CAPÍTULO IV

EL QUINTO DOMINIO COMO INTERÉS NACIONAL EN COLOMBIA, UNA PERSPECTIVA PARA CONCEBIR LAS NUEVAS FRONTERAS DEL SIGLO XXI*

Jessica Andrea Rodríguez Gómez
Ingrid Catalina Téllez Córdoba

* Capítulo de libro que expone resultados en conjunto de dos proyectos de investigación (i) "Nuevas Amenazas en el siglo XXI: Fronteras y Derechos Humanos", de la línea de investigación "Políticas y modelos de seguridad y defensa" del grupo de investigación "Centro de Gravedad", reconocido y categorizado en (A1) por COLCIENCIAS, registrado con el código COL0104976, vinculado al Centro de Estudios Estratégicos en Seguridad y Defensa Nacionales -CSEDN-, adscrito y financiado por la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia y (ii) "Construcción de Paz y Desarrollo Sostenible: una mirada desde los Derechos Humanos y el DICA", que hace parte de la línea de Investigación "Memoria Histórica, Construcción de Paz, Derechos Humanos, DICA y Justicia" del grupo de investigación "Memoria Histórica, Construcción de Paz, Derechos Humanos, DICA y Justicia", reconocido y categorizado en (C) por COLCIENCIAS registrado con el código COL0141423 vinculado al Centro de Investigación en Memoria Histórica Militar (CIMHM) y a la Maestría en Derechos Humanos, Derecho Internacional Humanitario y Derecho Internacional de los Conflictos Armados (DICA), adscritos y financiados por la Escuela Superior de Guerra " General Rafael Reyes Prieto" de la República de Colombia.

Resumen
Para poder comprender la importancia que debe tener el ciberespacio en Colombia, que este sea elevado a prioridad de interés nacional y que sea el quinto dominio por parte de la defensa colombiana, es imprescindible mirar hacia el pasado y analizar cómo la naturaleza de la guerra juega un papel preponderante para comprenderlo, toda vez que ha venido evolucionado con tal rapidez que el surgimiento de novedosas herramientas utilizadas a través del ciberespacio para vencer en conflictos es la herramienta de ventaja hoy en día más utilizada con eficacia, la cual pone en vulnerabilidad a quien no logre adaptarse a ella. Esto, con el fin de establecer una estrategia para proteger los intereses geopolíticos del Estado colombiano en su quinto dominio de la guerra.

Palabras clave
Quinto dominio, nuevas amenazas, ciberfronteras, seguridad multidimensional y geopolítica del quinto dominio.

Abstract
In order to understand the importance that cyberspace must have in Colombia, to be elevated to a priority of national interest and to be the fifth domain in the Colombian defense, it is essential to look to the past and analyze how the nature of the war plays a preponderant role to understand it, since it has evolved so rapidly that the emergence of new tools used through cyberspace to overcome conflicts, is the most used tool of advantage today, which puts in vulnerability those who are not able to adapt to it. This, in order to establish a strategy to protect the geopolitical interests of the Colombian State in its fifth domain of war.

Keywords
Fifth domain, new threats, cyber frontiers, multidimensional security and geopolitics of the fifth domain.

Introducción

La globalización trae consigo nuevos retos, esto ha hecho que las naciones transformen sus intereses con el fin de adaptarse a los desafíos que traen las nuevas guerras al mundo moderno. El desarrollo de las nuevas tecnologías ha traído consigo al ciberespacio como un nuevo campo de confrontación. A pesar de ser intangible y aparentemente sin fronteras, los Estados lo han expuesto como un territorio que enfrenta nuevas amenazas para la estabilidad del sistema internacional.

Además de todas las posibles definiciones que tengamos de Ciberespacio, también es un nuevo campo de batalla, debido a los riesgos y amenazas que su uso masivo plantea y a la cada vez más dependencia tecnológica de todo el planeta.

El presente capítulo tiene como objetivo estudiar el ciberespacio como frontera y como generador de los nuevos escenarios que están transformando la concepción de la geopolítica tradicional. Colombia como Estado-Nación y Las Fuerzas Militares de Colombia han concebido al Ciberespacio como el Quinto Dominio de la Guerra, esto ha sido un gran paso teniendo en cuenta que los dominios tradicionalmente definidos en las operaciones militares eran solo cuatro: aire, tierra, mar y espacio electromagnético. Sin embargo, el artificial quinto dominio o ciberespacio, cobrará relevancia cuando por parte del Estado colombiano se defina como parte del interés nacional permitiéndole a Colombia adaptarse a los nuevos contextos del siglo XIX y que como Estado-nación se prolongue en el tiempo, priorizando la supremacía que las tendencias globales le exigen para su conservación.

La iniciativa de este estudio surge ante la problemática de definir qué es el interés nacional para Colombia y como está enfrentando la inseguridad que nace desde el ciberespacio en su territorio. Bajo la perspectiva de la defensa reconocer el ciberespacio como interés nacional es abrirse en nuevo camino que se aproxime a nuevos conceptos, en este caso ciberfronteras.

