pp. 173-194). Brookings Institution Press.
- Inglis, C. (2018). Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace. En Lin, H. y Zegart, A. (Eds.), *Bytes, bombs, and spies* (pp. 19-44). Brookings Institution Press.
- Jones-Chaljub, S. (2022). *Conceptualización del ciberespacio humano*. Sello Editorial ESDEG.
- Kello, L. (2018). Private Sector Cyber Weapons: An Adequate Response to the Sovereignty Gap? En Lin, H. y Zegart, A. (Eds.), *Bytes, bombs, and spies* (pp. 357-378). Brookings Institution Press.
- Koh, H. H. (2013). International law in cyberspace. *Harvard International Law Journal*, 54(1), 1-26.
- Lindsay, J. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3), 365-404.
- Lindsay, J. (2025). Stuxnet revisited: From cyber warfare to secret statecraft. *Journal of Strategic Studies*, 48(4), 834-873.
- Loukas, G. (2015). *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann.
- Lynn III, W. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 89(5), 97-108.
- Mack, A. (1975). Why big nations lose small wars: The politics of asymmetric conflict. *World Politics*, 27(2), 175-200.
- Maldonado, C. (2024). En Ciencias de punta y tecnologías disruptivas en el ciberespacio como marco y condición para la ciberdefensa de Colombia. En Realpe, M. y González, A. (Eds.), *Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio* (pp. 111-142). Sello Editorial ESDEG.
- Medina, G. (2019). *La seguridad en el ciberespacio: Un desafío para Colombia*. Sello Editorial ESDEG.
- Mehan, J. (2008). *CyberWar, CyberTerror, CyberCrime*. IT Governance Publishing.
- Moulton, H.; Stavridis, J. y Uthoff, C. (2019). A National Strategy for the United States Cyberspace. En Lemieux, F. (Ed.), *Current and Emerging Trends in Cyber Operations: Policy, Strategy, and Practice* (pp. 113-129). Palgrave Macmillan.
- NIC (2024). *Updated IC Gray Zone Lexicon: Key Terms and Definitions*. Office of the Director of National Intelligence.
- Oakley, J. (2019). *Waging cyber war: Technical challenges and operational constraints*. Apress.
- O'Leary, M. (2019). *Cyber operations: Building, defending, and attacking modern computer networks*. Apress.
- Ormrod, D. y Turnbull, B. (2016). The cyber conceptual framework for developing military doctrine. *Defence Studies*, 16(3), 268-290.

- Poznansky, M. (2022). Revisiting plausible deniability. *Journal of Strategic Studies*, 45(4), 511-533.
- Realpe, M. (2024). El poder en la era digital: perspectivas sobre el ciberpoder. En Realpe, M. y González, A. (Eds.), *Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio* (pp. 143-166). Sello Editorial ESDEG
- Richards, J. (2014). *Cyber war: The anatomy of the global security threat*. Palgrave Macmillan.
- Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5-32.
- Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford University Press.
- Rid, T. y Buchanan, B. (2015) Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(2), 4-37.
- Saalman, L. (2021). China and its hybrid warfare spectrum. En Weissmann, M.; Nilsson, N.; Palmertz, B. y Thunholm, P. (Eds), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 95-112). Bloomsbury Publishing.
- Sanger, D. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. Crown.
- Scherkeller, M.; Goldman, E. y Harknett, A. (2022). *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Oxford University Press.
- Schmitt, M. y Vihul, L. (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
- Sersicov, G. (2025). The role of strategic culture in shaping Iran's cyber defense policy. *International Journal of Intelligence and CounterIntelligence*, 38(2), 658-689.
- Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies*, 40(7), 898-926.
- Smeets, M. y Lin, H. (2018). A Strategic Assessment of the U.S. Cyber Command Vision. En Lin, H. y Zegart, A. (Eds.), *Bytes, bombs, and spies* (pp. 81-104). Brookings Institution Press.
- Smith III, F; Kollars, N. y Schechter, B. (2023). Shall We Play a Game? Fundamentals of Cyber Wargaming. En Smith III, F; Kollars, N. y Schechter, B. (Eds), *Cyber Wargaming: Research and Education for Security in a Dangerous Digital World* (pp. 1-20). Georgetown University Press.
- Sweet, J. (2024). *Russian Hackers and the War in Ukraine: Digital Threats and Real-World Consequences*. Lexington Books.
- Valeriano, B y Maness, R. (2012, noviembre). The Fog of Cyberwar: Why the Threat Does Not Live up to the Hype. *Foreign Affairs*. <https://www.foreignaffairs.com/articles/2012-11-21/fog-cyberwar>
- Weissmann, M. (2021). Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone. En Weissmann, M.; Nilsson, N.; Palmertz, B. y Thunholm, P. (Eds), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 61-82). Bloomsbury Publishing.
- Warf, B. (2015). The Hermit Kingdom in cyberspace: Unveiling the North Korean internet. *Information, Communication & Society*, 18(1), 109-120.

- White, G. (2022). *The Lazarus Heist - From Hollywood to High Finance: Inside North Korea's Global Cyber*. Penguin Random House
- Whyte, C. (2016). Ending cyber coercion: Computer network attack, exploitation, and the case of North Korea. *Comparative Strategy*, 35(2), 93-102.
- Whyte, C. y Mazanec, B. (2023). *Understanding Cyber Warfare: Politics, Policy and Strategy*. Routledge.
- Willett, M. (2024). A short history of cyber operations. *Adelphi Series*, 64, 63-104.

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 (Lonergan & Lonergan, 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. Lonergan y Lonergan (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 interrupción 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. Zwilling 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.

Capítulo 6

El intercambio de información de ciberseguridad y ciberdefensa en las Fuerzas Militares de Colombia*

DOI: <https://doi.org/10.25062/9786287818705.06>

Diego Edison Cabuya Padilla

Hernán Darío Ochoa Góez

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente capítulo analiza los métodos actuales y propuestos para el intercambio de información en el ámbito de la ciberseguridad y la ciberdefensa, con especial énfasis en su aplicación en las Fuerzas Militares de Colombia. Se abordan, en primer lugar, los fundamentos del intercambio de información desde la perspectiva de la ciberseguridad, la ciberdefensa, la ciberinteligencia y las amenazas en redes, destacando la importancia de proteger la información clasificada en contextos operacionales y estratégicos. Posteriormente, se estudian prácticas internacionales empleadas por Fuerzas Militares de otros Estados, evidenciando modelos como el estadounidense y el brasileño, junto con sus estructuras de intercambio, clasificación, operaciones y capacidades tecnológicas. En paralelo, se analiza el sistema colombiano: su evolución normativa, institucional y doctrinal, así como los desafíos en interoperabilidad, gestión del riesgo y articulación interagencial. Como contribución central, se presenta una propuesta conceptual de método de intercambio de información cibernética, estructurada sobre seis componentes clave: marco normativo y doctrinal, criterios técnicos de clasificación, sistema nacional de intercambio, plataforma digital interoperable, gobernanza institucional y esquema de confianza compartida. La propuesta responde a la necesidad de anticiparse a amenazas emergentes, proteger infraestructuras críticas y articular los niveles estratégico, operacional y táctico de la ciberdefensa nacional.

Palabras clave: ciberdefensa, ciberinteligencia, ciberseguridad, intercambio de información cibernética, riesgos cibernéticos.

* Este capítulo de libro presenta los resultados del proyecto de investigación titulado "La Gobernanza del Ciberespacio: Desafíos y Oportunidades en procura de la autonomía y el control en el entorno Digital", vinculado a la línea de investigación Tecnología e Innovación en Defensa, del grupo de investigación "Ciberespacio, Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado como 'C' por MinCiencias y con código de registro COL0181179. Los puntos de vista pertenecen a los autores, y no necesariamente reflejan los de las instituciones participantes.

Diego Edison Cabuya Padilla

Doctor en Ciencias del Mar con énfasis en ciberseguridad y ciberdefensa marítima, Escuela Naval de Cadetes “Almirante Padilla”, Colombia. Magíster en Gestión Logística y en Gestión de la Información. Ingeniero Electrónico. Administrador de Empresas. Profesional en Ciencias Navales. Docente e investigador, Escuela Naval de Cadetes y de la Escuela Superior de Guerra. Investigador asociado de MinCiencias

<https://orcid.org/0000-0001-5338-9943> - Contacto: diego.cabuya@esdeg.edu.co

Hernán Darío Ochoa Góez

Magíster en Ciberseguridad y Ciberdefensa, y magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia. Profesional en Relaciones Internacionales y Estudios Políticos, Universidad Militar Nueva Granada, Colombia. Oficial de Inteligencia Naval de la Armada Nacional.

