PRIMERA INSTANCIA

REVISTA JURÍDICA

Número 24, Volumen 12

Enero-junio

2025

www.primerainstancia.com.mx

ISSN 2683-2151

REVISTA PRIMERA INSTANCIA, número 24, volumen 12, enero a junio de 2025, es una revista electrónica arbitrada en español de difusión vía red de cómputo desde el 2013, resultado de investigaciones científicas originales e inéditas, difunde resultados de estudios empíricos y teóricos preferentemente del área jurídica, con la periodicidad semestral (enero-junio / julio-diciembre).
Boulevard Presa de la Angostura, número 215-12, Fraccionamiento Electricistas Las Palmas, Tuxtla Gutiérrez, Chiapas, C.P. 29040, Tel. (52961) 6142659.
Página web: http: //www.primerainstancia.com.mx/revista-primera-instancia/
Correo: primerainstancia@Outlook.com
Alfonso Jaime Martínez Lazcano, titular de la Reserva de Derechos al Uso Exclusivo No. 04-2018-061813141600-203, otorgado por el Instituto Nacional del Derecho de Autor, ISSN 2683-2151.

Editorial

En esta vigésima quinta edición de *Primera Instancia*, nos posicionamos sin ambigüedades frente a las estructuras que perpetúan la exclusión, la simulación institucional y la omisión estructural en materia de derechos humanos. Esta revista no se limita a describir el estado del derecho positivo: lo interroga, lo incomoda y lo reconfigura desde una perspectiva crítica, situada y comprometida con la dignidad humana como metavalor rector.

Abrimos con una categoría doctrinal que ya se ha consolidado como eje continental de análisis. *"El negativismo jurídico: una categoría crítica para comprender la omisión estructural frente a los derechos humanos"*, formulado por Alfonso Jaime Martínez Lazcano, no como simple crítica al formalismo normativo, sino como denuncia estructural de una praxis judicial que bloquea sistemáticamente la aplicación efectiva del bloque de convencionalidad. Esta resistencia activa, disfrazada de neutralidad técnica, exige una ruptura epistemológica radical y una reconfiguración profunda de la formación judicial. No basta con reformar programas: hay que desmontar dogmas, desarticular simulaciones y reconstruir el pensamiento jurídico desde sus fundamentos.

Desde Bolivia, Paul Franco Zamora, en su artículo: *"Jurisprudencia constitucional y convencional en el marco de los principios de progresividad, prohibición de regresividad y sobre protección de los derechos de las y los adolescentes en el sistema penal boliviano"*, nos recuerda que la justicia restaurativa no es una utopía teórica, sino una herramienta concreta para humanizar el sistema penal juvenil. Su análisis jurisprudencial demuestra que el principio de progresividad no puede ser letra muerta cuando se trata de adolescentes vulnerables. La reparación, la reconciliación y el enfoque garantista deben ser parte integral de toda decisión judicial que aspire a la legitimidad ética y convencional.

El artículo *"Impuestos catastrales y aprovechamiento de la vivienda y espacios subutilizados. Una política fiscal para disminuir la pobreza y generar bienestar social"*,

escrito por Dasaev Sosa Arellano nos confronta con una paradoja fiscal que revela la tensión entre derecho constitucional y realidad estructural: mientras el derecho a la vivienda se consagra en la norma suprema, la especulación inmobiliaria y la acumulación de espacios baldíos profundizan la pobreza urbana. Su propuesta de impuestos catastrales como política redistributiva no es solo fiscal: es ética, social y jurídica, y exige una relectura crítica del rol del Estado en la justicia territorial.

Estefany Fabiola Justo Ramos aborda la *"Maternidad subrogada, derechos que tutela"* desde una perspectiva de derechos humanos, denunciando el vacío normativo y las prácticas clínicas sin regulación. Su llamado a legislar con racionalidad y empatía es urgente: la protección de la gestante, del recién nacido y de los padres intencionales no puede depender de la improvisación judicial ni de la lógica mercantil.

Andrea Marilú Rojano Sánchez a través de su artículo: *"Legitimación del desarrollo y conflictos ambientales"* denuncia la simulación de consultas en proyectos de desarrollo que afectan a pueblos indígenas. Su análisis del PDIT revela que el derecho al desarrollo no puede imponerse como modelo único, sino construirse desde la autodeterminación y el respeto a la diversidad cultural. La consulta previa, libre e informada no es un trámite: es un derecho sustantivo que exige veracidad, participación efectiva y reconocimiento de la pluralidad epistemológica.

Javier Guerrero Luna nos invita a repensar *"La CIDH y la vejez digna"* como derecho humano en riesgo. La CIDH ha sido clara: los Estados deben garantizar pensiones suficientes y sostenibles. Pero más allá del marco jurídico, se requiere una transformación cultural que supere el clientelismo y promueva el envejecimiento activo como paradigma de inclusión, dignidad y justicia intergeneracional.

Carlos Alfonso Guecha López y Jaime Cubides-Cárdenas nos sumergen en la *"Guerra cibernética, inteligencia artificial y nuevas amenazas a los Estados",* resaltando los desafíos de la ciberseguridad militar, la inteligencia artificial y la guerra digital. Su reflexión sobre el C6ISR y la planificación estratégica desde el conocimiento del adversario redefine el concepto de defensa nacional en tiempos de interconectividad total, donde el derecho internacional debe adaptarse a escenarios de conflicto no convencional.

Finalmente, el equipo de Sara Berenice Orta Flores, Blanca Torres Espinosa y Carlos Ernesto Arcudia Hernández documenta un caso emblemático "*Justicia agraria con perspectiva de*

género. Un caso de estudio en la huasteca potosina". La sentencia analizada no solo aplica el control de convencionalidad: lo hace desde una mirada interseccional que reconoce la triple discriminación de la mujer indígena adulta mayor, integrando enfoque territorial, étnico y generacional.

Cada artículo de esta edición es una pieza de resistencia crítica. Juntos, conforman un mosaico doctrinal que no se conforma con describir el derecho, sino que lo transforma desde sus márgenes, desde sus omisiones y desde sus urgencias. *Primera Instancia no. 25* no es una revista para leer pasivamente: es una invitación a pensar, a incomodar y a actuar.

Mtra. Merly Martínez Hernández
Secretaria adjunta del CAPL

Tuxtla Gutiérrez, Chiapas, 30 de julio de 2025.

ÍNDICE

GUERRA CIBERNÉTICA, INTELIGENCIA ARTIFICIAL Y NUEVAS AMENAZAS A LOS ESTADOS[1]

Carlos Alfonso GUECHA LÓPEZ[*]
Jaime CUBIDES-CÁRDENAS[**]

SUMARIO: I. *Introducción.* II. *Dominios emergentes*. III. *Ciberespacio*. IV. *Carrera tecnológica*. V. *La guerra fría moderna*. VI. *Batalla Multidominio*. VII. *Ataque cibernético*. VIII. *Ciberoperaciones*. IX. *Hacking*. X. *A manera de reflexión final. Planificación desde la seguridad cibernética.* XI. *Bibliografía.*

Resumen: La Guerra Cibernética ha estado con nosotros desde hace tiempo, ¿Cómo se desarrolla una Ciberguerra? ¿La Ciberguerra son los ataques informáticos? ¿Cuál es su diferencia? ¿Qué normativa se aplica? Ataques lanzados contra los sistemas de gestión de información electrónica militar, civil e infraestructura crítica de TI enmarcan acciones que puede ejecutarse sin violencia, y por lo tanto la dependencia de los sistemas informáticos

[1] Capítulo resultado del proyecto de investigación INV-DER-2957: "La responsabilidad administrativa en Colombia por la comisión de ataques informáticos dirigidos contra la infraestructura crítica del Estado" resultante de la "Convocatoria Interna para la Conformación de un Banco de Proyectos de Investigación Financiables - Vigencia 2019" de la UMNG, haciendo parte de la línea de investigación: "Constitución, Derecho Público y Estado" del grupo de investigación "Grupo de Derecho Público", reconocido y categorizado por MINCIENCIAS registrado con el código COL0028918 vinculado a la Facultad de Derecho, adscrito y financiado por la Universidad Militar Nueva Granada. Trabajo recibido el 1 de diciembre de 2024 y aprobado el 30 de abril de 2025.
[*] Abogado y Especialista en Gestión Pública de la Universidad de Los Andes, con Maestría en Derecho Público Interno y Doctorado en Derecho de la Universidad de Paris II Pantheon-Assas. Docente de Carrera de la Facultad de Derecho de la Universidad Militar Nueva Granada. Contacto: carlos.guecha@unimilitar.edu.co
[**] Doctor en Derecho por la Universidad Católica de Colombia. Abogado, y especialista en Derecho Público de la Universidad Autónoma de Colombia, especialista y Magister en Docencia e Investigación con énfasis en las ciencias jurídicas de la Universidad Sergio Arboleda y Magister en Derecho de la misma casa de estudios. Docente e integrante del grupo Pedagogía y Derecho de la Facultad de Derecho de la Universidad Colegio Mayor de Cundinamarca. Contacto: jalfonsocubides@unicolmayor.edu.co

intensivos del software puede hacer que las naciones sean vulnerables a una guerra sin violencia causando muerte, heridas, destrucción o daño durante los conflictos armados, aunque no exclusivamente en ellos, recolectando inteligencia con fines económicos, políticos.