Bajo el entendido que Colombia es foco de los diferentes Estados del mundo y punto geoestratégico global, la necesidad de priorizar sus dominios y evitar fricciones entre los mismos para proteger su interés nacional es inminente. Teniendo el control de sus dominios la posibilidad de maniobra frente a los desafíos de las nuevas formas de guerra que varía entre las políticas agresivas en ambientes modernos complejos le proporciona a Colombia elementos para su subsistencia y expansión a futuro.

Por lo tanto, se pretende con este estudio que el quinto dominio, es decir el ciberespacio sea de interés nacional en Colombia y sea protegido desde la defensa a través de la aproximación al concepto de ciber-fronteras como una de las nuevas figuras que surgen a partir de los modernos escenarios propios del siglo XIX.

Los revolucionarios cambios en las formas de guerras que se han dado a lo largo de la historia de la humanidad son de gran interés por parte de la defensa de los estados, hoy por hoy la búsqueda de adaptabilidad en pro de la supervivencia y la protección hacen que la existencia de los estados dependa de como estén preparados para ello. En el caso del Estado colombiano, comprender las nuevas amenazas que tornaron en obsoletas algunos de los antiguos medios de protección como lo eran las "fronteras" vistas como medios de resguardo de las sociedades, es el primer paso para facilitar la razón que merece este estudio. Por tal motivo, los conceptos como naturaleza de la guerra y un rápido recorrido por su evolución, el interés nacional, el ciberespacio, las tradicionales concepciones de fronteras, serán motivo de estudio.

El impacto que genera el uso del ciberespacio en la realidad física y geográfica hace que el control de sus coasociados y del territorio sea cada vez más difícil de manejar por parte de los Estados, quienes es además

son vulnerables no solo por las ofensivas que puedan surgir desde otras naciones sino por las amenazas que puedan generarse desde su interior entre la moderna convergencia delictiva. Adicional pueden verse inmiscuidos en situaciones donde sean transgredidos por otros Estados a falta de leyes acordes a esta nueva realidad cibernética.

Este espacio que ya no es ficción, y que convive con la realidad tangible, tiene efectos reales, inmediatos, reta las distancias, el tiempo en simultaneo, permite el choque entre dominios entre otros, es decir, las nuevas formas de guerra que ya no se caracterizan por conflictos simétricos fronterizos son hoy por hoy una verdadera amenaza para cualquier Estado, por lo tanto, se reitera la necesidad de crear ciber-fronteras en el ciberespacio.

1. La geopolítica del Quinto Dominio de la guerra

De esta manera, se ve la necesidad de examinar cómo en la actualidad existe en el sistema internacional un ambiente que ofrece características particulares debido a las interrelaciones y operaciones a nivel cibernético, este espacio se encuentra estrechamente vinculado a las estrategias de poder. Aquí, los "puntos de control" de Buzai son tomados para representar de modo virtual el surgimiento de nuevas fronteras derivadas del acceso a la red, entre los países centrales y periféricos de cada hemisferio, esto amplia la fragmentación en la conexión de los países de cada continente.

En la mencionada estrategia, la relación ventajosa de los mismos respecto a los periféricos permite un control de las nuevas fronteras del siglo XXI. En relación a la estructura teórica mencionada, la presentación del cuerpo de ideas extraídas de la geopolítica clásica de MacKinder permite trasladar las problemáticas de las relaciones de poder geográficas pero adaptadas a la actualidad, específicamente al ámbito del poder en el ciberespacio.

Este transcurso permitirá establecer una directa relación sobre la importancia de la dimensión geográfica con la realidad virtual. Por delimitación de espacio, se dejará de lado otras importantes variables

como la del ámbito de la ciberdefensa y se hará uso de ciertos ejemplos que permitan visualizar los efectos físicos y políticos en las relaciones de poder en el quinto dominio de la guerra. Por lo tanto, se asumirá la atención necesaria sobre las tres principales variables (ciberespacio, geopolítica y poder), intentando así alimentar la teoría del *heartland* cibernético y dar cuenta de cómo el nuevo escenario mundial en un contexto de globalización y de traspaso de información va más allá de las fronteras físicas.

Con el fin de entender al ciberespacio en términos de relaciones de poder. Basado en Halford John Mackinder, se analiza esta zona como un *heartland* cibernético para los Estados en el sistema internacional moderno. Por medio de la articulación del ciberespacio, la geopolítica y la seguridad y defensa de los Estados, se pueden analizar los puntos de control en la jerarquía de poder del mundo en el quinto dominio de la guerra "Ciberespacio".

Para comprender al ciberespacio como un nuevo escenario para los desafíos de los Estados, se plantea un marco teórico propiciado por MacKinder, quien por medio de la teoría del *heartland* ayuda a visualizar la estrategia de la hegemonía de poder así: *"Quien gobierne los flujos comunicacionales gobernará el heartland cibernético y quien gobierne el heartland cibernético controlará el mundo"* (Prado, 2018, p. 1).