<https://orcid.org/0009-0007-8979-1521> - Contacto: hernan.ochoa@armada.mil.co

Citación APA: Cabuya Padilla, D. E. & Ochoa Góez, H. D. (2026). El intercambio de información de ciberseguridad y ciberdefensa en las Fuerzas Militares de Colombia. 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, ciber-guerra y defensa del ciberespacio)* (pp. 379-408). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818705.06>

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

El ciberespacio ha desdibujado las fronteras tradicionales, y se ha consolidado como un nuevo dominio de confrontación estratégica donde los Estados y sus fuerzas militares enfrentan amenazas cibernéticas orientadas a desestabilizar sus intereses. En dicho escenario, la ciberdefensa ha sido incorporada a la agenda de seguridad nacional como responsabilidad directa de las fuerzas armadas, dadas las implicaciones operacionales, económicas, políticas y sociales de posibles ataques.

Las ciberamenazas —como el ciberespionaje, el terrorismo digital y la ciberdelincuencia— representan riesgos transnacionales que superan incluso los conflictos armados tradicionales. Los ataques cibernéticos, difíciles de atribuir, pueden afectar gravemente la seguridad nacional y causar daños irreversibles a infraestructuras críticas (IC) y sistemas de información. En Colombia estos sistemas, particularmente los de uso militar, se hallan expuestos a riesgos crecientes, debido a la necesidad de mantener información clasificada disponible en entornos vulnerables.

Para hacer frente a este desafío, el país ha avanzado en el desarrollo de capacidades institucionales como el Comando Conjunto Cibernético (CCOCI) y el Grupo de Respuesta a Emergencias Cibernéticas (ColCERT), creados para prevenir, detectar y responder a amenazas informáticas. No obstante, persisten desafíos estructurales como la escasez de recursos, la limitada interoperabilidad entre agencias y la necesidad de fortalecer la cooperación internacional.

Conceptualmente, la respuesta nacional se apoya en tres pilares: la ciberseguridad, orientada a proteger la confidencialidad, integridad y disponibilidad de la información; la ciberdefensa, centrada en la protección de infraestructuras estratégicas, y la ciberinteligencia, enfocada en la identificación y anticipación de amenazas de origen ciberterrorista.

A pesar de estos avances, el volumen y la sensibilidad de la información que se genera y circula diariamente en el entorno de la defensa nacional hacen imperativo

montar mecanismos seguros, estructurados y ágiles para su intercambio. Según el informe *X-Force Threat Intelligence Index*, de IBM (2025), Colombia es uno de los países más vulnerables de la región frente a ciberataques, junto con Argentina, Chile y Brasil.

En respuesta, Colombia ha reforzado su marco de cooperación internacional. En 2013 suscribió un acuerdo con la Organización del Tratado del Atlántico Norte (OTAN) sobre seguridad de la información, desde 2016 participa activamente en el Foro Iberoamericano de Defensa Cibernética y en 2024 entró oficialmente al Centro de Competencia Cibernética de América Latina y el Caribe (LAC4). Todas ellas son participaciones de Colombia en contextos internacionales que promueven el intercambio de conocimientos en la materia.

Estos antecedentes evidencian la urgencia de implementar un método seguro y estandarizado de intercambio de información, alineado con las necesidades operacionales y los protocolos vigentes. La tendencia regional confirma que las Fuerzas Armadas están priorizando la inversión en capacidades de ciberseguridad, no como medida reactiva, sino como un enfoque preventivo frente a amenazas persistentes (Cornaglia & Vecelli, 2017).

En el contexto descrito, la presente investigación propone un método para optimizar el intercambio de información de ciberseguridad y ciberdefensa entre las Fuerzas Militares de Colombia. Su propósito es mejorar los procesos operacionales mediante la estandarización de mecanismos seguros y eficaces, fortalecer la base institucional de conocimiento y contribuir al desarrollo de capacidades cibernéticas alineadas con las exigencias estratégicas del país.

El objetivo central es identificar las bases de un modelo conceptual viable de intercambio de información que pueda ser adoptado operacionalmente por las Fuerzas Militares. En este marco se plantea la siguiente pregunta de investigación: ¿Qué método de intercambio de información de ciberseguridad y ciberdefensa debería adoptar Colombia para sus Fuerzas Militares?

El intercambio de información desde la ciberseguridad, la ciberdefensa, la ciberinteligencia y las amenazas de las redes de información

La globalización y los retos del siglo XXI han introducido al ciberespacio como un nuevo dominio de confrontación, donde convergen los intereses estratégicos de los Estados y sus fuerzas militares con amenazas que buscan desestabilizar el orden institucional mediante el uso malicioso de las redes de información

(Cabuya-Padilla & Castaneda-Marroquin, 2024). En tal escenario, los sistemas de información de las Fuerzas Militares de Colombia se enfrentan a un riesgo creciente, dado que su exposición constante a redes digitales —imprescindible para asegurar la disponibilidad y actualización de información— también incrementa su vulnerabilidad. Esta información, en su mayoría, tiene carácter confidencial y es clave para el funcionamiento institucional y la seguridad nacional.

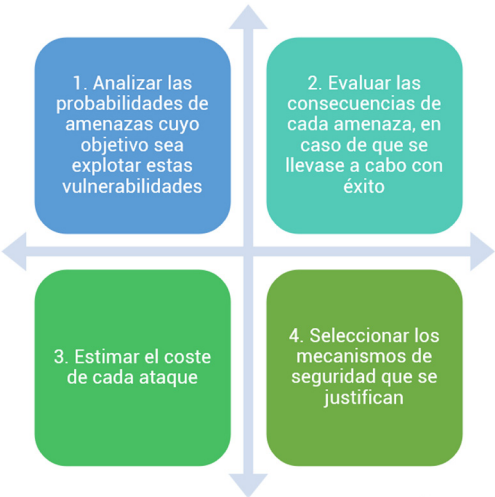
Para comprender la relevancia del ciberespacio y del intercambio seguro de información en el ámbito militar, se propone un marco conceptual que articula la ciberseguridad, la ciberdefensa y la ciberinteligencia, con el objetivo de analizar y enfrentar las amenazas que afectan directamente la integridad, disponibilidad y confidencialidad de las redes de información de las Fuerzas Militares.

La ciberinteligencia

La ciberinteligencia surge como una necesidad estratégica en un entorno intangible —el ciberespacio— que, si bien facilita las interacciones sociales y operativas, también representa un campo de riesgos latentes para la seguridad y defensa nacionales. Su función esencial es recolectar, procesar y analizar información que permita identificar actores hostiles, como ciberterroristas, sus capacidades y objetivos, para anticipar posibles ataques y proteger la infraestructura crítica del Estado.

La figura 1 ilustra las principales medidas de ciberinteligencia orientadas a identificar vulnerabilidades y desafíos en el sistema.

Figura 1. Medidas desde la ciberinteligencia para identificar las vulnerabilidades y desafíos del sistema



Fuente: elaboración propia, con base en (UIT, 2015).

Según Enrique Cubeiro (2016, pág. 50), la ciberinteligencia se sustenta en el reconocimiento del ciberespacio como la mayor fuente de datos provenientes de fuentes abiertas. Las herramientas empleadas permiten obtener información según parámetros complejos, incluso desde la web profunda, apoyando el ciclo de inteligencia mediante funciones como traducción automática, geolocalización y representación gráfica de relaciones entre identidades digitales.

Complementariamente, Gruszczak (2016) amplía esta visión al destacar que la ciberinteligencia opera sobre fuentes tanto abiertas como cerradas, lo cual reafirma su papel estratégico en la vigilancia proactiva del ciberespacio. Ante incidentes de ciberseguridad, esta disciplina resulta crucial para rastrear el origen de las amenazas, interpretar sus implicaciones y generar escenarios de respuesta que faciliten la toma de decisiones en contextos de crisis.

La ciberseguridad y la ciberdefensa

La ciberseguridad se entiende como el conjunto organizado de medidas destinadas a prevenir, evitar y minimizar potenciales daños a redes y sistemas de información propios (Ganuza, 2020). En el contexto del Estado, dicha disciplina resulta decisiva para garantizar el resguardo de la información crítica en entornos cada vez más digitalizados y expuestos a amenazas complejas y persistentes.

El Manual de Seguridad de las TIC, del Centro Criptológico Nacional, define la ciberseguridad como “las medidas para proteger la información almacenada, procesada o transmitida por los Sistemas de Información, de manera que se aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios sistemas” (Centro Criptológico Nacional, 2021).

La gestión de la seguridad de los datos no se limita únicamente al plano técnico. Implica también considerar aspectos como la seguridad personal, la protección de instalaciones, la salvaguarda de documentación y la integridad de los propios sistemas TIC. La ciberseguridad, en ese sentido, adquiere un rol operativo, al asegurar el funcionamiento continuo de los sistemas de información frente a amenazas de tipo ciberterrorista o ataques deliberados.

Por su parte, la ciberdefensa se define como el uso de las “capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional o los intereses nacionales” (Departamento Nacional de Planeación, 2017). Esta capacidad va más allá de la

protección pasiva de la información, al integrar una dimensión activa, estratégica y táctica en la defensa de infraestructuras críticas, redes militares y plataformas tecnológicas frente a ciberataques sofisticados.

La figura 2 presenta la clasificación de las capacidades de ciberdefensa, y destaca los distintos niveles y componentes que conforman una arquitectura de defensa efectiva en el ciberespacio.