Palabras Clave: Carrera tecnológica, ciberdefensa, ciberespacio, control militar, guerra cibernética.

Abstract: Cyber warfare has been with us for some time, how does a cyber war develop? Cyberwar is cyber attacks? What is your difference? What regulations are applied? Attacks launched against military, civilian electronic information management systems and critical IT infrastructure frame actions that can be executed without violence, and therefore the dependence on software-intensive computer systems can make nations vulnerable to war without violence causing death, injury, destruction or damage during armed conflicts, although not exclusively in them, collecting intelligence for economic, political or social destabilization purposes. Cyber security evolves rapidly from a technical discipline to a strategic concept.

Keywords: Technological career, cyber defense, cyberspace, military control, Cyber warfare.

I. INTRODUCCIÓN

La Guerra Cibernética es definida como "La penetración no autorizada por parte de, en nombre de, o en apoyo de, un gobierno en el computador o red de otra nación, o cualquier otra actividad que afecte al sistema de un computador, en el cual el propósito es agregar, alterar o falsificar datos, o causar la interrupción o daño a un computador, dispositivo de red o los objetos que controla un sistema de computador".[2] Esta última década de mayor interconectividad global y accesibilidad a las herramientas cibernéticas, la Guerra Cibernética se ha convertido en un componente vital de la guerra convencional, un nuevo dominio militar por derecho propio; los últimos diez años los principales pensadores de

[2] RICHARD A., Clarke y ROBERT, Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, HarperCollins Publishers, Nueva York, 2012, p. 228.

seguridad están luchando para definir la Guerra Cibernética como parte de la estrategia y táctica militar, estos ataques se han organizado para debilitar la capacidad de lucha contra la guerra de un Estado-Nación.

La razón por la cual los ataques cibernéticos son ahora preferidos por los actores estatales y no estatales es la dificultad en la detección de la fuente de ataque debido a la simplicidad en la falsificación de datos en el mundo cibernético y en la dificultad respecto de la atribución del ataque cibernético.

La Guerra Cibernética está íntimamente ligada con los ataques cibernéticos; desde la aparición en escena de los primeros gusanos y virus experimentales hasta los ataques altamente sofisticados en objetivos variados como instituciones financieras, instalaciones militares o infraestructura de servicios esenciales, ese ha sido el resultado mismo de los establecimientos gubernamentales, corporativos y militares altamente conectados en red en el que la amenaza cibernética es mutante, la misma aparece con mayor frecuencia y oportunidad. Los sistemas de Tecnologías de Información parecen abarcar cada vez más no solo la vida cotidiana sino también las operaciones y actividad de las Fuerzas Militares.

Los sistemas de Comando y Control Militar (C2) y los sistemas de armas inteligentes operaran en red con mayor interacción y uso del computador; los mismos se encontrarán cada vez más vinculados a la estrategia y despliegue de las Fuerzas, lo que los expondrá a riesgos de seguridad, ante los conflictos.

Una primera aproximación de la guerra y los conflictos la entrega el teórico militar Prusiano Carl Von Clausewitz padre de la estrategia militar moderna definió la guerra como "el empleo de las batallas para conseguir el fin de la guerra",[3] expresa que la guerra es la continuación de la política por otros medios y un acto de fuerza para obligar al adversario al cumplimiento de nuestra voluntad.[4]

La Guerra surge al intentar resolver conflictos políticos a partir de la violencia, es claro que para alcanzar este objetivo por completo el enemigo debe ser prácticamente desarmado, y el desarme se convierte en el objeto inmediato de las hostilidades. Al final del segundo milenio (diciembre del año 2000), la definición de Clausewitz ya no describe el espectro completo de la guerra moderna que se vislumbra hoy día.

[3] *Cfr.* KARL VON, Clausewitz, *Sobre la guerra* (1832-1834), libro 1, cap. 7, traducción de J.J. Graham, 2002.
[4] ÁLVAREZ RUBIO, Ariel, "El conflicto en Colombia, una perspectiva desde la polemología", *Estudios de Seguridad y Defensa*, 2014, no. 3, vol. 1, p. 24. https://tinyurl.com/2n9shprt

En el futuro, tendremos el potencial de hacer la guerra sin el uso de la violencia y cumplir la segunda mitad de la definición de él solo con la utilización de programas o aplicaciones de computador, si bien la naturaleza de la guerra sigue siendo la misma, el carácter de la guerra está experimentando "cambios" con catalizadores como lo son las redes sociales, las operaciones cibernéticas y de información, y con pequeños vehículos aéreos no tripulados disponibles hoy día de forma comercial, lo que conduce a un campo de batalla cada vez más letal donde todos los dominios serán impugnados y congestionados, se observa entonces que la comprensión de los conflictos en general y de la guerra en referencia al modelo definido por Clausewitz (hace ya un poco más de 170 años) se aleja de la forma en que los conflictos se desarrollan en éstas últimas dos décadas; prácticamente en los inicios del siglo XXI con las nuevas guerras, esto es, por la violencia y uso de la fuerza generalizada en el que se utiliza algún tipo de mecanismo diseñado con un objetivo en común y específico: dañar vidas humanas, estructuras o sistemas en general.

El aumento no lineal, el uso y la confiabilidad de las Tecnologías de la Información y Comunicaciones (TIC´s) avanzarán, en este entorno digital, las personas, las instituciones y gobierno toman las precauciones necesarias, desde el nivel personal hasta el nivel estratégico, y se adaptarán para vivir u operar en esa nueva forma de entorno, por ello asegurar una política de ciberseguridad sólida en un Estado, requiere de la participación directa tanto de los individuos, institución, y del gobierno para estar en el mismo estándar de la seguridad.

Las organizaciones militares deben estar preparadas para operar en esta nueva forma de entorno operativo lleno de software malicioso como las Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés) y software de ciber-espionaje. "Las APT utilizan vectores de ataque únicos y herramientas personalizadas ajustadas para el objetivo en particular, lo que hace que la detección sea un gran desafío ya sea que se utilicen técnicas de detección de anomalías o firmas";[5] la cantidad y complejidad de los ataques cibernéticos ha venido en constante aumento.

Los adversarios apuntan a los Sistemas de Comunicaciones e Información (CIS, por sus siglas en inglés) de las organizaciones gubernamentales, militares e industriales, así como

[5] VIRVILIS, Nikos, VANAUTGAERDEN, Bart y SERRANO SERRANO, Oscar, "Changing the game: The art of deceiving sophisticated attackers", *NATO CCD COE Publications*, 2014. https://tinyurl.com/59drvr45

a las infraestructuras críticas, dichas organizaciones están dispuestas a invertir grandes cantidades de dinero, tiempo y experiencia a fin de lograr sus objetivos. Las soluciones de seguridad tradicionales han fallado repetidamente para mitigar tales amenazas. Para defenderse contra adversarios tan sofisticados se requiere rediseñar las defensas, desarrollando tecnologías enfocadas más en la detección que en la prevención.

Se analiza la ciberseguridad desde la perspectiva militar a la luz de los posibles desafíos, la estructura organizativa y el proceso de toma de decisiones militares (MDMP). Las APT´s son campañas concertadas para reunir información sobre individuos, instituciones de gobierno o particulares, a diferencia de los gusanos y los virus, que normalmente atacan de forma indiscriminada. Es importante entender que los ataques dirigidos implican una planificación inteligente con respecto al objetivo o clase de objetivos elegidos (ya sea un objetivo militar o particular).

Las APT requieren una conexión física a los dispositivos y un método de ex filtración de información; precisamente las APT pueden incluir *malware* altamente sofisticado cuyo desarrollo requiere personas hábiles con experiencia en múltiples campos, así como significativos recursos financieros que involucran su desarrollo.