El sistema internacional moderno se ha enfrentado a la dinámica expansiva de los Estados, la geografía entorno físico-geográfico de los mismos se halla en constante movimiento; la perspectiva organicista de los Estados planteada por Ratzel plantea que las unidades políticas nunca descansan en sus cicatrices fronterizas, recrean constantemente la necesidad de un nuevo "lebensraum" Espacio Vital donde comprender los cambios a nivel sistémico (Laube, 2013, p. 27).

En la actualidad, este nuevo espacio vital ya no se refiere a las fronteras de tierra, mar o aire de las naciones, sino que se traslada al ciberespacio como nueva zona de interés para el sistema. Por tanto, la reducción de la geografía a la cartografía no debe continuarse con una reducción de la geografía a la política y sus necesidades culturales, sino que la geografía puede hoy extenderse a las conexiones cibernéticas de las realidades

sociales, y a partir de esta nueva relación elaborar un análisis político del mismo (Prado, 2018, p. 3).

De esta manera, la geopolítica permite relacionar elementos claves como el territorio, la sociedad y el poder. La teoría del *heartland* que propicia MacKinder toma relevancia en este estudio porque logra aunar estos factores y traducirlos con la idea de la conquista geoestratégica, en este caso del ciberespacio como zona de interés geoestratégico de los Estados.

Toda evolución tecnológica y la comprensión de las nuevas tecnologías de la información y de las comunicaciones (TICS) generan a cambios que modifican a nivel político y geoestratégico, las líneas de acción de los Estados. De esta manera, la profunda transformación en la tradicional forma de librar la guerra que las TICS generan es sólo la punta del iceberg de un complejo sistema de interrelaciones entre poder, tecnología y sociedad. (S Gastaldi y C Justribó, 2014)

La manipulación de las tecnologías cibernéticas refuerza la relevancia de la geografía, a través de la cibergeografía los Estados requieren de un nuevo trabajo sobre sus políticas en torno a la ciberdefensa, la detección y neutralización de nuevos desafíos en el ciberespacio como zona de influencia o hinterland sobre el cual ejercer control o trazar alianzas con alcance e interés político (Creig, 2002).

Por lo anterior, los Estados deben considerar la importancia de la geografía cibernética, por medio de esta los policymakers deberían trazar el mapa de intereses de cada país, explorar en su análisis los flujos de información, las bases de datos y reconocer, por consiguiente, la universalidad de la geografía cibernética y sus nuevas fronteras espaciales.

La teoría del *heartland* de Mackinder brinda una gran importancia otorgada a los accidentes geográficos, de manera que la esfera de acción del sistema humano abarca una extensión de dominio mundial. Hecho que permite comprender cómo las actuales estrategias de poder cibernéticas se encargan a través de los departamentos de defensa o corporaciones, como por ejemplo RAND (Research And Development) en Estados Unidos, no sólo de preservar y velar por el ámbito de seguridad y control de las informaciones, sino que aquellos países centrales con puntos de

control en los flujos de información logran imponer su voluntad política sobre asuntos internos de otros Estados. (Prado, 2018)

No obstante, hay quienes se mantienen escépticos sobre los verdaderos peligros de un gran ataque por internet. "No se trata de una guerra nuclear", como lo dijo Martin Libicki, experto en ciberguerra del centro de investigación Rand Corporation. Un ciberataque que sea tan costoso y peligroso como una guerra convencional al estilo de Irak y Afganistán". Para él, en teoría, un acto de "ciberterror" paralizaría al país únicamente por unos días o unas semanas, aunque reconoce que el componente defensivo de la estrategia es esencial, pues el país no podría estar inoperable unos días durante momentos críticos.

El origen de un ciberataque es muy difícil de averiguar, todos los países están enfrentados en el ciberespacio y tienen aliados como en el mundo físico, pero aun siendo aliados, también se espían unos a otros.

Por tanto, el ciberespacio es virtual pero no es imaginario, es un dominio artificial que existe en abstracto, es inmenso, se considera que para el año 2015 cerca de tres billones de humanos han cambiando las formas económicas de ver el mundo, a través de múltiples naciones que han ido creado infraestructuras independientes, el ejemplo de las redes que sumergieron al mundo en grandes cambios para controlar la industria a causa de la constante interacción. En consecuencia, este ecosistema funcional, propende a los habitantes del mundo a cualquiera sea peligroso para la aldea global (Klimburg, 2017, p. 25).

Alexander Klimburg afirma que hay muchos rankings de poderes basados en percepciones de sus elementos constitutivos, el conteo de capacidades cibernéticas, armas cibernéticas, tecnológicas destrezas, etc., esto es porque hay demasiadas variables y muchos de los componentes y capacidades se conservan ocultas. Lo anterior, concuerda con la falta de oportunidad de conocer las pretensiones de los Estados toda vez que la confidencialidad es necesaria cuando de seguridad de defensivas u ofensivas se trata. Mientras que Estados Unidos se basa en muchos de esos parámetros, el poder del quinto dominio es más poderoso, también es el más vulnerable, como lo demuestran los sucesivos ataques en él. A medida que los ataques invaden más profundamente en el dominio de

la información, los países democráticos se encuentran más vulnerables ya que es mucho más difícil para estos países equilibrar la seguridad versus otros miles de consideraciones (Klimburg, 2017, p. 26).