Figura 2. Clasificación de las capacidades de la ciberdefensa



Fuente: elaboración propia, con base en Organización Tratado Atlántico Norte (OTAN, 2016).

Tipos de información en ciberseguridad y ciberdefensa

En el marco de las operaciones de ciberseguridad y ciberdefensa, es fundamental distinguir los distintos tipos de información que sirven de insumo para la toma de decisiones estratégicas y operacionales. Esta información se clasifica principalmente en dos enfoques: inteligencia cibernética y ciberinteligencia.

En primer lugar, la *inteligencia cibernética* se refiere a la información necesaria para el funcionamiento, mantenimiento y mejora de los sistemas de protección y defensa cibernética. Según el Instituto Nacional de Ciberseguridad de España (INCIBE, 2018), esta puede categorizarse en cinco tipos esenciales:

- Indicadores de compromiso (IoC): evidencias técnicas de que un sistema ha sido vulnerado o está siendo atacado, como direcciones IP maliciosas, firmas de *malware* o patrones de tráfico anómalo.
- Técnicas, Tácticas y Procedimientos (TTPs): conocimiento detallado de los métodos utilizados por los atacantes para planear y ejecutar ciberataques.
- Alertas de seguridad: notificaciones que advierten sobre vulnerabilidades activas, amenazas emergentes o campañas de ataques en curso.
- Informes de inteligencia de amenazas: análisis más elaborados sobre el contexto, motivación, capacidades y objetivos de los actores hostiles.
- Información generada automáticamente por herramientas de seguridad: datos obtenidos en tiempo real por sistemas de detección de intrusos, *firewalls* o antivirus, entre otros.

En segundo lugar, el enfoque de *ciberinteligencia* amplía el espectro de análisis al integrar la recopilación de información táctica y estratégica del ciberespacio, orientada a objetivos militares específicos. Esta incluye los mismos elementos de la inteligencia cibernética, pero los adapta y extiende según los requerimientos operacionales, y así permite anticipar movimientos del adversario, evaluar vulnerabilidades en IC y fortalecer capacidades defensivas en tiempo real.

Ambos tipos de información deben ser gestionados por plataformas automáticas de intercambio y análisis, diseñadas para procesar grandes volúmenes de datos y facilitar su distribución oportuna. Estas plataformas de inteligencia sobre amenazas deben permitir:

- La correlación de indicadores entre actores institucionales.
- El almacenamiento seguro de información crítica.
- La generación de conocimiento útil para acciones preventivas y de detección temprana.

Este tipo de arquitectura colaborativa facilita construir una red de cooperación nacional sobre amenazas cibernéticas, con miras a una respuesta coordinada, efectiva y basada en evidencia ante ataques dirigidos.

Ciberamenazas

El ciberespacio ha redefinido las dinámicas del sistema internacional, e impulsado así el desarrollo de nuevas tecnologías y fomentado el uso masivo de internet. Sin embargo, dicha transformación ha generado nuevos desafíos de seguridad que afectan a todos los actores, en particular a los Estados. Entre tales desafíos se destacan el ciberespionaje, las operaciones de grupos terroristas, la ciberdelincuencia y la protección de infraestructuras críticas, todos ellos en expansión dentro de un entorno altamente digitalizado y deslocalizado.

Las amenazas cibernéticas dificultan la atribución de responsabilidades, debido a su capacidad para ejecutarse desde cualquier parte del mundo y a través de múltiples capas de ocultamiento. Como señaló el exfiscal Jesús Cardenal en 2019, “la comunicación en redes entre terroristas y los sabotajes informáticos son delitos que crecerán un 10.000 %” (Escuela Superior de Guerra., 2019). Esta advertencia anticipaba el crecimiento exponencial del cibercrimen y su complejidad operativa.

Los Estados son blanco habitual de ciberataques provenientes de otros actores estatales o no estatales, motivados por intereses políticos, económicos, geoestratégicos o militares. Estos ataques presentan ventajas tácticas para los ofensores: bajo costo, alto impacto potencial, baja exposición directa y dificultad para atribuirlos. Incluso, la infraestructura tecnológica de un tercer país puede ser empleada como plataforma intermedia para ejecutar el ataque, lo cual refuerza el anonimato del agresor (Villalba, & Corchado, 2017).

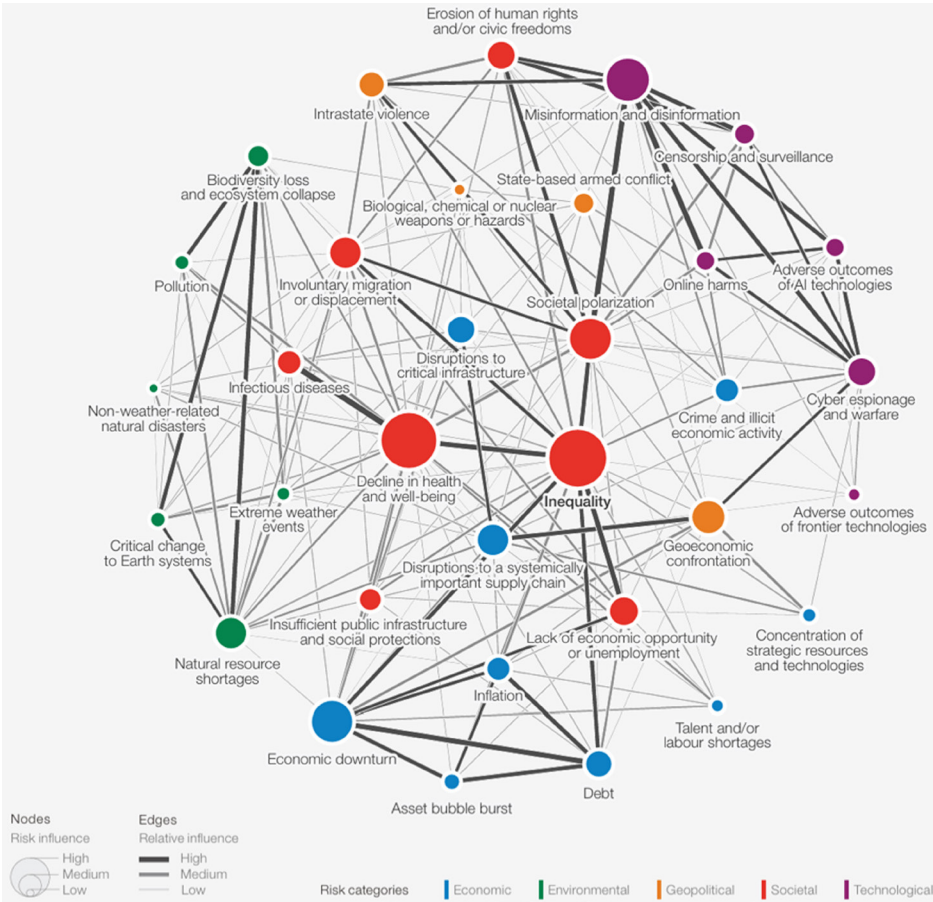
Ante el panorama descrito, la ciberseguridad y la ciberdefensa deben articular estrategias operacionales mediante el control de sistemas institucionales de información. Su objetivo es planear, anticipar, dirigir y ejecutar acciones defensivas permanentes en el ciberespacio protegiendo la confidencialidad, disponibilidad e integridad de las tecnologías de la información y la comunicación (TIC) frente a amenazas ciberterroristas.

Desde hace más de una década el World Economic Forum ha ubicado las amenazas cibernéticas y al entorno de la información entre los principales riesgos globales, junto a eventos como los desastres naturales o las crisis económicas. En su informe de 2025 se estimó que los delitos cibernéticos generan pérdidas globales anuales por más de 445 mil millones de dólares, lo que supera incluso los ingresos anuales de economías como la chilena (World Economic Forum, 2025).

El informe identifica a los ciberataques y la creciente ciberdependencia como amenazas de alta probabilidad e impacto, que ya superan en relevancia a riesgos tradicionales como el desempleo o los conflictos interestatales. En el mapa global

de interconexión de riesgos 2025 (figura 3), los ciberataques aparecen vinculados directamente con otros riesgos sistémicos: interrupciones en IC, mal uso de tecnologías y robo y fraude de datos, así como fallos en la gobernanza nacional, terrorismo y tensiones geopolíticas. Esta red de conexiones refuerza la idea de que las amenazas cibernéticas no pueden entenderse de forma aislada, sino como elementos catalizadores de crisis multidimensionales.

Figura 3. Mapa de interconexión de los riesgos



Fuente: (World Economic Forum, 2025, pág. 9).

Para que los Estados desarrollen una comprensión efectiva de las ciberamenazas deben considerar tres elementos fundamentales (Villalba, A., & Corchado, J, 2017):

- Intereses: Se refiere a los activos que pueden verse comprometidos por ciberataques, especialmente los vinculados con la seguridad y defensa nacional. Entre ellos destacan la confidencialidad, disponibilidad, trazabilidad y autenticidad de la información institucional.
- Amenazas: hace alusión a los objetivos, eventos y actividades que, ejecutadas por actores hostiles —como ciberterroristas o servicios de inteligencia hostiles—, tienen capacidad para afectar los intereses estratégicos de un Estado.
- Resiliencia: implica la capacidad de los sistemas de información para resistir, absorber y recuperarse de un ciberataque. Esto incluye tanto la ausencia de vulnerabilidades como la existencia de mecanismos de respuesta y estrategias de mitigación eficaces.