II. DOMINIOS EMERGENTES

Se han ido añadiendo al conflicto humano nuevas dimensiones de interacción y esta apreciación se observa más en detalle cuando vemos la evolución de la Guerra y los dominios emergentes: inicialmente la Guerra se desarrolló en tierra, posteriormente en el mar y gracias a la evolución tecnológica la guerra se libró con aviones en el aire, observamos entonces como el conflicto humano evoluciona; como lo hace y evoluciona todo en el tiempo, paralelo a la evolución tecnológica del aire las acciones de las Fuerzas Armadas de un Estado-Nación evolucionaron de igual forma en el espectro electromagnético.

En esa evolución tecnológica; se encuentra inmerso el computador, diseñado con propósitos militares, creado en secreto precisamente para ayudar al trabajo de la inteligencia, todos los computadores son únicos y útiles; los mismos a su vez y toda la tecnología que emerge en ellos es de igual forma vulnerable al espionaje. La evolución tecnológica del computador en sus primeras décadas después de su invención fue limitada su capacidad de cómputo, sólo hasta comienzos del siglo XXI se vislumbra y se hace más notorio el

incremento respecto de su evolución, en sus primeras décadas a pesar del grado de especialización del computador en diferentes actividades se hizo más visible con el aporte para la automatización de tareas. El computador siempre ha estado presente en el escenario de la Guerra.

El primer computador programable de primera generación se hace presente en la historia con la invención del ingeniero Alemán Konrad Zuse tras la creación del Z1 (computador que fue controlado por programas que operaron en un Z3 en el año de 1941), para esa misma época a finales de 1940 los esfuerzos de investigación y desarrollo de la compañía Engineering Research Associates (ERA, por sus siglas en inglés) se enfocaban en el desarrollo de máquinas de propósito especial en el uso de la Criptología con aplicaciones Criptológicas, ERA utilizó ésta tecnología aplicada a la criptografía en el desarrollo de grandes proyectos en computadores digitales en los Estados Unidos y Gran Bretaña.[6]

La Escuela de Códigos y Cifrado del gobierno de Reino Unido (GC&CS, por sus siglas en inglés) un lugar de guerra y máquinas situada a 80 kilómetros de Londres en Bletchley Park y los participantes del Gobierno de los Estados Unidos de Norte América,[7] es la cuna de la informática moderna y uno de los secretos mejor guardados de Reino Unido tras la Segunda Guerra Mundial.

Uno de los muchos logros de GC & CS durante la Segunda Guerra Mundial fue el desarrollo y uso extensivo del "primer computador digital electrónico a gran escala del mundo del llamado COLOSSUS", cuya construcción fue liderada por Tommy Flowers; quien dedicó diez meses; desde principios de febrero hasta principios de diciembre de 1943. La máquina COLOSSUS en sí no se utilizó para romper el código Enigma, fue utilizado para descifrar un código del ejército alemán llamado Lorenz. El trabajo de Alan Turing y sus colegas desempeñó un papel clave en ayudar a los científicos e ingenieros en la filosofía y desarrollo de los computadores modernos.

En agosto de 1947 la compañía ERA se encamino en el proyecto Atlas (el nombre designado para el proyecto fue una broma interna: el número 1101 es en binario el número 13, por eso se cita o hace referencia a la "Tarea 13" de la Agencia de Seguridad Nacional

[6] SNYDER, Samuel, "Computer Advances Pioneered by Cryptologic Organizations", *Annals of the History of Computing*, 1980, no. 1, vol. 2, pp. 61-62.
[7] *Cfr.* STERLING, Christopher*, Military Communications: From Ancient Times to the 21st Century*, ABC-CLIO, Oxford, 2007.

[por sus siglas en inglés, NSA] quien inicio el proyecto), la Armada de los Estados Unidos fue el patrocinador Militar otorgó acceso al trabajo con computadores en otros proyectos gubernamentales. ERA basado en el proyecto Atlas posteriormente en el año de 1951 introdujo un equipo o máquina comercial, fue éste el decimotercer trabajo otorgado por la Armada de los Estados Unidos a la compañía ERA, posteriormente el proyecto ERA 1101 cambio de nombre, se renombró como UNIVAC 1101.

La compañía Remington Rand usó la arquitectura de la 1101 como base para una serie de máquinas hasta la década de 1960 fueron los primeros fabricantes de máquinas de oficina americana, conocido originalmente como el fabricante de máquinas de escribir y más adelante Se han enmarcado muchos acontecimientos a través de la historia involucrando los computadores con las operaciones de inteligencia y con la infraestructura utilizada por un Estado-nación para ganar o librar la Guerra, la victoria de una fuerza, un comando, o de un equipo de estrategas utilizando la tecnología, el computador se concibió para espiar, se construyó y se concibe desde entonces para hackear o romper códigos, a través de los años los computadores han sido utilizados como soporte en la Ciberdefensa de un Estado-nación.

La Ciberdefensa es el conjunto de acciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal con los recursos informáticos y tele informáticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos[8] con el conocimiento claro y preciso de cómo son llevadas a cabo las acciones hostiles del atacante a fin de impedir o interrumpir las fuerzas enemigas que utilicen los mismos recursos en el cumplimiento de su misión.

Los dominios emergentes de la guerra han evolucionado de manera constante a lo largo de la historia. Del mismo modo, la tecnología se mantiene como un componente esencial y permanente en la seguridad de los Estados-nación, reflejando su influencia continua en los conflictos actuales.

El siguiente dominio emergente en la Guerra es el Ciberespacio sin mencionar el creciente empleo del espacio con fines Militares, a mediados del año 2010 el subsecretario de Defensa de los Estados Unidos, William Lynn señaló que el ciberespacio “debe ser reconocido como un territorio de dominio igual que la tierra, el mar y el aire en relación a la

[8] *Cfr.* BECERRA, Jairo, *et. al.*, *Derecho y big data*, Editorial Universidad Católica de Colombia, Bogotá, 2018.

Guerra" ratificado en la revista The Economist;[9] al igual que el uso de la fuerza, los ataques armados y todos aquellos actos de Guerra, la tecnología ha añadido en el tiempo dimensiones a los nuevos conflictos.

El análisis de los conflictos recientes se caracteriza por líneas difusas entre guerra y paz, estatales y no estatales, regulares e irregulares, convencionales y no convencionales, las Fuerzas armadas de todo el mundo se enfrentan más aun en esta última década con el dilema de la planificación y estructura de las mismas, a través del Ciberespacio son posibles las manifestaciones de violencia entre Estados, según Gastón Bouthoul inventor en 1942 del neologismo "polemología"[10] y pionero de la sociología de la guerra, profesor de la Escuela de Altos Estudios Sociales, vicepresidente del Instituto Internacional de Sociología, "La Guerre" escrito en francés ha sido traducida al inglés, árabe, japonés, portugués y español, demostrando su obra la gran aceptación en todas las esferas geopolíticas.

La Polemología estudia la guerra como fenómeno social, en ella se estudia la clasificación de los conflictos según su intensidad, localización, periodicidad, morfología y causalidad, utilizando métodos cualitativos y cuantitativos.[11]

La Guerra es un hecho mil veces repetido, fenómeno social que, como todos los fenómenos sociales, tienen sus causas y motivos a los que obedecen, individuos de la sociedad militar, deben entender el cómo y el porqué de sus actuaciones como entes sociales, para aumentar los intangibles del poder relativo de combate.

Hasta mediados del siglo pasado, la guerra, como expresión de una estrategia de conflicto, se consideraba de carácter convencional por parte de los estrategas y polemólogos, la Guerra trataba de un choque de voluntades con amplio gasto de recursos, donde se buscaba el punto de desequilibrio en una batalla decisiva (ejemplos de ello: Varsovia, Verdún, Cambrai, Alamein, Kursk, Diem Bien Phu) para derrotar al enemigo (este es un concepto clave en la teoría militar de Jomini de 1977).[12]

Si bien la naturaleza de la Guerra sigue siendo la misma, el carácter de la guerra actualmente se encuentra experimentando cambios con catalizadores como las redes sociales,

[9] The Economist, *Cyberwar. The Threat from the Internet*, 2010, no. 8689, vol. 396, pp. 3-9.
[10] BOUTHOUL, Gaston, *Traité de polémologie*, Payot, París, 1970, pp. 3-4.
[11] GUTIÉRREZ VALDEBENITO, Omar, *Sociología militar*, Instituto Francés de Polemología, Santiago, 2002, p. 237.
[12] *Cfr.* JOMINI, Antoine-Henri, *El arte de la guerra*, Edaf, Madrid, 1977.

la inteligencia artificial, las operaciones cibernéticas y de la información, lo que conduce a un campo de batalla cada vez más letal donde todos los dominios emergentes serán congestionados particularmente por las operaciones cibernéticas, una vez más resaltar palabras de Clausewitz: “la Guerra cambia con el tiempo, adaptándose al mismo, con sus condiciones previas y por supuesto, cambiará con sus posteriores evoluciones”.