Superar el abismo entre la realidad de las apariencias estatales y utopía del ciberespacio libre de amenazas en un mundo ideal. De conformidad con Klimsburg el ciberespacio cambia tan rápidamente que parece haberse superado por los acontecimientos relacionados con su tema central de advertir a las democracias liberales de los peligros de la ampliación ciberseguridad a la seguridad de la información.

Sin embargo, al tratar de examinar los poderes democráticos y emergentes distintos a los Estados líderes del mundo o la idea de coaliciones de internet libre que fortalezcan aquellos Estados en vía de desarrollo ya sea bajo el liderazgo de las potencias o por sus propias agrupaciones, permitiendo demostrar que no se pueden subestimar los Estados, el autor enuncia a India y Brasil teniendo capacidades de "ofensiva creciente", y mantiene durante su escrito que el propósito en la comunidad global y entre gobiernos hoy en día se ha distorsionado toda vez que Estados manipuló la ciberseguridad global hasta el final de la primera década del siglo XXI, pero decidió no hacerlo de manera tajante puesto que la multidisciplinariedad que abarca este intangible restringe su capacidad de abarcarlo todo (Klimburg, 2017, p. 27).

2. El Quinto Dominio como la nueva frontera del siglo XXI

A continuación, se estudiará el ciberespacio bajo la perspectiva de ser una de las grandes amenazas globales, el detonante que abre fronteras y permite el acceso a lugares en tiempos simultáneos violando soberanías de forma silenciosa e invisible.

La idea de Manfred Grautoff de que la Humanidad pudiera desaparecer no es una idea lejana cuando a través de las relaciones internacionales y la geopolítica se comprende que cada nación tiene la indiscutible labor de protegerse de las nuevas formas de guerra que atemorizan

el mundo con bombas nucleares, ciberataques y ciberterrorismo entre otros.

En primer lugar, el concepto de ciberespacio fue creado por William Gibson (1948) quien lo concebido como un nuevo universo paralelo creado por humanos en las computadoras, la actual línea de comunicación por excelencia del mundo. El autor en mención hizo una descripción de lo que existía al interior de las computadoras y sus interconexiones; definió el espacio antropológico de la red informática como el lugar donde todos los usuarios al ingresar al ciberespacio se convierten en cibernautas, y quienes al mismo tiempo conforman cibersociedad, como las nuevas alternativas de socialización (Hernández, L; Ceceñas, P y Martínez, D, 2017).

Luis Manuel Martínez Hernández, insiste en describir el ciberespacio como un tráfico de conocimientos, entretenimiento, identidades alter humanas por medios electrónicos que transfiguraron la vida en sociedad.

Con dichas conexiones simultáneas a través de este espacio intangible, la transnacionalización es un hecho, en este sentido el concepto de fronteras se desfigura dándole un cambio abrupto a su concepción original, enfrentando al mundo a contextos que traspasan barreras físicas favoreciendo los procesos de integración planetaria a los que se resistieron las sociedades del pasado, moldeando la dimensión del conflicto humano a tiempos modernos, teniendo siempre en cuenta que mientras el ser humano esté involucrado en zonas donde coexistan unos con otros habrá conflicto (Commons, 2014).

Esta nueva figura no física que le permite a cualquier ciudadano del mundo indiscriminadamente acceder a otros lugares, personas, datos, información, entre muchos, en tiempo real; reta la supervivencia no solo de los individuos sino de los Estados desde el concepto de la geopolítica y su seguridad, los que en el pasado se sentían protegidos por fronteras artificiales o naturales, hoy en día se hayan vulnerables en un espacio incomprensible a la simple vista del ser humano, el ciberespacio.

De esta manera, el concepto de frontera puede entenderse como zonas contiguas y que le otorgan roles y competencias diferentes en la arena internacional. Desde una aproximación clásica de las Relaciones

Internacionales, se conciben las fronteras como delimitaciones físicas y geográficas entre países, estas tienen la misión de preservar la soberanía estatal y la seguridad nacional; la corriente teórica puede catalogarse como la *liberal* y entiende los espacios fronterizos como escenarios de cooperación e integración entre los Estados, más que como áreas de tensión y conflicto; finalmente, la tercera vertiente adopta una posición más crítica frente a la concepción tradicional de las zonas limítrofes y, por ende, alude a factores de identidad e ideas para sostener que más allá de su expresión física y territorial, las fronteras son constructos sociales que reproducen relaciones de poder, las cuales pueden propagarse por medio del lenguaje (Borda, 2014, p. 58).

En términos generales, estas tres aproximaciones teóricas sobre las fronteras proponen un debate acerca de la idea que se tiene de conceptos como la soberanía territorial, el Estado - Nación, la seguridad nacional, el papel de las zonas limítrofes en las relaciones entre Estados y el tipo de interacción que éstas generan.

El termino ciberespacio fue creado por el hombre, fue consolidado en el siglo XXI, en donde su rápido acceso fue determinado como "igualdad y horizontalidad" para los Estados, lo que encubre una jerarquía de poderes, específicamente de países centrales con mayor soberanía tecnológica que los periféricos y en donde el conflicto armado internacional podría tener lugar.