Dentro del conjunto de amenazas persistentes, el espionaje cibernético representa uno de los mayores desafíos. Este es impulsado a menudo por servicios de inteligencia extranjeros que operan al servicio de organizaciones hostiles. Dichos actores suelen disponer de abundantes recursos técnicos, humanos y financieros, así como de acceso a herramientas de ataque de procedencia diversa, muchas veces desarrolladas internamente.

Estados con regímenes autoritarios o sin controles democráticos efectivos disfrutan de mayores márgenes de maniobra en el ciberespacio. Aunque existe un consenso internacional sobre la aplicación del derecho internacional al ciberespacio, estos actores operan al margen de las normativas ejecutando operaciones ofensivas sin supervisión jurídica ni restricciones estatales. Esa ventaja táctica les permite llevar a cabo acciones altamente eficaces con bajo riesgo de atribución o represalia.

El informe conjunto del Centro Nacional de Inteligencia (CNI) y el CCN-CERT identificó cuatro vectores de ataque recurrentes en operaciones de ciberespionaje (CCN-CERT, 2008):

- Primer vector: obtención de información estratégica. Se basa en la recolección masiva y automática de datos provenientes de internet y de las comunicaciones entre nodos. El tráfico no cifrado resulta particularmente vulnerable, ya que puede ser interceptado y analizado fácilmente.
- Segundo vector: ataques dirigidos. Se ejecutan contra sistemas específicos pertenecientes a individuos u organizaciones de interés estratégico. Las herramientas de ataque son diseñadas a medida, utilizando información técnica y de ingeniería social previamente recopilada sobre la víctima.

- Tercer vector: debilitamiento de estándares técnicos. Consiste en manipular o vulnerar implementaciones criptográficas generando fallas deliberadas, que pueden ser explotadas posteriormente para comprometer la seguridad de los sistemas.
- Cuarto vector: manipulación selectiva de sistemas. Se centra en la modificación de equipos o servicios mediante la inserción de puertas traseras, alteraciones en la seguridad perimetral o configuraciones comprometidas, para así facilitar futuras intrusiones o accesos no autorizados durante fases posteriores del ataque.

Dada la creciente sofisticación y el impacto potencial de los ciberataques, varios Estados han incorporado explícitamente las operaciones cibernéticas como parte fundamental de su estrategia militar. Dichas acciones, ejecutadas tanto por actores estatales como por organizaciones criminales cibernéticas, tienen como propósito interferir en el desarrollo de operaciones militares convencionales o afectar infraestructuras críticas del adversario.

Los programas de ciberataques —por su naturaleza indirecta— están diseñados para inutilizar redes de comunicaciones, paralizar infraestructuras logísticas o comprometer sistemas esenciales como los de salud pública y respuesta a emergencias. En tales casos, aunque el ataque no se realiza mediante medios cinéticos, sus efectos son directos y estratégicos (Villalba & Corchado, 2017).

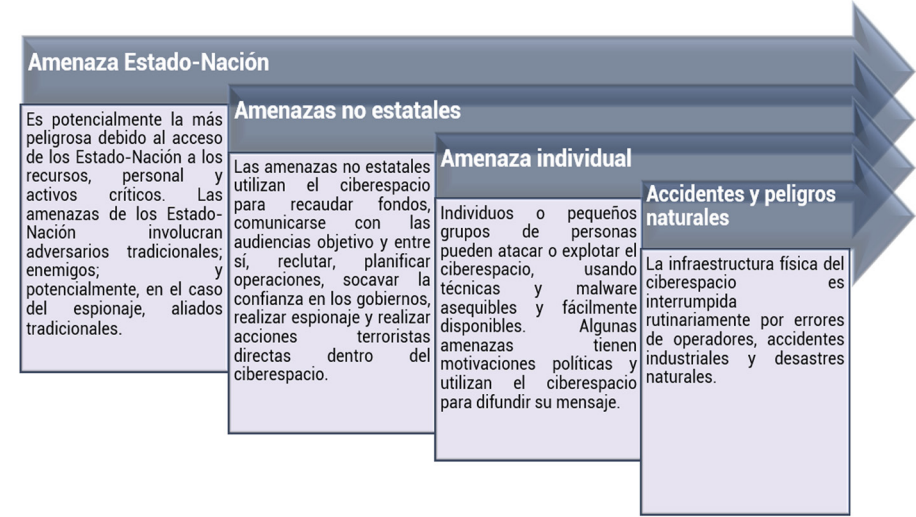
En el caso de Colombia, se han clasificado los desafíos cibernéticos en cuatro grandes categorías, según el enfoque adoptado en cooperación con el Gobierno de Estados Unidos (2018):

- Amenazas y anonimato: Dificultades para identificar con precisión a los actores hostiles y atribuir responsabilidades.
- Geografía: Limitaciones impuestas por la distribución territorial y la cobertura de infraestructura digital.
- Tecnología: Brechas tecnológicas que impiden una respuesta eficaz y autónoma.
- Infraestructura pública e industria privada: Necesidad de coordinación entre sectores críticos que comparten la responsabilidad de la seguridad cibernética.

Estos elementos se integran en la figura 4, la cual sintetiza los desafíos principales que enfrentan las Fuerzas Militares de Colombia en el entorno cibernético.

Esta clasificación permite priorizar capacidades, orientar recursos y definir estrategias diferenciadas según el tipo de riesgo identificado.

Figura 4. Clasificación de desafíos cibernéticos



Fuente: Elaboración propia, con base en (Gobierno de Estados Unidos de América, 2018).

En síntesis, el intercambio de información en las Fuerzas Militares de Colombia requiere una integración articulada entre ciberseguridad, ciberdefensa y ciberinteligencia, concebidas como capacidades complementarias frente a amenazas persistentes y en evolución. La identificación temprana de actores maliciosos, vulnerabilidades críticas y vectores de ataque, junto con el despliegue de tecnologías especializadas y plataformas seguras, resulta decisiva para anticipar, mitigar y neutralizar incidentes cibernéticos. Una adecuada gestión de la información clasificada y operativa no solo refuerza la protección de la infraestructura crítica nacional, sino que también fortalece la postura estratégica del país en el escenario global de confrontación digital.

Sistemas de intercambio de información cibernética utilizados por los Estados

Tomando en cuenta que los ciberataques afectan directamente la estabilidad y desarrollo de los Estados, muchos gobiernos ya han implementado capacidades

para llevar a cabo operaciones y estrategias desde sus fuerzas militares en el ciberespacio. Los cibercriminales operan con el objetivo de destruir o inutilizar las redes de información de las instituciones para usarla a su favor o hacer inaccesible su información.

Las Fuerzas Militares de Estados son instituciones que manejan una gran cantidad de información confidencial, y de ello depende el éxito de las operaciones que tienen como fin la garantía de la Seguridad y Defensa Nacionales. Por tal motivo, desde el Ministerio de Defensa Nacional de cada estado deben adoptarse medidas orientadas a proteger, monitorizar, analizar, detectar y responder a los ataques encaminados a dañar o comprometer las redes o los sistemas de información.

Con el fin de examinar las falencias existentes en el método de intercambio de información de las Fuerzas Militares de Colombia, en las siguientes páginas se hace un análisis comparado entre los sistemas de información de otros Estados y el sistema que usan las Fuerzas Militares de Colombia, a fin de tomar dichos casos como lecciones aprendidas.

Modelos internacionales de intercambio de información cibernética en las Fuerzas Armadas

En el actual escenario geopolítico, el ciberespacio se ha vuelto un nuevo dominio de confrontación estratégica. Ante el aumento de incidentes cibernéticos a gran escala, los Estados han activado mecanismos de alerta y han reforzado el papel de sus fuerzas armadas priorizando la capacidad para identificar, contener y responder a amenazas emergentes. En ese contexto, el intercambio seguro de información sensible constituye un componente crítico para lograr los objetivos estratégicos nacionales (Saz, 2016).

Los servicios de inteligencia son clave en la defensa frente a ataques cibernéticos, los cuales pueden afectar IC y desestabilizar sistemas políticos o económicos. La creciente vulnerabilidad digital exige plataformas tecnológicas robustas, redes intrínsecamente seguras y capacidades especializadas dentro de las estructuras militares para garantizar una respuesta oportuna y eficaz.

El intercambio de información en el ámbito de la inteligencia militar exige protocolos estrictos de seguridad que garanticen la protección de datos sensibles. A nivel internacional, las doctrinas de inteligencia varían: mientras en Europa el énfasis está en la obtención y análisis de datos para generar conocimiento estratégico, en América Latina persiste cierta ambigüedad conceptual entre los términos "información" e "inteligencia". En Estados Unidos, el concepto de inteligencia ha sido estandarizado desde finales del siglo XX, influenciado por su evolución doctrinal

en las distintas ramas de sus fuerzas armadas, y formalizado en agencias como el CNI español, anteriormente conocido como CESID (Sainz, 2012).