En ésta última década los Estados Unidos a través del Comando de Doctrina y Entrenamiento del Ejército (TRADOC) y el Comando de Combate Aéreo (ACC) han determinado que sus capacidades cibernéticas combinadas en un dominio múltiple serán necesarias para garantizar el éxito del combate futuro.

“La guerra no determina quién tiene la razón, solo quién queda” Bertrand Russell el hablar de Guerra Ciberespacial; de Guerra Cibernética no implica el surgimiento de una nueva clase de Guerra, se trata de la misma práctica hostil, sólo que a partir del uso de tecnologías que implican un cambio cualitativo en la forma de llevar a cabo las operaciones y táctica utilizada dentro de la Guerra o un acto de hostilidad unilateral, existen muchas otras formas de hacer la Guerra.

El incremento significativo en incidentes cibernéticos; el poder militar evidencia un cambio fundamental en el pensamiento, la estructura u organización y cómo es su accionar ante una eventual confrontación. Las hostilidades o agresiones por medios cibernéticos han aumentado de una forma drástica.

Estados Unidos encabeza el índice de las cinco potencias militares más poderosas del mundo. La India, Pakistán, Israel, Sudán del Sur y Corea del Norte nunca firmaron el tratado de No Proliferación Nuclear (NPT, Nuclear Non-Proliferation Treaty, por sus siglas en inglés) mientras que Corea del Norte renunció al tratado NPT en el año 2003.

Estas últimas dos décadas los Estados Unidos ha librado guerras contra enemigos inferiores en capacidad tecnológica, estas mismas circunstancias le han proporcionado una ventana para que sus adversarios observen las tácticas utilizadas y con ellas entre en escena la participación de nuevas tecnologías en interacción con el uso del computador como soporte en la ejecución de operaciones cibernéticas considerándose el uso del mismo como un factor asimétrico operacional que abarata el costo de la Guerra en contraste al armamento estratégico ofensivo utilizado por un Estado-nación como el sistema de defensa estratégica contra misiles balísticos (BMD, por sus siglas en inglés), en el contexto de la crítica al

concepto de disuasión nuclear tras la Guerra Fría y de la política de seguridad y defensa basados en el espacio.

Las acciones militares de Estados Unidos en Afganistán y Siria, las pruebas de los sistemas balísticos nucleares de Corea del Norte, los misiles balísticos intercontinentales con los que actualmente cuenta Estados Unidos, Rusia, China y Corea del Norte, reflejan el poderío militar de estas potencias y Estado-nación. Actualmente Francia dispone de misiles balísticos IRBM [siglas en inglés de Intermediate-Range Ballistic Missile, que significa misil balístico de alcance intermedio] de muy largo alcance y está finalizando el desarrollo de un ICBM de lanzamiento submarino (misil balístico intercontinental para submarinos).

El primer diseño práctico de una plataforma de lanzamiento con base en submarinos fue desarrollado por los alemanes cerca del final de la Segunda Guerra Mundial, con un tubo de lanzamiento que contenía una variante de misil balístico V-2 y fue remolcado detrás de un submarino). La estrategia militar ha sido un factor decisivo y predominante en el planeamiento y dirección de las campañas bélicas, así como también del movimiento y disposición estratégica de las Fuerzas Armadas en un Estado-nación.

La competencia estratégica en las generaciones anteriores fue encaminada al acceso de los recursos naturales y a la capacidad industrial, que luego podría ser utilizada por el ingenio humano. Los componentes necesarios para impactar de forma sustancial y negativa las vidas de países enteros permanecieron en gran medida en manos de las grandes potencias; esto es y ha sido mediante el desarrollo del misil balístico de largo alcance, a través del armamento nuclear o con la utilización de agentes químicos o un biológico, aunque esto último está en medio de una revolución perturbadora.

III. CIBERESPACIO

A diferencia de esta carrera armamentista, en ésta última década y con el uso del Ciberespacio se vislumbra aún más el cambio en la operación y planeación estratégica por capacidades de las Fuerzas Militares de los países, el Ciberespacio ha sido designado como el quinto dominio operacional de la Guerra, el que interactúa junto a los otros dominios: tierra, aire, mar y el espacio exterior. Sin embargo, a diferencia de estos cuatro dominios; el Ciberespacio está construido completamente por humanos.

En la Cumbre de la OTAN de 2016 en Varsovia, se prestó especial atención a la seguridad cibernética, los jefes de Estado y de Gobierno reconocieron el ciberespacio como un nuevo entorno operacional en el que la OTAN tiene las mismas funciones de defensa que en el aire en tierra y mar. Si bien las definiciones técnicas abundan, una forma útil de visualizar y definir el ciberespacio es dividirlo en tres (3) capas, representando en cada una de estas capas un nivel desde el cual se pueden dirigir las operaciones cibernéticas.

Como es explicado por Martin Libicki, la primera capa es física e incluye todos los componentes de *hardware* del ciberespacio, como computadoras, teléfonos inteligentes, enrutadores y cables. Sobre esto descansa una segunda capa, el nivel sintáctico que contiene las instrucciones que permiten que estas máquinas funcionen y los protocolos que permiten la comunicación entre ellas. La tercera y última capa es la semántica, toda la información almacenada en el propio computador, parte de esta información es, como señala de forma semántica, pero de naturaleza sintáctica[13] (información almacenada en el computador pero que proporciona instrucciones para la máquina, como un controlador de impresora o software que controla la máquina), mientras que gran parte de la capa semántica es "Lenguaje natural" es información como documentos u hojas de cálculo. Por citar un ejemplo, cargar a la "nube" una imagen desde un teléfono inteligente implica las siguientes acciones entre las capas:

La capa física (el teléfono, la torre móvil que envía y recibe las señales, y la unidad de almacenamiento y el servidor que proporciona y establece el almacenamiento en la nube). La capa sintáctica es el sistema operativo y las aplicaciones utilizadas para tomar la imagen y conectarse en la nube. Por último, se encuentra en la capa semántica (el archivo que contiene la imagen en sí). El ciberespacio establece el accionar de las operaciones cibernéticas y que los actores (muchas veces aquí la operación conjunta, los cibersoldados) son grupos más pequeños y dinámicos, los que pueden competir contra los poderes regionales o mundiales de forma inimaginable en otros dominios.

A pesar de que la potencia principal en tecnología sean los Estados Unidos en utilización y uso del Ciberespacio, y que se haya substraído (robado o hakeado) su armamento cibernético, dice mucho sobre la realidad del dominio del Ciberespacio, éste hecho hace que la "toma de decisiones estratégicas" en el ciberespacio sea mucho más difícil

[13] *Cfr*. LIBICKI, Martin*, Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Mónica, 2009.

simplemente porque las amenazas son menos visibles (son cibernéticas), amenazas que son persistentes en el tiempo y el riesgo de sorpresa estratégica es mayor.

IV. CARRERA TECNOLÓGICA

Hoy existe una carrera tecnológica en curso más democrática, más igualitaria y, por lo tanto más impredecible con el uso de la "Inteligencia Artificial" (IA), los computadores (supercomputadores) de hoy pueden aprender cosas, por su cuenta hace dos (2) décadas atrás (en el siglo pasado no podían efectuar los cálculos requeridos para el aprendizaje por la limitada capacidad de cómputo en su evolución tecnológica), los computadores eran capaces de dominar el comportamiento humano, pero necesitaban mucha experiencia humana para poder guiar prácticamente su desempeño.

Todo evoluciona normalmente con el tiempo, por lo que los avances en el aprendizaje automático con la IA hacen posible que los computadores dominen problemas muy complejos sin confiar en la codificación de la experiencia humana en sus algoritmos de aprendizaje, el avance tecnológico de las últimas décadas ha hecho posible que el computador domine problemas bastante complejos.