Dado que internet encubre esta supuesta la igualdad y la horizontalidad, Buzai reconstruye en un análisis político, diciendo que a pesar de que el ciberespacio posee centros y periferias y genera una nueva geografía y fronteras entre los Estados. Lo que encubre entonces son las nuevas desigualdades del siglo XXI que muestran nuevas fronteras sedientas de cercanía virtual y con dependencia tecnológica (Buzai, 2014).

En el escenario internacional, el espacio geopolítico ha extendido su conceptualización clásica dividida en terrestre, marítima y aérea, y añade, asimismo, el espacio ultraterrestre y el cibernético. En palabras de Buzai: "el ciberespacio aparece como una matriz electrónica de interconexiones entre bases de datos digitales, a través de sistemas computacionales conectados en la red" (Buzai, 2014, p. 87).

Teniendo en cuenta lo anterior, el Estado colombiano ha adoptado al Ciberespacio como nuevo campo de batalla o quinto dominio después de la tierra, el mar, el aire y el espacio, esto debido a los riesgos y amenazas que su uso masivo plantea y a la dependencia tecnológica del sistema internacional.

En este sentido, la importancia de que la ciencia y tecnología se haya modernizado de manera rápida repercutió en las formas de cómo se abordan las guerras en el pasado. Con las nuevas herramientas que le proyectó la industria a la sociedad y a los conflictos con avances de producción de armamento más la con tecnología moderna, se ha determinado que en el ámbito militar las sociedades debían replantear las concepciones clásicas de seguridad y defensa, así como en sus planteamientos estratégicos (Gil, 2017).

En consecuencia, dichos cambios en la concepción de la defensa y seguridad tradicional comprendieron que los enemigos de los Estados utilizan con más frecuencia ofensivas de destrucción que limitan las reacciones oportunas de la defensa, jugando con la movilidad en el tiempo y en el espacio, salvándose de ser catalogados como victimarios por falta de pruebas imputables, sin evidencia física (tangible) sin localización, es poco probable que existan represalia o justicia.

Por lo anterior, este intangible sin fronteras creado por el ser humano, advierte de nuevas amenazas no solo entre Estados, sino para las empresas y los mismos ciudadanos hoy en día, así como en otros dominios de la guerra "se pueden combatir guerras o estar en ellas sin haberse declarado" (Carracosa, 2017) (Pérez, 2017).

Los nuevos términos que surgen a partir de este universo son el de la Aldea global de McLuhan Marshall, como expresión de la exponencialmente creciente de interconectividad humana a escala global que nace por los medios electrónicos de comunicación. En 1968, McLuhan publicó el libro Guerra y paz en la Aldea Global. La velocidad de las comunicaciones transformaría los grupos sociales humanos proyectando su estilo de vida similar al de una aldea, el progreso tecnológico repercute en visualizar a los habitantes del planeta como seres capaces de conocerse unos a otros y a comunicarse de manera instantánea y directa. (Marshall, 1995).

El principio que destaca en este concepto es el de un mundo interrelacionado, con estrechez de vínculos económicos, políticos y sociales, producto de las tecnologías de la información y la comunicación (TIC), particularmente Internet, como disminuidoras de las distancias y de las incomprensiones entre las personas y como promotoras de la emergencia de una conciencia global a escala planetaria, al menos en la teoría. Esta profunda interrelación entre todas las regiones del mundo originaría una poderosa red de dependencias mutuas y, de ese modo, se promovería tanto la solidaridad como la lucha por los mismos ideales, al nivel, por ejemplo, de la ecología y la economía, en pos del desarrollo sustentable de la Tierra, superficie y hábitat de esta aldea global.

Por otro lado, no deja de ser verdad que, como ya evidenciaba la teoría del efecto mariposa (teoría del caos), un acontecimiento en determinada parte del mundo puede tener efectos a una escala global, como por ejemplo las fluctuaciones de los mercados financieros mundiales.

3. La defensa de los Estados y el Quinto Dominio de la guerra

El cómo se concebía la guerra en espacios fronterizos del pasado, parece hoy en día ser arcaico, los duelos eran los escenarios típicos que definían el dominio de las poblaciones, territorios y recursos, a través de confrontaciones cuerpo a cuerpo que por lo general tenían lugar en zonas fronterizas físicas. La estrategia daba como resultado el número de bajas y el debilitamiento del enemigo lo cual determinaba la victoria (Calduch, 1993).

De acuerdo con Alberto Bolívar Ocampo en su artículo "La era de los conflictos asimétricos", el autor no estaba equivocado cuando afirmó que con el advenimiento de la Revolución Industrial y la disponibilidad en el campo de batalla de medios capaces de desplazar grandes masas de personas y de desatar poderosos fuegos de artillería en la búsqueda de la atrición, mediante el enfrentamiento de potencia contra potencia y el empleo ingente de recursos, seguramente quedaría también en el pasado

con las anteriores formas precarias de guerra, pero también advierte que la evolución es constante y en el futuro más próximo desatará guerras sin siquiera moverse de su lugar de origen, por lo tanto, surge el concepto de guerras asimétricas quedado la guerra armamentista de una u otra forma reducida (Bolívar, 2002).