La eficacia en la toma de decisiones operacionales depende en gran medida del flujo oportuno y seguro de información hacia los niveles de mando. En el contexto actual, el ciberespacio se ha consolidado como el medio idóneo para la transmisión de datos estratégicos, lo cual exige que los sistemas de inteligencia operen de manera articulada desde el nivel táctico. Sin garantías de seguridad en la información, el éxito de una operación puede verse comprometido seriamente.

Según datos de la Organización de Estados Americanos (OEA, 2019), el manejo de información clasificada en los Estados es altamente reservado. Aunque existen acuerdos bilaterales y multilaterales, los mecanismos específicos para el intercambio no se hacen públicos, dada su naturaleza crítica y el alto riesgo asociado a su exposición.

A pesar de los esfuerzos por adoptar una Estrategia de Seguridad Cibernética común, la respuesta de los Estados miembros frente a la delincuencia cibernética sigue siendo desigual. La mayoría reconoce el impacto negativo de las amenazas cibernéticas sobre las capacidades de defensa, pero enfrenta limitaciones estructurales.

En América Latina, dos factores son en especial críticos: la escasez de recursos dedicados a fortalecer las capacidades de ciberseguridad y la falta de personal especializado con experiencia práctica para implementar políticas eficaces (OEA, 2019).

Los países que han logrado avances significativos en materia de seguridad cibernética han invertido sostenidamente en el desarrollo de plataformas seguras, redes intranet robustas y personal capacitado en ciberdefensa. La OEA, por su parte, promueve programas de intercambio de buenas prácticas entre sus Estados miembros, orientados a fortalecer los sistemas nacionales y garantizar la circulación segura de información sensible dentro de las instituciones gubernamentales.

Los grupos de delincuencia organizada continúan ampliando sus propias capacidades cibernéticas, mientras los colectivos de *hackers* incrementan su número y nivel de sofisticación. Esta evolución plantea un reto creciente para los Estados, que deben reforzar sus mecanismos de coordinación e intercambio de información con agencias de seguridad, proveedores de servicios de internet y actores del sector privado. Desmantelar redes ilícitas requiere inteligencia técnica especializada, conocimiento profundo de los métodos de operación y control sobre los canales financieros utilizados por los ciberdelincuentes (OEA, 2019).

En este escenario, entender el ciberespacio como un nuevo campo geopolítico de batalla se vuelve esencial para el éxito de las operaciones militares. Por ello, numerosos Estados han ido creando estructuras militares especializadas —cibercomandos— integradas a sus fuerzas armadas, a fin de actuar de forma coordinada en este dominio intangible.

España constituye un ejemplo destacado. Sus fuerzas armadas han sido objeto de agresiones cibernéticas dirigidas a comprometer servicios críticos, lo que impulsó el desarrollo de estrategias nacionales orientadas a enfrentar los riesgos asociados al uso del ciberespacio. La ciberseguridad fue incorporada como un eje fundamental de la política de seguridad nacional ampliando el concepto tradicional de seguridad más allá del ámbito militar y policial para abordar nuevas amenazas de carácter digital (Ministerio de Defensa de España, 2013).

El Servicio de Inteligencia de España desempeña un papel clave en este esfuerzo proporcionando elementos de análisis para la toma de decisiones estratégicas en ciberseguridad. Sus funciones incluyen la obtención y tratamiento de información tanto en territorio nacional como en cooperación con servicios extranjeros, lo cual resulta indispensable, dada la naturaleza transnacional de las (Villalba, A., & Corchado, J, 2017, pág. 101).

Por su parte, la Oficina Nacional de Seguridad (ONS), como autoridad responsable de la protección de información clasificada, vela por el cumplimiento de normativas relacionadas con el resguardo de datos sensibles en contextos nacionales e internacionales. En materia de ciberseguridad, esta oficina colabora activamente en la protección de sistemas críticos y activos estratégicos frente a amenazas digitales (Ministerio de Defensa de España, 2013).

El Mando Conjunto de Ciberdefensa español, además de garantizar la seguridad de las redes militares, desarrolla capacidades ofensivas y defensivas, incluyendo acciones preventivas, reactivas, de alerta temprana y de explotación del entorno digital, con el fin de generar superioridad informacional en el ciberespacio (Ministerio de defensa España., 2014).

En ese contexto, el traspaso de información entre fuerzas militares requiere comprender y aplicar principios de inteligencia que aseguren la reserva y el manejo adecuado de la información crítica. Aunque muchos de estos métodos son clasificados, existen modelos de cooperación internacional que permiten compartir conocimientos y capacidades en escenarios conjuntos, y fortalecer así las operaciones militares y la defensa cibernética cooperativa.

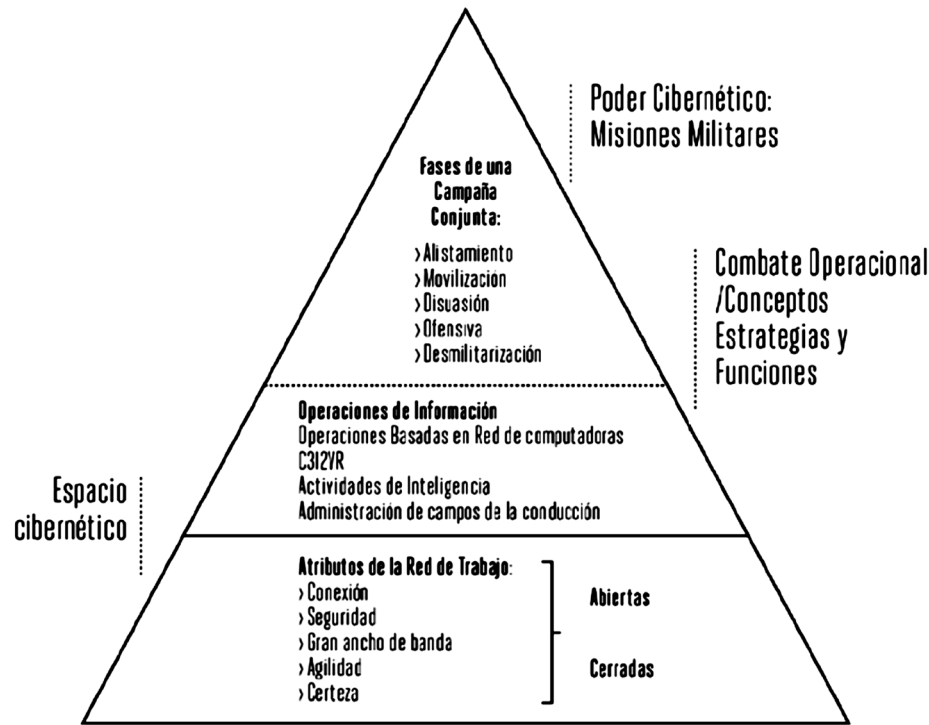
El éxito del intercambio de información interagencial radica en garantizar su seguridad, clasificación adecuada y control sobre los posibles vectores internos de riesgo. La mitigación de amenazas internas —como filtraciones o infiltraciones— requiere no solo medidas técnicas, sino también el fortalecimiento de la lealtad institucional y la gestión estratégica del talento humano. Estos esfuerzos deben acompañarse del desarrollo continuo de plataformas tecnológicas y métodos seguros de intercambio de datos (Becerra, 2019).

En el caso de Estados Unidos, la doctrina operacional en el ciberespacio está formalizada en la *Joint Publication 3-12: Cyberspace Operations* (2018), que integra dicho dominio en las operaciones conjuntas. Esa doctrina distingue tres tipos de operaciones: ofensivas (OCO), defensivas (DCO) y defensa de la red de información del Departamento de Defensa (DODIN). Las OCO buscan proyectar poder a través del espacio cibernético; las DCO están orientadas a proteger las redes propias o aliadas, y las operaciones DODIN se centran en el diseño, operación y protección de las redes del Departamento de Defensa, para asegurar la integridad, disponibilidad, confidencialidad y autenticidad de los sistemas de información (Joint Force Development, 2018).

En contraste, América Latina enfrenta importantes desafíos estructurales. Según el Banco Interamericano de Desarrollo (BID), el 80 % de los países carecen de una estrategia nacional de ciberseguridad (BID, 2016; Cabuya-Padilla & Castaneda-Marroquin, 2024). Brasil ha sido una excepción relativa, al avanzar en el diseño de una política nacional impulsada por amenazas crecientes. Sin embargo, enfrenta obstáculos en la definición de prioridades y en la implementación efectiva de sus lineamientos estratégicos (Diniz et al., 2014).