El circuito integrado es hoy sinónimo del concepto de progreso tecnológico, se puede observar que en estas siete décadas transcurridas que abarcan desde la invención del transistor (en los Laboratorios Bell), se ha logrado un progreso incesante con un desarrollo de dispositivos semiconductores, "la ley de Moore", a pesar de las advertencias regulares de los observadores de la industria sobre los límites inminentes.

Estamos publicando un análisis que muestra que desde 2012, la cantidad de cómputo utilizada en las carreras más grandes de entrenamiento de IA ha aumentado exponencialmente con un tiempo de duplicación de 3.5 meses (en comparación, "a Ley de Moore" tuvo un período de duplicación de 18 meses). Desde el año 2012, esta métrica ha crecido en más de 300,000 veces (un período de duplicación de 18 meses produciría solo un aumento de 12 veces). Las mejoras en el cálculo han sido un componente clave del progreso de la IA, por lo que mientras esta tendencia continúe, vale la pena prepararse para las implicaciones de los sistemas que están muy lejos de las capacidades actuales.[14]

[14] *Cfr.* Open AI, *AI and Compute*, 2018.

Hoy en día se argumenta que los desafíos tecnológicos y estructurales actuales que enfrenta la industria no tienen precedentes y socavan los incentivos para una acción colectiva continua en investigación y desarrollo, que ha sustentado los últimos 50 años de transformación en el orden mundial,[15] la potencia de cálculo ha mejorado con el número de transistores que se pueden colocar en un solo computador, pero por otro lado, las crecientes preocupaciones sobre las vulnerabilidades cibernéticas han restringido parte del entusiasmo que podría haber existido en torno a las comunicaciones de radio que han sido mejoradas con el tiempo, ya que ha revitalizado el interés de Rusia y China en la guerra electrónica.

La IA con la robótica y los aviones automatizados han vuelto mucho más capaces a las unidades de procesamiento pequeñas permitiendo guiarlos en sobrevuelos del campo de batalla, de igual forma los misiles interceptores de defensa (Hit-to-kill), al igual que los Sistemas de Defensa de Área de Altitud (THAAD) junto con los Sistemas de Misiles Estándar pueden maniobrar lo suficientemente bien como para chocar con una amenaza entrante, los morteros pueden dirigirse por sí mismos a través de señales de GPS.

V. LA GUERRA FRÍA MODERNA

Con el progreso en los computadores ha llegado una vulnerabilidad cibernética mayor, este desarrollo puede, en circunstancias de guerra, ser incluso más significativo que los atributos positivos del computador. El uso de supercomputadores y la evolución en la capacidad de cómputo en los mismos asociada a su aprendizaje (factor determinante para entrenar una red neuronal), motivó aún más la investigación que data estas últimas dos décadas prácticamente en temas aplicados a la Ciberseguridad y la Ciberdefensa de un Estado-nación y en la escritura del libro "Guerra Cibernética – Amenaza Mutante"[16] desde ya hace un poco más de nueve años, cuando apenas los medios de comunicación se hicieron más activos y participes con lo sucedido el 27 de abril de 2007 (el inicio de una serie de ataques cibernéticos que afectó varios sitios de internet de organizaciones en Estonia).

[15] CALLOWAY, Audra, *El Ejército desarrolla mortero de precisión guiado por láser*, U.S. Army, 2017. https://tinyurl.com/ya779pbv

[16] *Cfr.* CÁCERES, Jairo, *Historia del sistema de información logístico coordinado del sector defensa de Colombia SILOG*, Esdegue, Bogotá, 2018; *Cfr.* CÁCERES, Jairo y GUTIÉRREZ, Juan*, Guerra cibernética, defensa en la red y vectores de ataques con redes neuronales*, Esdegue, Bogotá, 2018.

Justamente el aprendizaje automático ha permitido que el computador aprenda cosas, que sus propios programadores humanos no pueden hacer (el ataque se lleva a cabo con asistencia y participación directa de un humano). La ofensiva vista en Estonia fue reconocida, en su momento, como de gran nivel de sofisticación y fue estudiado como el segundo ejemplo más grande de una Guerra Cibernética patrocinada por el gobierno o un Estado-nación, los ataques dispararon la importancia del tema de la seguridad informática en la milicia moderna, y a pesar del gran impacto producido por lo sucedido con un ataque de Denegación de servicios, este tipo de ataque fue de alta relevancia para el gobierno estonio.

A la luz y conocimiento de varios estrategas de seguridad para los Estados-nación la IA traerá consigo un amanecer de nuevas formas de violaciones cibernéticas que evitan y sobrepasan los medios tradicionales de contrarrestar los ataques y quizás muchos medios de comunicación.

Técnicos y profesionales en seguridad o los mismos cibersoldados tendremos que enfrentar la máquina y no al humano; el reto es entender como ofrecer una defensa proactiva que responda de igual forma con IA y repela el ataque cibernético o mitigar el riesgo en la red con la capacidad de reacción necesaria y suficiente como lo hace el atacante, (podría decirse que las Redes Neuronales y su capacidad de cómputo se encontraban y una hibernación obligada por la capacidad de cómputo requerida, y ahora emerge encontrando nuevos dominios emergentes).

Al igual que la Guerra Fría en las décadas de 1940 y 1950, con la evolución tecnológica y el aumento significativo en la capacidad de cómputo cada Estado-nación tiene motivos suficientes para temer que su oponente obtenga una ventaja tecnológica.

La creciente velocidad y precisión de los programas de aprendizaje profundo, a menudo llamados redes neuronales artificiales o simplemente “redes neuronales” por su parecido con las conexiones neuronales en el cerebro, en la década de 1960,[17] algunos científicos informáticos creían que faltaban solo 10 años para que funcionara un sistema de inteligencia artificial viable, ya en la década de 1980, una ola de nuevas empresas comerciales colapsó, dando lugar a lo que algunas personas llamaron el “invierno de la IA”, pero los

[17] MARKOFF, John, *Scientists See Promise in Deep-Learning Programs*, New York Times, 2012. https://tinyurl.com/4a6seja5

logros en ésta última década impresionado un amplio espectro de expertos en informática respecto de la utilización e implementación de la IA.

En los próximos años cada arma tendrá la capacidad de decidir autónomamente a quién matar: uno de los grandes dilemas éticos de la IA aplicada a la guerra,[18] de igual forma la IA en esta década con la evolución tecnológica respecto la capacidad de computo puede ser utilizada para descubrir nuevas moléculas que podrían conducir a nuevos fármacos (sustancias que sirven para curar o prevenir una enfermedad, para reducir sus efectos sobre el organismo o para aliviar un dolor físico).

El acceso a la tecnología y las técnicas de IA ofrece en éstas dos últimas décadas un mejor panorama en la Ciberdefensa para un Estado-nación al brindar una mayor capacidad de cómputo, la tecnología hoy en día oferta una poderosa inteligencia de máquina avanzada a cualquier número de grupos que puedan pagarla, con la evolución tecnológica los riesgos de proliferación pueden ser difíciles de manejar.

La IA podría ser la forma en que Rusia puede reequilibrar el cambio de poder creado por los Estados Unidos que gastan a Rusia casi 10 a 1 en defensa cada año.[19] Vladimir Putin en el primer día del año 2017 nuevo año escolar en Rusia, en la ciudad de Yaroslavl, al noreste de Moscú dijo que el país tomaba la iniciativa en la esfera de la IA basada en computador, la que gobernará el mundo. La IA le dará a la humanidad tecnologías que pueden mejorar nuestras vidas, pero igualmente permitirá a los gobiernos y otros librar un tipo de guerra mucho más terrible y aterradora, una Guerra Cibernética.

Las técnicas y la tecnología de la IA ofrecen una poderosa inteligencia de máquina avanzada a cualquier número de grupos que puedan pagarla, justamente hace 20 años, la capacidad de cómputo era muy limitada este fue la base de la investigación y posterior escritura del Libro Guerra Cibernética, el computador puede, de forma autosuficiente y proactiva, determinar si una infraestructura crítica es vulnerable a las vulnerabilidades conocidas de seguridad cibernética, un Programa de Aprendizaje Automático "*Machine Learning Program*", por sus siglas en inglés es un subcampo de las ciencias de la

[18] MARÍN, Nicolás, "Armas inteligentes, ¿la próxima revolución de la guerra?", El Espectador, 2018. https://tinyurl.com/4v6732jn

[19] GIGOVA, Radina, *¿Quién cree Vladimir Putin que gobernará el mundo?*, CNN Mundo, 2017. https://tinyurl.com/4uw46tht

computación y una rama de la IA cuyo objetivo es desarrollar técnicas que permitan que los computadores aprendan.