La guerra cibernética no es una guerra convencional ya que no existen fronteras ni leyes sobre este espacio. Pero, en el año 2013 el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (CCD-COE) publicó el Manual de Tallin, este expone sugerencias sobre el acercamiento del ciberespacio como zona de importante para la seguridad y defensa de las naciones al Derecho Internacional y las responsabilidades de los Estados en los conflictos cibernéticos.

Este Manual resulta necesario para encuadrar las acciones ofensivas y defensivas de actores en el ciberespacio, lo que requiere un encuadramiento normativo de la dinámica de los conflictos en ese nuevo ambiente operacional signado por lo tecnológico, siendo ésta la primera en su tipo.

En un mundo cada vez más interrelacionado por el denominado proceso de globalización e incrementado por el ciberespacio, las Políticas de Defensa de los Estados constituyen un factor preponderante para la fijar alianzas y proyectos en conjunto que aseguren el desarrollo de los mismos acordes al nuevo escenario mundial (Fonseca, Perdomo, Arozarena y Ortiz, 2013).

Las políticas de Defensa de los Estados deben atender al concepto de Fronteras Virtuales, este como nuevo fenómeno de nuevas interacciones que se producen en el sistema. La función de la Defensa es similar para las distintas naciones, tendiendo como objetivo prioritario mantener la Soberanía y la integridad territorial.

Las Nuevas Amenazas y riesgos han hecho surgir una visión más amplia del problema abarcando todos los aspectos de la realidad de un país, la Defensa Nacional, así como aspectos económicos, tecnológicos y ambientales, ampliando los conceptos de Seguridad Internacional, el surgimiento de la nueva amenaza de ciberataques a infraestructuras críticas que ponen en riesgo la libertad de acción de los Estados comienza a ser cada vez atendido en la agenda de amenazas asimétricas dando como

respuesta la creación de organismos responsables para contrarrestarles en el marco de nuevas políticas de seguridad y defensa cibernética (Fonseca, Perdomo, Arozarena y Ortiz, 2013, p. 128).

Una guerra sigue siendo guerra a pesar de que ésta sea librada en el ciberespacio en vez de los ámbitos tradicionales de tierra, agua y del aire. Así, esta zona debe seguir siendo considerada como un escenario más en el cual los Estados a través de sus Fuerzas Militares participarían en guerras cibernéticas, cabe investigar si es posible aplicar el "ius ad bellum" (o el derecho que regula el recurso de la fuerza por parte de los Estados) y el "ius in bello" (Derecho de la Guerra o Derecho Internacional Humanitario, que regula el comportamiento durante el uso de la fuerza en un conflicto armado), siendo éste uno de los mayores desafíos para los hombres del derecho.

Tener en cuenta al quinto dominio como territorio y dentro de los intereses nacionales es fundamental para preservar la defensa de los valores y principios constitucionales y democráticos, así como los derechos fundamentales de los ciudadanos en el ciberespacio, especialmente en la protección de sus datos personales, su privacidad, su libertad de expresión y el acceso a una información veraz y de calidad (Chadwick, 2015, p. 5).

La necesidad inminente que han venido desarrollando los países para cuidar su quinto dominio después del atentado del 9 / 11 en Nueva York, ha aumentado estratégicamente, los convenios internacionales y las alianzas cada vez son más fuertes, la relevancia que han cobrado ha internacionalizado la necesidad estratégica de cooperar para dar resultados ante ofensivas en el quinto dominio. El orden mundial es una constante en movimiento, para Estados Unidos el reto diariamente es enorme, la nueva estrategia de inteligencia de EE. UU. se centra en las amenazas cibernéticas y la IA, exponiendo ante el mundo el cuidado de sus ciberfronteras, protegiéndose como Estado Nación de sus enemigos. De acuerdo con la publicación por Daniel Holl - La Gran Época de 26 de enero de 2019 "Los países y organismos antagónicos a Estados Unidos están ampliando su capacidad para amenazar la seguridad estadounidense, según la última Estrategia Nacional de Inteligencia emitida

por el Director de Inteligencia Nacional (DIN)". La estrategia es actualmente dirigida por Daniel Coats, en un documento que resumen de la dirección estratégica de las agencias de inteligencia de Estados Unidos para los próximos cuatro años (Holl, 2019).

La importancia del quinto dominio se ve reflejado en la estrategia que identificó las amenazas cibernéticas y las tecnologías emergentes como la inteligencia artificial (IA) dos campos que China ha venido trabajando con bastante rapidez y que cautela la seguridad del país del hemisferio. El informe describe los ataques cibernéticos como un desafío institucional del gobierno de Estados Unidos, mientras que causan enormes costos económicos cuando se pone en peligro la información confidencial.