A nivel doctrinal, las Fuerzas Militares suelen estructurar su poder cibernético en tres niveles jerárquicos, como se observa en la figura 5. En la base del triángulo se encuentran las redes abiertas y cerradas, junto con capacidades de conectividad segura, resiliencia y alto rendimiento. El nivel intermedio comprende las funciones operacionales, estrategias y acciones como las operaciones de redes computacionales (en inglés, NCO, por las iniciales de Network Computer Operations) y las operaciones de información. En la cúspide se ubican las misiones militares articuladas con el empleo del poder cibernético en todas las fases de una campaña (De Vergara, E., & Trama, G, 2017, pág. 141).

Figura 5. Estructura del poder cibernético militar



Fuente: De Vergara y Trama (2017, p. 141).

Los sistemas cibernéticos militares pueden clasificarse como abiertos o cerrados. Los sistemas abiertos permiten el acceso a través de credenciales y suelen estar conectados a infraestructuras comerciales. Su seguridad depende del cifrado, autenticación y uso de herramientas de protección, pero su exposición a redes públicas los hace inherentemente más vulnerables. Por tal motivo, muchas fuerzas armadas trabajan en el desarrollo de soluciones propias con mayores garantías de control.

En contraste, los sistemas cerrados están restringidos a nodos autorizados y operan de forma aislada, sin conexión con redes abiertas. Aunque no todos los Estados han implementado plenamente este modelo —como es el caso de Argentina—, su uso garantiza mayores niveles de seguridad, disponibilidad y confiabilidad de la información transmitida. Sin embargo, no están exentos de riesgos: siguen siendo susceptibles a infecciones por medios físicos, como dispositivos USB contaminados (De Vergara & Trama, 2017, p. 142).

En contextos como el de Estados Unidos, los sistemas *Secret Internet Protocol Router Network* (SIPRNet) y *Secure Telephone Units* (STU) son ejemplos de redes militares cerradas que permiten el control total sobre el acceso, el tráfico y los nodos. Dichos sistemas no solo garantizan un uso seguro y eficiente de la información, sino que también contribuyen de forma decisiva al éxito de las operaciones militares mediante su resiliencia y confiabilidad (Kramer, 2009).

En conjunto, los modelos internacionales revisados evidencian que el intercambio de información cibernética en el ámbito militar requiere estructuras técnicas robustas, protocolos interoperables y marcos doctrinales sólidos. La seguridad, la clasificación, la cooperación interagencial y el dominio del ciberespacio como entorno operacional emergen como factores determinantes en la construcción de capacidades estratégicas que permitan anticipar y neutralizar amenazas en escenarios complejos y dinámicos.

Sistema de intercambio de información de las Fuerzas Militares de Colombia

En la actual sociedad de la información, los sistemas digitales y las estrategias orientadas a proteger los activos estratégicos de las organizaciones son fundamentales. La protección de la confidencialidad de la información no solo afecta al ámbito militar, sino también a sectores como la economía, la política, la educación y las comunicaciones.

Colombia ha registrado avances importantes en materia de tecnologías de la información y las telecomunicaciones, lo que ha exigido una rápida adaptación institucional para garantizar la seguridad nacional. En dicho proceso, las Fuerzas Militares han unificado esfuerzos para prevenir, controlar y neutralizar amenazas en el ciberespacio.

Como señala Niño (2015), el uso coherente de las tecnologías debe responder a una alineación entre los intereses nacionales e internacionales. En ese marco, se han establecido normas para prevenir el uso indebido de los recursos tecnológicos, en línea con principios de seguridad digital.

En 2011 el Gobierno colombiano expidió el primer documento CONPES en ciberseguridad y ciberdefensa, lo que dio origen a entidades clave, como el Grupo de Respuesta a Emergencias Cibernéticas (ColCERT) y el Comando Conjunto Cibernético (CCOCI). Este último, bajo el mando del Ministerio de Defensa Nacional, tiene la misión de prevenir, detectar, neutralizar, analizar y responder ante amenazas informáticas que comprometan la seguridad del Estado. Además, cada Fuerza

—Ejército, Armada y Fuerza Aeroespacial— ha desarrollado capacidades propias en ciberdefensa, complementadas por el Centro Cibernético Policial en el ámbito de la ciudadanía (CONPES 3701).

El desarrollo institucional prosiguió con la creación de Unidades Cibernéticas específicas en cada Fuerza, desde donde el CCOCI coordina operaciones de ciberdefensa según el tipo de amenaza y el rol funcional de cada componente. Este enfoque fue consolidado en el Plan Nacional de Desarrollo 2014-2018 (Departamento Nacional de Planeación, 2014). En 2016 el CONPES 3854 —Política Nacional de Seguridad Digital— incorporó la gestión del riesgo como un eje estratégico determinando principios y dimensiones que permiten fortalecer la capacidad de respuesta de actores públicos y privados ante amenazas digitales (Comando Conjunto Cibernético, 2017, págs. 11-12).

Los destacamentos militares trabajan de forma continua en la identificación de riesgos, la corrección de fallas y la reacción ante agresiones, especialmente en los entornos intranet de sus unidades. Alineados con la Resolución 57/53 de la ONU, Colombia ha adoptado criterios internacionales para el uso legítimo y seguro de las TIC (OEA, 2019, págs. 1-2).

La acción conjunta de las Fuerzas Militares en ciberdefensa es clave para neutralizar amenazas que ponen en riesgo la seguridad nacional y el desarrollo del país. En ese contexto, la gestión del riesgo, la anticipación de incidentes y la percepción ciudadana sobre la seguridad son factores decisivos, incluso si ello implica restricciones a ciertas libertades en aras de proteger infraestructuras críticas (IC) (Becerra, 2019).

En cuanto al intercambio de información, se han definido lineamientos estratégicos que incluyen: procesos de clasificación y compartición a nivel operativo y táctico; una taxonomía estandarizada para el manejo de datos cibernéticos, y el desarrollo de una plataforma tecnológica que permita la transferencia segura y en tiempo real de información entre actores clave del ecosistema de ciberdefensa.

La creciente amenaza en el ciberespacio proviene de actores estatales y no estatales que persiguen objetivos como espionaje, sabotaje, terrorismo o criminalidad organizada. De acuerdo con cifras oficiales, el cibercrimen en Colombia aumentó en el 34 % a lo largo del último año, con más de 60.000 denuncias registradas y más de 30.000 incidentes reportados (Presidencia de la República de Colombia, 2018, pág. 29).

En conclusión, Colombia sí ha avanzado significativamente en la consolidación de un sistema de intercambio de información cibernética en el sector defensa,

al articular políticas públicas, capacidades operativas y estructuras técnicas especializadas. Sin embargo, la evolución constante del entorno digital exige continuar fortaleciendo la interoperabilidad entre actores, la estandarización de procedimientos y la adopción de tecnologías seguras que permitan anticipar, mitigar y responder de forma eficaz a las amenazas en el ciberespacio.

Método de intercambio de información cibernética para las Fuerzas Militares de Colombia

Uno de los indicadores clave de la preparación cibernética de un país es su capacidad para establecer mecanismos seguros y sostenibles de intercambio de información entre el Estado, la industria y otros actores estratégicos. Dichas capacidades son fundamentales para identificar, evaluar y responder a ciberataques que puedan afectar sectores críticos como las telecomunicaciones, el comercio o la defensa (Hathway, 2015, pág. 18).

Existen al menos cuatro modelos reconocidos de intercambio de información, liderados: 1) por el Gobierno; 2) por la industria; 3) por organizaciones sin ánimo de lucro, y 4) modelos híbridos, que integran sectores gubernamentales, académicos y privados. Cada uno presenta desafíos únicos, como el equilibrio entre rapidez en el intercambio, confidencialidad de los datos, respeto por las libertades civiles y sostenibilidad operativa. No obstante, todos requieren dos factores esenciales para su éxito: confianza institucional y claridad en los roles, responsabilidades y objetivos (Hathaway, 2010).

Para que estos esquemas sean efectivos, debe definirse con precisión qué información debe compartirse, quién tiene acceso, y qué medidas deben adoptarse para proteger los datos una vez divulgados. La complejidad aumenta cuando los miembros del sistema son Estados soberanos con distintas prioridades de seguridad (Hathway, 2015, pág. 19). En el caso colombiano, resulta indispensable contar con mecanismos formales y procedimientos acordes con la normativa nacional que permitan establecer responsabilidades claras, aplicar sanciones cuando sea necesario y garantizar la integridad de la información transmitida en el sistema de comunicaciones del sector defensa.

La protección de las tecnologías de la información y las comunicaciones (TIC) en el teatro de operaciones del ciberespacio requiere la integración efectiva entre ciberseguridad, ciberdefensa y ciberinteligencia. Esta sinergia permite anticipar, planear, dirigir y ejecutar acciones coordinadas frente a amenazas terroristas y

otras formas de agresión digital. Dado que las amenazas cibernéticas afectan directamente la estabilidad de los Estados y la resiliencia de sus instituciones, es imprescindible tener la capacidad para anticipar y neutralizar incidentes críticos mediante mecanismos de seguridad estructurados (Sancho, 2018). La globalización y la convergencia tecnológica han intensificado la frecuencia, sofisticación y alcance de los ataques, y ello evidencia la necesidad de adoptar modelos más robustos de protección de la infraestructura nacional.