Concretamente se trata de crear programas capaces de generalizar comportamientos a partir de una información suministrada en forma de ejemplos. (Se suministran técnicas de ataque avanzadas y el computador las aprende, de igual forma su contraparte es efectuar ataques avanzados a partir del aprendizaje para evadir las defensas cibernéticas en una red de computadores objetivo).

VI. BATALLA MULTIDOMINIO

El computador por aprendizaje permite explorar grandes cantidades de datos y, por consiguiente, puede efectuar predicciones de alta confianza sobre la existencia de ataques de seguridad. La IA ha hecho un progreso increíble en estos últimos años con el aumento de la capacidad de cálculo en los supercomputadores y la interacción del aprendizaje dirigido y puesta final del conocimiento en los computadores. Con la capacidad actual de cálculo de los supercomputadores hay fenómenos que hace veinte años no se podían simular con precisión suficiente, hoy día con la IA se puede establecer y sacar provecho en la defensa y el ataque militar.

El computador también como mucha de la tecnología también es vulnerable a ser explotado por terceros por una amplia gama de razones, entre ellas la Ciberdelincuencia y la Guerra Cibernética, esto pone en peligro la seguridad de individuos, corporaciones y los Estado-nación.

Se observa entonces que el dominio cibernético se ha convertido en un “campo de batalla multidominio” para el acceso, la influencia, la seguridad y el control de las Fuerzas Militares de un Estado-nación, con ello las implicaciones estratégicas de estos desarrollos paralelos serán profundas, particularmente cuando se combinen exitosamente con la IA obligado a los militares a realinearse bajo lo que generalmente se le ha denominado “Batalla Multidominio”, la IA crea una amenaza cibernética más amplia, la perspectiva del blanco contra el cual se lanza un ataque cibernético y la naturaleza de los atacantes establece una nueva dimensión de la seguridad con la estrategia que debe asumir un Estado-nación en su Ciberdefensa.

"Hoy en día podemos construir redes neuronales gigantescas que ya son útiles para abordar problemas reales. El procedimiento es recopilar los datos del problema y con ellos entrenar una red neuronal. Esta red neuronal va a hacer predicciones sobre los comportamientos de ese sistema y va a actuar como un simulador basado en ecuaciones".[20]

El entorno de la información está siendo transformado por la revolución digital la que se encuentra respalda por los dominios emergentes, "la revolución industrial del siglo XXI es la revolución de la información". A medida que los sistemas militares (sistemas balísticos nucleares, control terrestre sobre flota de drones armados, etc.) dentro de un marco de guerra basado en operaciones de red de computadores se vuelve cada vez más autónomo, con el desarrollo inteligente de sistemas no tripulados en todos los dominios, la vulnerabilidad de estos sistemas militares se convierte en una preocupación importante con las prácticas de interferencia o el "control externo de los mismos".

Hoy en día está dada la posibilidad de enjambres autónomos (drones con autonomía de vuelo) se están convirtiendo en plataformas de armas del futuro espacio de batalla, con la capacidad de corromper, deshabilitar o dirigir remotamente al enjambre como factor decisivo en el combate, Estados Unidos ha instalado sistemas de IA en las estaciones de control terrestre para su flota de drones armados (MQ-1C), estableciendo capacidad de operar en enjambres gestionados por humanos, pero también se incorporó Ciberdefensa con el uso de IA para proteger el sistema.

La rápida evolución de la tecnología y el uso de los computadores es caracterizada hoy en día por la inestabilidad, complejidad, incertidumbre e información que se encuentra omnipresente en los mismos, las fuerzas armadas de un Estado-nación requieren operar en múltiples dominios. Desde el fondo de los océanos hasta la profundidad del espacio y en el ciberespacio las Fuerzas Armadas de un Estado-nación deben prepararse a fin de mantener y lograr superioridad táctica y la independencia estratégica frente a cualquier forma de amenaza.

"El desafío surgirá cuando los militares miren el marco del campo de batalla de la batalla multidominio, la fuerza en su conjunto tiende a estar geográficamente separada. Los efectos pueden ocurrir en la ubicación, pero en diferentes momentos". Al común de la gente

[20] VALERO, Mateo, *Supercomputación y revolución de la información*, The New Barcelona Post, 2018. https://tinyurl.com/uztjex6t

le gusta hablar sobre cómo será diferente el futuro de la guerra, pero ya ha comenzado a llegar. "La Batalla Multidominio" es un concepto diseñado para abordar este mundo cambiante: "Debemos poder superar las capacidades defensivas integradas de nuestro adversario, evitar el aislamiento y la fractura de dominios y preservar nuestra libertad de acción".[21]

La batalla multidominio busca integrar "Operaciones Multidominio" con el objeto de coordinar operaciones sin problemas a través de los cinco dominios: aire, tierra, mar, espacio y cibernética. Los dominios emergentes particularmente en esta última década, como el ciberespacio y el espacio, y el uso contradictorio de estos campos de batalla tienen hoy en día la imperiosa necesidad de replantear el propio ciberespacio como un ejemplo que desafía la estructura de la organización actual de la Fuerza Armadas en un Estado-nación.

La magnitud y la implacabilidad de un sondeo altamente automatizado e inteligente (Defensa en la red y vectores de ataque con Redes Neuronales) o el análisis de software en busca de vulnerabilidades muy seguramente constituirá una poderosa capacidad cibernética ofensiva/defensiva ante la generalización y grados de especialización y persistencia de la amenaza cibernética.

El Departamento de Defensa de los Estados Unidos busca acelerar su capacidad para detectar y responder a los ataques cibernéticos enemigos. Si bien la detección y la respuesta ante posibles ataques cibernéticos no son nuevas; en términos de seguridad informática ha asumido una mayor importancia ya que los ataques cibernéticos se combinan con operaciones cinéticas en todo el espacio de batalla.

Los comienzos de grandes cambios en el carácter de la guerra han sido visibles en lugares como el este de Ucrania y el Medio Oriente. A través de estos campos de batalla, los poderes rivales hicieron inversiones y desarrollaron doctrinas, proporcionando una amplia evidencia de que las guerras futuras prometen una letalidad extrema no vista desde la Segunda Guerra Mundial.

En el corazón de este enfoque defensivo está el Comando y Control (C2) de la defensa de red de un sistema de Ciberdefensa y las acciones del departamento de defensa de un Estado-nación. El Cuartel General de la Fuerza Conjunta - Red de Información del

[21] *Cfr.* PERKINS, David y HOLMES, Jame, "Multidomain Battle: Converging Concepts Toward Joint Solution", *JFQ 88*, 2018. https://tinyurl.com/yadwvmje

Departamento de Defensa (JFHQ-ODIN), es el componente del Comando Cibernético de los Estados Unidos frente a millones de ataques diarios de un amplio espectro de adversarios. Investigadores y hackers han demostrado que los sistemas integrados en red son vulnerables al ataque remoto. El programa de Sistemas Cibernéticos Militares de Alta Seguridad (HACMS) de DARPA está creando tecnología para la construcción de sistemas ciberfísicos seguros y protegidos.

VII. ATAQUE CIBERNÉTICO

En marzo de 2017, el 49,7% de la población mundial (más de 3,7 mil millones de personas) utilizó Internet (77,4% de la población de Europa y 88,1% de América del Norte). La evolución de la tecnología ha transformado el uso de internet y la actividad cibernética volviéndolas cada vez más interconectadas con las operaciones militares en el ciberespacio. Esto hace difícil establecer una línea divisoria entre lo civil y militar, ya que en el ciberespacio convergen actores comerciales y gubernamentales, así como civiles, tanto a nivel interno como internacional. Estas interacciones tienen un impacto significativo en las operaciones cibernéticas militares. Mientras que la "Guerra Cibernética" se centra exclusivamente en sistemas militares, la "guerra de redes" se extiende al ámbito civil, reflejando las complejidades crecientes de este entorno digital.[22]

Existe un vacío en referencia a las operaciones militares, muy seguramente porque los países son renuentes a expresar o manifestar públicamente sus debilidades cibernéticas, puesto que con ello no harían otra cosa que difundir sus vulnerabilidades, el revelar una vulnerabilidad puede llegar a significar que un Estado-nación renuncia a la oportunidad de recolectar inteligencia crucial que podría frustrar un ataque terrorista, detener el robo de propiedad intelectual de ese Estado o nación o incluso descubrir las vulnerabilidades más peligrosas que están siendo utilizadas por hackers para explotar las redes y sistemas de información.