Para Colombia como aliado estratégico de Estados Unidos, la cooperación debe ser constante, el Cibercomando colombiano ha demostrado por primera vez, la identificación de la infraestructura critica, las ofensivas y defensivas; es un paso para proyectar la seguridad nacional con enfoque al quinto dominio y no quedarse a la espera de amenazas latentes. Las nuevas mejoras en la capacidad militar y de inteligencia resulta ser para el adversario un juego de ajedrez, el orden mundial depende de cuánto poder y dominio se tenga en las ciberfronteras de los Estados y según la nueva estrategia estadounidense, China es uno de los pocos países mencionados específicamente en el documento.

"La modernización militar china y la búsqueda continua del predominio económico y territorial en la región del Pacífico y más allá siguen siendo una preocupación", según el informe, aludiendo a los avances geopolíticos del régimen chino a través de las inversiones en todo el mundo del proyecto 'Un Cinturón, Una Ruta', así como a su agresiva defensa de las reivindicaciones territoriales en el Mar del Sur de China.

La estrategia también desarrolla a través del control del quinto dominio facilidad de reacción en vía satélite, o la proyección de una amenaza potencial en este campo. Son alrededor de 17 entidades del poder ejecutivo que conforman la Comunidad de Inteligencia (CI), en los Estados Unidos, con 2 agencias independientes, 8 elementos de defensa y otros 7 departamentos (Captura de pantalla / dni.gov).

Para el país que lleva la batuta en el orden mundial es claro que, si se pone en peligro el quinto dominio abarcado en todas sus dimensiones, "las amenazas cibernéticas representarán un riesgo cada vez mayor para la salud pública, la seguridad y la prosperidad".

Por otro lado, el control estratégico del quinto dominio representa la agresión de la inteligencia artificial que es manipulada a través de este dominio, Agresión por Inteligencia Artificial; el sistema Su, sistema Skynet de cámaras de seguridad mejoradas por la inteligencia artificial, y que cubrirá todo el país asiático para el año 2020, aprovechándose de su sistema político llevará a cabo la vigilancia en tiempo real de sus ciudadanos. Lo que dificulta para el resto de los Estados que su población esté de acuerdo y puedan perder credibilidad en sistemas demócratas y con libertades preestablecidas.

Por su parte "La principal responsabilidad de nuestro Gobierno es con nuestro pueblo y con nuestros ciudadanos: atender sus necesidades, garantizar su seguridad, preservar sus derechos y defender sus valores", aseguró Donald Trump durante la presentación de la nueva estrategia de Seguridad Nacional.

En variadas ocasiones China ha dicho que se debe reconocer "los errores del pasado para colocar a Estados Unidos en el lugar que merece", y enfatizó la necesidad de "crear fronteras", "proteger la patria" e incluir un plan económico internacional que defienda también sus intereses. Por lo cual se puede inferir que no es un secreto la rivalidad del control de sus dominios en especial el quinto que hace más vulnerable la defensa de cualquier país, inclusive, así sea el primero en el sector defensa.

La nueva política refleja sus prioridades de "Estados Unidos, primero" de proteger el territorio y las fronteras y las ciberfronteras al fortalecer el ejército y la ciber seguridad con sus ya nombrados 17 departamentos que lo conforma, para proyectar fuerza en el exterior y aplicar políticas comerciales más favorables Estados Unidos trabaja constantemente con sus alianzas y cooperaciones, la instucionalidad y la legitimidad varía de cuán villano parezca ante el mundo por lo cual la cooperación se hace cada vez más importante.

El presidente actual promulgó la necesidad de defender valores nacionales, de proyectar el interés nacional como el Estado de derecho y los derechos individuales, para que sus coasociados se sientan seguros contribuyendo a verse como un Estado sólido, estable, próspero y soberano.

La posición de influencia de los Estados Unidos en el mundo como fuerza positiva que puede contribuir a generar las condiciones para la paz, el buen manejo de la teoría de la contención y el buen desarrollo de los países que por años lo han visto como un antagonista de extractor de recursos para sus propios intereses.

4. Las amenazas del Quinto Dominio

Así como las amenazas que enfrentan mar, tierra y aire; el quinto dominio es un fenómeno que enfrenta amenazas como el crimen, la guerra y el terrorismo; estas acciones están experimentando un fuerte apogeo que contrasta con la débil preparación de los Estados y organizaciones para hacerles frente.

Las ciberamenazas son todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Abarcan un amplio abanico de acciones. Las ciberamenazas se caracterizan por su diversidad tanto en lo que concierne a capacidades como a motivaciones. Afectan a la práctica totalidad de los ámbitos de la Seguridad Nacional, como la Defensa Nacional, la seguridad económica o la protección de las infraestructuras críticas, entre otros, y no distinguen fronteras.

De acuerdo a Taylor Owen en su escrito *Disruptive power "the crisis of the state in the Digital Age",* Estados Unidos, quien creó Internet en principio como un proyecto de investigación de defensa, ahora considera el ciberespacio un dominio o campo de batalla potencial de igual importancia que la tierra, el aire del mar y el espacio exterior, por lo cual los actores que amenacen con ataques deben ser controlados y foco de su control. En consecuente Taylor cita a el profesor Yochain Berkman, de la Universidad de Harvard quien advirtió que los individuos pueden ahora

hacer cosas que reemplacen o amenacen las diferentes instituciones incluidas las de las relaciones internacionales, la diplomacia, el desarrollo y la guerra (Chadwick, 2015).