Para consolidar una verdadera capacidad de colaboración e intercambio de información, es indispensable estandarizar los sistemas empleados, para así facilitar una articulación eficiente entre las entidades responsables de la seguridad y defensa del país.

En tal sentido, la protección de infraestructuras críticas debe apoyarse en sistemas capaces de anticipar riesgos mediante la recolección y análisis de datos de múltiples fuentes. Las amenazas actuales ya no pueden ser enfrentadas con métodos tradicionales: requieren plataformas avanzadas que detecten señales tempranas dispersas y permitan activar mecanismos de respuesta y recuperación ágiles y eficaces (Escuela Superior de Guerra., 2019).

El Ministerio de Defensa Nacional requiere una plataforma especializada para el intercambio de información cibernética que permita consolidar el conocimiento sobre amenazas que afectan la ciberseguridad y la ciberdefensa institucional. Esta plataforma debe facilitar la identificación de ataques que comprometan redes, sistemas y activos críticos, y permitir que se ajusten medidas de protección, mejorar la capacidad de monitoreo y promover acciones preventivas entre administradores y usuarios.

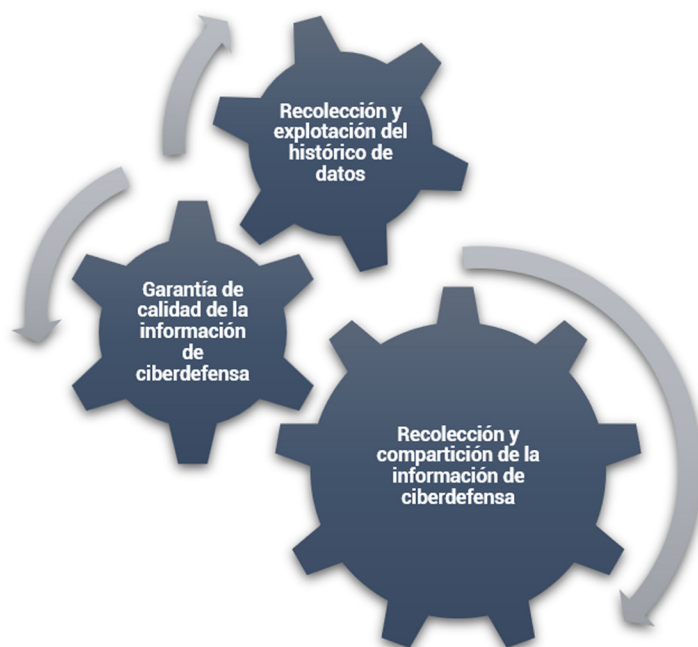
Un sistema de intercambio eficaz fortalecería la articulación entre organismos del sector defensa generando capacidades conjuntas para emitir alertas tempranas, compartir indicadores de compromiso y sistematizar lecciones aprendidas frente a amenazas comunes. En ausencia de dicha plataforma interagencial se reduce la capacidad de anticipación ante riesgos ya detectados por otras fuerzas, y se debilita, por tanto, la respuesta nacional frente al cibercrimen.

La gestión del riesgo cibernético debe entenderse como una responsabilidad colectiva del Estado, que implique cooperación nacional e internacional bajo el principio de responsabilidad compartida. Ello permitiría acciones articuladas y transnacionales frente a actores maliciosos cada vez más sofisticados.

Esta capacidad de colaboración debe ser inherente a toda organización de ciberdefensa. Para ello, se requiere una infraestructura que facilite el intercambio de información técnica y operativa mediante servicios de mensajería segura,

videoconferencia, chats especializados y herramientas colaborativas como pizarras digitales. La información compartida debe cumplir estándares de calidad, lo que incluye datos sobre vulnerabilidades, amenazas, incidentes, riesgos, activos y medidas implementadas, todo bajo formatos estructurados que optimicen su análisis y uso estratégico (Escuela Superior de Guerra, 2019). La figura 6 incorpora esta complejidad en el marco de la capacidad de las organizaciones de seguridad de los sistemas de información.

Figura 6. *Capacidad de las organizaciones de seguridad de los sistemas de información*



Fuente: elaboración propia (Escuela Superior de Guerra, 2019).

La interoperabilidad es un componente esencial en los sistemas de intercambio de información cibernética. Permite garantizar la confidencialidad, integridad, disponibilidad, autenticación y no repudio de los datos; reduce los tiempos de respuesta, y mejora la seguridad mediante la coordinación entre múltiples organismos. Además, favorece el conocimiento situacional compartido, optimiza recursos y permite sincronizar actividades de ciberdefensa en tiempo real (Escuela Superior de Guerra, 2019, págs. 14-15).

En línea con este enfoque, las políticas de defensa de Colombia vienen enfatizando la importancia de fortalecer las alianzas internacionales en materia de

seguridad. Colombia ha buscado consolidarse como socio estratégico de la OTAN y de Estados Unidos promoviendo el intercambio de conocimientos en áreas clave como inteligencia, operaciones militares, lucha contrainsurgente, narcotráfico y gestión de riesgos.

Este esfuerzo también incluye la mejora continua en capacidades logísticas, estándares interoperables y doctrinas en ciberdefensa. Para eso se requiere una formación constante del personal militar, así como el desarrollo de operaciones combinadas que aseguren una mayor integración con fuerzas aliadas. Como parte de dicha estrategia, se renovó el programa de cooperación *Individual Partnership Cooperation Program* (IPCP), con énfasis en desminado, ciberdefensa y combate al crimen organizado (Presidencia de la República de Colombia, 2018, págs. 51-52).

Finalmente, la seguridad técnica de los sistemas utilizados es un aspecto crítico. La protección de los sistemas operativos, a menudo expuestos a riesgos y vulnerabilidades, debe ser abordada desde un enfoque preventivo, que garantice su integridad y minimice la posibilidad de modificaciones maliciosas o fallas que comprometan la seguridad de la información intercambiada.

Con base en los modelos internacionales analizados, las necesidades específicas del entorno estratégico colombiano, junto con las capacidades ya existentes en materia de ciberdefensa, se propone un modelo híbrido adaptado a las Fuerzas Militares de Colombia, con los siguientes elementos clave:

- Modelo base propuesto:
 - o Modelo híbrido colaborativo, articulado entre el Ministerio de Defensa Nacional, la industria nacional, el sector académico y aliados estratégicos internacionales, para garantizar sinergias, confianza y capacidades sostenibles.
- Componentes estructurales del sistema:
 - o Plataforma nacional segura de intercambio de información cibernética (con estándar STIX/TAXII), que integre:
 - Las Unidades Cibernéticas de cada Fuerza.
 - El Comando Conjunto Cibernético (CCOCI).
 - El Centro Cibernético Policial.
 - El CSIRT Defensa.
 - Las entidades civiles con funciones críticas (por ejemplo, infraestructura crítica energética o de comunicaciones).

- o Sistemas interoperables con capacidades de:
 - Clasificación automática de información.
 - Compartición de alertas tempranas.
 - Indicadores de compromiso (IoC) y análisis de amenazas en tiempo real.
 - Canal seguro para lecciones aprendidas.
- Principios de funcionamiento:
 - o Confianza mutua institucional: mediante acuerdos interinstitucionales de cooperación y confidencialidad.
 - o Criterios comunes de clasificación y taxonomía de información cibernética.
 - o Responsabilidad compartida en la gestión del riesgo cibernético.
 - o Interoperabilidad con aliados estratégicos: como la OTAN y Estados Unidos, asegurando estándares compatibles para operaciones combinadas.
- Capacidades clave que debe garantizar:
 - o Protección de información clasificada y crítica.
 - o Coordinación en tiempo real en caso de incidentes.
 - o Mejora de la conciencia situacional cibernética conjunta.
 - o Fortalecimiento de la anticipación, reacción y resiliencia institucional.
- Requisitos para su implementación:
 - o Desarrollo normativo y técnico para garantizar confidencialidad, autenticación, disponibilidad y no repudio.
 - o Capacitación continua del personal militar y técnico.
 - o Inversión sostenida en plataformas, redes seguras e infraestructura crítica.
 - o Inclusión del componente de ciberinteligencia en el ciclo de planeamiento militar.

Esta propuesta busca equilibrar la necesidad de proteger la información sensible con la urgencia de compartir datos clave entre organismos de seguridad y defensa para neutralizar amenazas cibernéticas de forma oportuna, anticipada y coordinada. Así, Colombia avanzaría hacia un modelo integral de ciberdefensa colaborativa en el ámbito militar.

Figura 7. Esquema general de las bases del modelo conceptual propuesto

**Propuesta de método de intercambio de información de
ciberseguridad y ciberdefensa para las Fuerzas Militares de Colombia**

- Adoptar un modelo híbrido de intercambio de información
- Plataforma tecnológica interoperable
- Clasificación de la información según estándares establecidos
- Garantía de seguridad y confianza en el intercambio
- Colaboración en tiempo real frente a incidentes
- Colaboración en tiempo real frente a incidentes



Fuente: elaboración propia.