El año 2018 establece un punto de referencia nuevo (enmarca diez años del uso de "ataques cibernéticos" en apoyo de operaciones militares cinéticas, en el 2008 durante la guerra de Georgia: en el que se conmemora el conflicto bélico que dejó unas 1.700 personas

[22] ARQUILLA, John, *et. al.,* "En el campamento de Atenea: Preparación para el conflicto en la era de la información", *Naval War College Review,* 1999, no. 2, vol. 52, pp. 1-2. https://tinyurl.com/yjdm8rfs

muertas y miles de desplazados, de acuerdo con las cifras oficiales.) En la Guerra de Georgia hackers rusos se habrían dedicado a bloquear algunas de las principales páginas del gobierno georgiano en Internet, este ataque cibernético ha sido considerado como la primera guerra cibernética que acompañó a un conflicto bélico a gran escala, desde entonces, se han multiplicado los ataques cibernéticos, Rusia consideró las operaciones cibernéticas junto con las de las Fuerzas Especiales Terrestres y Terrestres como operaciones principales a partir del inicio de la campaña contra Ucrania.[23]

Los ataques cibernéticos han se han convertido en ésta última década en una fuente de amenazas porque son capaces de acceder a sistemas de información gubernamentales, militares y diplomáticos, por ésta razón el asegurar el más alto nivel de protección de las redes de Comando, Control, Comunicaciones, Computadores, Defensa Cibernética y Sistemas de Combate e Inteligencia, Vigilancia y Reconocimiento (C6) para la gestión internacional de crisis y defensa nacional/colectiva se ha convertido en una de las principales prioridades para las Fuerzas Armadas de un Estado o nación, por consiguiente no es sorpresa que con el advenimiento de la era cibernética, se persiga de igual forma establecer una sólida capacidad para la defensa cibernética.

VIII. CIBEROPERACIONES

Actualmente las fuerzas militares y del orden nacional, organizaciones del sector público y privado deben lidiar con la infiltración constante por parte de los ciberatacantes, los ataques diseñados específicamente o con intervención de malware (del inglés malicious software, programa malicioso o maligno, también llamado badware, código informático malicioso), el malware dinámico o de características avanzadas busca a través del engaño esquivar con facilidad las herramientas de detección de amenazas tradicionales y explotar las debilidades inherentes a las redes modernas de acuerdo a la estructura y arquitectura de seguridad en cada organización, con ello la imperiosa necesidad de parches y detección de vulnerabilidades a la velocidad de máquina, escalables y automatizadas es grande y está creciendo rápidamente a medida que más y más sistemas, desde electrodomésticos hasta grandes plataformas militares, se conectan y dependen de Internet.

[23] GORDON, Michael R., "La estrategia militar innovadora del Kremlin desconcierta a todos", *La Nación*, 2014, no. 1, vol. 3, pp. 2-3.

Hoy en día, el proceso de encontrar y contrarrestar errores, hacks y otros vectores de infección cibernética y su ciberdefensa aún sigue siendo efectivamente artesanal. Entre muchos otros ejemplos se cita el error de seguridad de "Heartbleed" el cual ha estado y existido en muchos de los sistemas informáticos del mundo (prácticamente durante casi dos años y medio sin ser detectado o antes de que se descubriera y se distribuyera una solución en el año 2014), este sólo tipo de error con aprovechamiento de un programa maligno (*malware*) dirigido llego a generar aproximadamente medio millón de servidores de aplicación seguros vulnerables a robos o infiltración dirigida y coordinada.

Sin embargo, la infiltración no siempre implica un robo de datos ni otras formas de daños para la organización, especialmente si las mismas dominan la detección y respuesta rápida ante ataques, pero siempre existirá el conocimiento y capacidad del atacante para derrotar las defensas y controles de seguridad más avanzados, es por ello las organizaciones deben buscar intrusos activamente mediante un examen constante de su ambiente de TI detectando signos sutiles de actividad maliciosa o sospechosa, identificando estos signos tempranos de problemas, las organizaciones deben desarrollar nuevas capacidades de análisis de datos y respuesta ante incidentes cibernéticos (7x24, los 365 días del año), es prácticamente un examen constante del ambiente de TI en cada estructura interna de red, es una detección de signos sutiles de actividad maliciosa o sospechosa. Identificando estos signos tempranos de problemas, las organizaciones deben desarrollar nuevas capacidades de análisis de datos y respuesta ante incidentes.

Los principales marcos o "frames" de seguridad cibernética solo describen cuáles deberían ser las prácticas ideales, pero tienen poca, si alguna orientación sobre cómo implementar una solución parcial en Ciberseguridad o Ciberdefensa aplicada que es el mejor valor para el costo, cuando el financiamiento no es adecuado para lograr el ideal.

Las ciberoperaciones con el uso del computador se han constituido en las operaciones de las fuerzas militares como instrumento para la coerción y desgaste. "El ejército de los Estados Unidos está reforzando las defensas cibernéticas para contrarrestar las amenazas de los hackers que intenten obtener acceso a misiles nucleares y otras armas".[24]

[24] KATZ, Benjamin, *U.S. Beefs Up Cyber Defenses to Thwart Hacks of Nuclear Arsenal*, Bloomberg, 2016. https://tinyurl.com/2bvzjt2k

IX. HACKING

Ante la imperiosa necesidad de establecer una defensa cibernética automatizada, la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA), agencia del Departamento de Defensa de Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar estableció el primer torneo de hacking en este tipo de requerimientos.

En ésta última década en sistemas y tecnología hemos visto una lista de nuevas certificaciones de seguridad centradas en "*hacking*", son estas habilidades perfectas para personal sobre el terreno en busca de vulnerabilidades dentro de las organizaciones que utilizan métodos que un actor malintencionado emplearía para ganar acceso al sistema. Existen infinidad de herramientas que ofrecen la capacidad de buscar, encontrar, controlar e informar sobre su entorno, el obtener información y las prácticas de inteligencia son factores determinantes que desde hace varias décadas impulsan las operaciones en diferentes Estados o naciones. Desde siempre ha sido necesario contar con la capacidad de "recopilar información sobre un adversario" con ello se hace necesario pensar como el atacante desarrolla la capacidad dentro de nuestras arquitecturas a fin de contar igualmente con la capacidad de mitigar y/o reducir el riesgo siempre latente en la tecnología. La importancia de utilizar inteligencia ayuda a guiar la toma de decisiones de los comandantes militares para las operaciones futuras.

En muchos de los eventos realizados en Latinoamérica (seminarios, simposios, conferencias relacionadas con la seguridad digital y temas en referencia a la seguridad nacional) el planteamiento y teoría de dichos eventos en su gran mayoría no se ve influenciada con el planeamiento en referencia a las "operaciones militares", tampoco se diserta respecto de capacidades cibernéticas, tecnología militar y la interacción de los computadores en la estrategia de seguridad de un Estado, o respecto de la metodología y estructura militar utilizada en las operaciones del ciberespacio o espacio cibernético (escenario de posibles conflictos u hostilidades), en su gran mayoría los temas tratados se ven opacados por el desconocimiento y entendimiento de las operaciones en redes de computadores, de la metodología o marco utilizado en la evaluación de la seguridad, y específicamente en lo que concierne a seguridad en redes de computadores. Los computadores e internet son prácticamente dependientes de los seres humanos para obtener información.

El 21 de octubre del año 2016 una de las armas cibernéticas más poderosas y conocidas de ésta última década se publicó en línea, hoy día cualquiera puede utilizarla, la botnet "Mirai" basó su ataque principalmente en la ausencia de mejores prácticas de seguridad en el espacio del Internet de las Cosas (IoT), fue uno de los ataques de botnets DDOS (Denegación de servicios distribuidos, pos sus siglas en inglés) más grandes dirigido a "Dyn", compañía que controla una parte significativa de la infraestructura del sistema de nombres de dominio de Internet.

Una botnet es una red de computadores infectados con una variedad de *malware*. La capacidad de conectar dispositivos embebidos con capacidades limitadas de CPU, memoria y energía significa que IoT puede tener aplicaciones en casi cualquier área. La botnet Mirai tomó Internet por sorpresa cuando superó varios objetivos de alto perfil con algunos de los ataques de denegación de servicio distribuidos más grandes registrados actualmente (DDoS), este *malware* fue lo suficientemente fuerte como para eliminar segmentos enteros de Internet en países específicos. "Mirai" puede representar un cambio radical en el nuevo desarrollo evolutivo en las botnets desafiando con ello a los proveedores de servicios de Internet (ISP), de una u otra forma los ISP´s serían incapaces de procesar cientos de gigabytes de datos por segundo.

En lugar de usar computadores, la botnet Mirai infectó y aprovechó dispositivos más pequeños que comprenden el Internet de las cosas, incluidos enrutadores y cámaras de seguridad que tienen funciones de Ciberseguridad limitadas. El resultado fue un ataque masivo de 1,2 Terabytes por segundo que abrumó a los servidores Dyn e interrumpió sitios web como Twitter, The Guardian, Netflix y CNN, Mirai puede representar un cambio radical en el desarrollo evolutivo de las botnet.

Consecuentes con el desarrollo del *malware* a la medida los ciberdelincuentes y los Estado-nación de igual forma tienen acceso a una herramienta autosuficiente (la botnet Mirai) para desconectar casi cualquier sistema, precisamente éste es un tema que hace reestructurar la estrategia con el uso de potencial armamento cibernético y el pensamiento en sí mismo respecto de la seguridad cibernética.

Los expertos en Ciberseguridad habían advertido durante los últimos años respecto de posibles escenarios de confrontación respecto del aprovechamiento de la vulnerabilidad de un sistema conocido, este es uno de los cientos o millones de ataques que con la evolución

del malware se ha organizado y sistemáticamente se ha ido estructurado a través del tiempo, debilitando la capacidad de lucha de un Estado o nación. En el año 2015 el presidente Barack Obama ordenó a los funcionarios del Pentágono intensificar sus ataques cibernéticos y electrónicos contra el programa de misiles de Corea del Norte con la esperanza de sabotear los lanzamientos de prueba en los primeros segundos. Pronto, una gran cantidad de cohetes militares del Norte comenzaron a explotar, desviaron su rumbo, se desintegraron en el aire y se sumergieron en el mar.

X. A MANERA DE REFLEXIÓN FINAL. PLANIFICACIÓN DESDE LA SEGURIDAD CIBERNÉTICA

La seguridad cibernética debe planificarse en torno a la idea de lograr no solo una seguridad parcial, se ha de contar con los recursos financieros para hacer todo perfectamente todo el tiempo, porque la misma evoluciona muy rápidamente.

El comando y el control es la base sobre la cual se construyen la planificación y la ejecución de las operaciones militares, desde la presencia en tiempo de paz hasta las operaciones distintas de la guerra, la respuesta a las crisis, la guerra regional o mundial, el comando y control es la herramienta de uso esencial que usa el comandante al frente de las operaciones para hacer frente a la incertidumbre del combate y dirigir sus fuerzas para cumplir la misión asignada, refleja la forma en que organizamos, entrenamos y luchamos.

Los comandantes siempre buscan la solución “siguiente mejor” para alcanzar la supremacía sobre los adversarios en los dominios fundamentales para los sistemas de defensa y seguridad nacional, hoy en su última generación el C6ISR (Comando, Control, Comunicaciones, Computadores, Defensa Cibernética y Sistemas de Combate e Inteligencia, Vigilancia y Reconocimiento), ha desarrollado y definido el término “C2” (Comando y Control) por y para el ejército, pero realmente se relacionan con todos los aspectos de la organización militar.

Las acciones encomendadas en una operación requieren determinar factores diferenciadores que contribuyan al éxito de una operación, por ello en el ámbito militar es necesario implementar y establecer una Ciberdefensa sobre la base del conocimiento adquirido (esto es, cuando se conoce más al fondo al atacante, las técnicas, operaciones y medios utilizados), el conocimiento determina la forma de integrar las operaciones

cibernéticas de red de computadores al planeamiento en el nivel operacional, utilizando elementos del arte y diseño operacional.

La información es una herramienta vital para la toma de decisiones, es por esta razón y su tendencia en las últimas dos décadas ha sido el de contar con componentes o sistemas que aseguren el acceso a la calidad y veracidad de la información (recolección de información para la toma de acciones ofensivas o defensivas) afectando el ciclo y toma de decisiones del adversario a fin de proteger el propio, esto es; por medio de acciones desarrolladas en los diferentes dominios, los sistemas militares están altamente interconectados para comunicar, interceptar y controlar vastas franjas de territorio, en el mar y en el ciberespacio. Los desafíos de seguridad nacional de los Estados deben clasificarse adecuadamente y dividirse en desafíos de seguridad, desafíos de seguridad nacional (HLS, Homeland Security por sus siglas en inglés) y desafíos de defensa militar (Ciberdefensa), la Ciberdefensa Militar requiere que las organizaciones militares hagan frente a un invasor u otra amenaza que obligue a los militares a maniobrar dentro de un espacio dado utilizando los diversos modos de batalla. De otra parte, la Ciberseguridad y las fuerzas del orden (como la policía) proporcionan seguridad a los ciudadanos del Estado.

XI. BIBLIOGRAFÍA

Doctrina

BECERRA, Jairo, *et. al.*, *Derecho y big data*, Editorial Universidad Católica de Colombia, Bogotá, 2018.

BOUTHOUL, Gaston, *Traité de polémologie*, Payot, París, 1970.

CÁCERES, Jairo y GUTIÉRREZ, Juan*, Guerra cibernética, defensa en la red y vectores de ataques con redes neuronales*, Esdegue, Bogotá, 2018.

CÁCERES, Jairo, *Historia del sistema de información logístico coordinado del sector defensa de Colombia SILOG*, Esdegue, Bogotá, 2018.

GUTIÉRREZ VALDEBENITO, Omar, *Sociología militar*, Instituto Francés de Polemología, Santiago, 2002.

JOMINI, Antoine-Henri, *El arte de la guerra*, Edaf, Madrid, 1977.

KARL VON, Clausewitz, *Sobre la guerra* (1832-1834), libro 1, cap. 7, traducción de J.J. Graham, 2002.

LIBICKI, Martin*, Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Mónica, 2009.

RICHARD A., Clarke y ROBERT, Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, HarperCollins Publishers, Nueva York, 2012

STERLING, Christopher*, Military Communications: From Ancient Times to the 21st Century*, ABC-CLIO, Oxford, 2007.

Hemerografía

ÁLVAREZ RUBIO, Ariel, "El conflicto en Colombia, una perspectiva desde la polemología", *Estudios de Seguridad y Defensa*, 2014, no. 3, vol. 1, pp. 11-253. https://tinyurl.com/2n9shprt

ARQUILLA, John, *et. al.,* "En el campamento de Atenea: Preparación para el conflicto en la era de la información", *Naval War College Review,* 1999, no. 2, vol. 52, pp. 1-2. https://tinyurl.com/yjdm8rfs

GORDON, Michael R., "La estrategia militar innovadora del Kremlin desconcierta a todos", *La Nación*, 2014, no. 1, vol. 3, pp. 2-3.

PERKINS, David y HOLMES, Jame, "Multidomain Battle: Converging Concepts Toward Joint Solution", *JFQ 88*, 2018. https://tinyurl.com/yadwvmje

SNYDER, Samuel, "Computer Advances Pioneered by Cryptologic Organizations", *Annals of the History of Computing*, 1980, no. 1, vol. 2, pp. 61-62.

VIRVILIS, Nikos, VANAUTGAERDEN, Bart y SERRANO SERRANO, Oscar, "Changing the game: The art of deceiving sophisticated attackers", *NATO CCD COE Publications*, 2014. https://tinyurl.com/59drvr45

Páginas de internet

CALLOWAY, Audra, *El Ejército desarrolla mortero de precisión guiado por láser*, U.S. Army, 2017. https://tinyurl.com/ya779pbv

GIGOVA, Radina, *¿Quién cree Vladimir Putin que gobernará el mundo?*, CNN Mundo, 2017. https://tinyurl.com/4uw46tht

KATZ, Benjamin, *U.S. Beefs Up Cyber Defenses to Thwart Hacks of Nuclear Arsenal*, Bloomberg, 2016. https://tinyurl.com/2bvzjt2k

MARÍN, Nicolás, "Armas inteligentes, ¿la próxima revolución de la guerra?", El Espectador, 2018. https://tinyurl.com/4v6732jn

MARKOFF, John, *Scientists See Promise in Deep-Learning Programs*, New York Times, 2012. https://tinyurl.com/4a6seja5

Open AI, *AI and Compute*, 2018.

The Economist, *Cyberwar. The Threat from the Internet*, 2010, no. 8689, vol. 396, pp. 3-9.

VALERO, Mateo, *Supercomputación y revolución de la información*, The New Barcelona Post, 2018. https://tinyurl.com/uztjex6t