Conclusiones

Las amenazas cibernéticas han evolucionado en complejidad y volumen, hasta convertirse en un desafío crítico para la seguridad nacional de Colombia. El crecimiento acelerado de estas amenazas y su vinculación con el uso de nuevas tecnologías representan un riesgo directo para las Fuerzas Militares, cuyas capacidades dependen cada vez más de sistemas tecnológicos para la navegación, armamento, transporte, información y comunicaciones.

La vulnerabilidad de las infraestructuras y redes críticas no solo compromete la seguridad y defensa del país, sino que también impone costos económicos significativos y afecta la estabilidad social. Por ello, resulta decisivo alinear las agendas de seguridad nacional y económica, y reconocer la ciberseguridad como un pilar para la protección del crecimiento digital y del desarrollo estratégico nacional.

Uno de los retos centrales de la ciberdefensa es garantizar el funcionamiento estable de la sociedad en el entorno digital generando condiciones de confianza suficientes para la integración segura de tecnologías como el Internet de las Cosas (IoT). Esta confianza es clave para el aprovechamiento del potencial del ciberespacio en la vida cotidiana, tanto en el ámbito civil como en el militar.

La ciudadanía, en su interacción diaria con plataformas digitales, enfrenta múltiples vulnerabilidades. Su capacidad de respuesta es limitada, lo que justifica la necesidad de implementar iniciativas pedagógicas que promuevan la conciencia cibernética, el uso responsable de la tecnología y la protección de la información personal ante ataques como el robo de contraseñas, el espionaje en redes o la infiltración de *software* malicioso.

Para proteger las infraestructuras críticas del país, resulta prioritario transformar el enfoque actual de gestión de datos desarrollando sistemas resilientes capaces de anticiparse a los riesgos. Esto requiere una arquitectura flexible y adaptativa frente al carácter dinámico del ciberespacio, lo que implica integrar la seguridad civil y militar bajo una estrategia nacional unificada.

Finalmente, se concluye que Colombia debe adoptar un modelo híbrido de intercambio de información cibernética, basado en una plataforma tecnológica interoperable que articule a las Fuerzas Militares con organismos civiles y aliados internacionales. Este modelo debe combinar elementos gubernamentales, industriales y académicos, garantizar estándares de clasificación, seguridad y confianza, y promover la colaboración en tiempo real frente a incidentes. La interoperabilidad, la gestión del riesgo y la anticipación a las amenazas deben ser los principios rectores para consolidar esta capacidad estratégica nacional.

Referencias

- Becerra, J. (2019). La Seguridad en el Ciberespacio Un desafío para Colombia. En G. Medina, *La Seguridad*. Bogotá.
- Banco Interamericano de Desarrollo [BID]. (2016). *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe*. Banco Interamericano de Desarrollo.
- Cabuya-Padilla, D., & Castaneda-Marroquin, C. (2024). Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima - MARCIM: estado del arte y metodología. *DYNA*, 169-179. doi:10.15446/dyna.v91n231.109774
- Cabuya-Padilla, D., Alvarado Carvajal, C., Carrascal Ortiz, R., Riola Rodríguez, J., Fajardo-Toro, C., & Escandon Bernal, S. (2022). Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990-2021. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informação*, 197-210.
- Cabuya-Padilla, D., Díaz-López, D., Martínez-Páez, J., Hernández, L., & Castaneda-Marroquin, C. (2025). SERDUX-MARCIM: Maritime Cyberattack simulation using Dynamic Modeling, Compartmental Models in Epidemiology and Agent-based Modeling. *International Journal of Information Security*, 122.
- CCN-CERT. (2008). *Sistema de alerta temprana*. Centro Criptológico Nacional Español y Centro Nacional de Inteligencia de España.
- Centro Criptológico Nacional. (2021). *Guía de Seguridad de las TIC CCN-STIC 201*. Centro Criptológico Nacional.
- Comando Conjunto Cibernético. (2017). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia*. Comando General de las Fuerzas Militares.
- Cornaglia, S., & Vecelli, A. (2017). La ciberdefensa y su regulación legal en Argentina (2006-2015). *URVIO - Revista Latinoamericana de Estudios de Seguridad*.
- Cubeiro, E. (2016). Ciberinteligencia. En A. Díaz, *Conceptos Fundamentales de Inteligencia*. Tirant lo Blanch.
- De Vergara, E., & Trama, G. (2017). *Operaciones militares cibernéticas*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.
- Departamento Nacional de Planeación. (2014). *Plan Nacional de Desarrollo 2014-2018*. Presidencia de la República de Colombia.
- Departamento Nacional de Planeación. (2017). *CONPES 3854 - Política Nacional de Seguridad Digital*. Bogotá.
- Diniz, G., Muggah, R., y Misha, G. (2014). Deconstructing cyber security in Brazil: Threats and responses. *Strategic Paper 11*, 3-32.
- Escuela Superior de Guerra. (2019). Ciberseguridad y ciberdefensa UD1. Introducción a la Ciberdefensa.
- Escuela Superior de Guerra. (2019). Fundamentos de Ciberdefensa: documentación técnica.
- Escuela Superior de Guerra. (2019). Ciberseguridad y Ciberdefensa UD2. Capacidades de ciberseguridad y Ciberdefensa.
- Ganuza, N. (2020). Guía de ciberdefensa: orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar. Junta Interamericana de Defensa.

- Gobierno de Estados Unidos de América. (2018). *Cyberspace Operations* - Joint Publication 3-12.
- Gruszczak, A. (2016). *Intelligence security in the European Union*. Springer <https://link.springer.com/book/10.1057/978-1-137-45512-3>
- Hathaway, M. (2010). *Why Successful Partnerships are Critical for Promoting Cybersecurity*. The New Muga Internet.
- Hathway, M. (2015). *Índice de preparación cibernética 2.0: Un plan para la preparación cibernética: Una línea de base y un índice*. Potomac Institute for Policy Studies.
- IBM. (2025). *X-Force Threat Intelligence Index*. IBM.
- INCIBE. (2018). *Memorias Cybersecurity Summer Botcamp*.
- Joint Force Development. (2018). *Joint Publication 3-12: Cyberspace Operations*.
- Kramer, F. (2009). *Cyberpower and National Security*. National Defense University Press and Potomac Books.
- Ministerio de Defensa de España. (2013). *Estrategia de Seguridad Nacional. Un proyecto compartido*.
- Ministerio de defensa España. (2014). *MCCD-RD872 - Organización FAS*. Ministerio de defensa España.
- Moreno, L. (2017). *Seguridad de la Información y tendencias estratégicas de ciberseguridad*. Sala de prensa. Escuela Militar de Cadetes "General José María Córdova".
- Niño, F. (2015). *Concepto de Ciberseguridad organizacional*. Universidad Militar Nueva Granada.
- Organización de Estados Americanos [OEA]. (2019). La OEA y AWS presentan un "White Paper" para fortalecer la capacidad de seguridad cibernética en las Américas a través del marco de seguridad cibernética del NIST.
- Organización de Naciones Unidas [ONU]. (1999). Asamblea General de las Naciones Unidas del 4 de enero de 1999.
- OTAN. (2016). NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. Warsaw Summit.
- Presidencia de la República de Colombia. (2018). *Política de Defensa y Seguridad PDS - Para la Legalidad, el Emprendimiento y la Equidad*.
- Sainz, J. (2012). *Inteligencia Táctica*. Universidad Complutense de Madrid.
- Sancho, C. (2018). Ciberinteligencia: Contextualización, aproximación conceptual, características y desafíos. Centro de Investigaciones y Estudios estratégicos, Cuaderno de trabajo N°1.
- Saz, M. (2016). *Conferencia: Operaciones Militares en el Ciberespacio*.
- UIT. (2015). *Medición de la Sociedad de la Información*. UIT.
- Villalba, A., & Corchado, J. (2017). Análisis de las ciberamenazas. En *Cuadernos de estrategia* (pp. 97-138). Ministerio de Defensa España.
- World Economic Forum. (2025). *The Global Risks Report*. <https://www.weforum.org/publications/global-risks-report-2025/>
- Zhaoyang, D. (2014). *Smart Grid Cyber Security*.



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

En el siglo XXI, el poder ya no se proyecta únicamente mediante fuerzas militares o control territorial. Cada vez con mayor frecuencia, la competencia estratégica se desarrolla en el ciberespacio, un entorno donde infraestructuras digitales, redes globales y sistemas algorítmicos sostienen el funcionamiento de las sociedades contemporáneas.

Este volumen explora las bases tecnológicas de ese nuevo campo de batalla. A través de un recorrido que conecta la historia de la computación y la cibernética con la evolución del ciberespacio como dominio estratégico, el libro analiza cómo las infraestructuras digitales se han convertido en elementos críticos para la seguridad nacional. Ciberguerra, *dark web*, infraestructuras críticas y arquitectura del poder informacional aparecen aquí como componentes centrales del conflicto contemporáneo.

Este libro forma parte de "El Campo de Batalla Digital: La Defensa Nacional en la Era Algorítmica", una obra en tres volúmenes dedicada a analizar la transformación del conflicto en el entorno digital.



ISBN 978-628-7818-66-8