El profesor Yochain no está equivocado con las afirmaciones anteriores en sus estudios, el crimen en el quinto dominio comprende un amplio espectro de delitos entre los que cabría citar la piratería de software, juegos, música o películas; estafas, transacciones fraudulentas, acoso y explotación sexual, pornografía infantil, fraudes de telecomunicaciones, amenazas, injurias, calumnias, etc. Como se puede deducir, el cibercrimen persigue fundamentalmente conseguir un beneficio económico, pero también incluye el dominio de Internet con fines inmorales.

En cuanto al terrorismo, aunque está muy vinculado con el cibercrimen, se diferencia de ésta en que no persigue principalmente un fin económico, sino que se centra más en aquellas acciones en las que se persigue intimidar, coaccionar y causar daños con fines fundamentalmente político-religiosos. El ciberespacio se está consolidando como un santuario de terroristas debido a que está siendo utilizado cada vez más por éstos. Las acciones que llevan a cabo en él pueden ser de financiación, guerra psicológica, reclutamiento, comunicación, adoctrinamiento, propaganda, entre otras. Teniendo en cuenta que las guerras actuales se libran tanto en el campo de batalla como en la esfera de la información, la superioridad militar de un bando en el campo de batalla convencional puede provocar que el más débil se focalice en la red con el fin de equilibrar la balanza de poder (Chadwick, 2015, p. 10).

La falta de regulación y la ocultación que ofrece la red hace que los grupos terroristas realicen sus acciones con total impunidad. El cierre de sitios web no supone ningún problema para ellos ante la facilidad con la que encuentran nuevos servidores donde colocar sus páginas y seguir con sus actividades.

El carácter transversal de las amenazas exige que la ciberseguridad sea afrontada con una perspectiva integral que comprenda a las administraciones públicas, al sector público y privado y a la sociedad en su conjunto, en tanto puede tener implicaciones simultáneas en aspectos

tan diversos como la soberanía, los derechos fundamentales, la defensa, la economía y el desarrollo tecnológico.

La defensa de los Estados debe evolucionar continuamente para ir adaptándose a una amenaza que lleva la iniciativa y que se multiplica por el efecto que genera su alto grado de impunidad. Todo ello, mientras la superficie a defender se incrementa y complica cada día.

En este sentido, la seguridad de las redes y sistemas de información requiere potenciar las medidas de prevención, detección y respuesta, fomentando la seguridad por diseño y por defecto, que debe estar incorporada tanto en el desarrollo de productos y servicios tecnológicos, como en su actualización o manera de utilización.

5. El Quinto Dominio de la guerra como interés nacional en Colombia

En el caso de Colombia, no es claro afirmar que el ciber espacio sea parte del interés nacional. En términos de defensa, como ya se ha reiterado en este escrito, éste quinto dominio sería, entonces, la clave para mantener la estabilidad de los Estados nación.

En el Manual de Tallin, el ciberespacio debe ser visto como esos nuevos espacios contemporáneos susceptibles de llevar a la humanidad hacia la ciberguerra, quizás hablando en términos más macabros hacia el ciberapocalipsis. Por tanto, la nueva regulación del Derecho Internacional y las responsabilidades de los Estados en los conflictos cibernéticos es inminente, el modo político de soberanía no desaparece, este punto hace referencia al concepto positivista de la norma, es decir, según los planteamientos de Ariel Vercille, la norma deberá articularse con los diferentes dispositivos tecnológicos que está agrandando la concepción de soberanía al quinto dominio, el ciberespacio (Vercelli, 2004).

Lawewnce Lessig afirmó que quien cree los códigos y quien maneje la tecnología estará, sin ningún intermediario legislando, construyendo el futuro de las naciones y las culturas. Las nuevas regulaciones logran moldearse con el diseño de los entornos digitales y comienzan a direc-

cionar las conductas, los espacios en Internet a través de un nuevo arte regulativo (Lessig, 1999).

En Colombia apropiarse de todo este escenario es una necesidad que no puede desconocerse, es importante entender quién es Colombia para el mundo, y cuáles son las ventajas de la posición geoestratégica que posee. El acceso a dos océanos, al amazonas, el clima, la diversidad, la fauna, los recursos.

Así las cosas, Colombia se ha visto involucrada en estos nuevos contextos y no puede desconocer que es en el ahora y no en el mañana que la regulación sincronizada con su legislación debe ser un hecho para tener el control de su Estado.

Colombia ha dado muestras de su interés cuando en el año 2015 creó el Comando Conjunto para la Ciberseguridad. Colombia entendió que; si se considera que el ciberespacio es un nuevo espacio social múltiple de la realidad virtual, compuesto por una matriz de datos digitales donde se interactúa con el resto del mundo, con quienes tienen el poder; no puede ser material secreto del Estado y por el contrario de ser entendido como interés nacional público al cuidado.

Clemente Herrero afirma que a la vez que se protege la información. "Esto ocurre entre ciertos países que cuentan con un comando central con base en parámetros de inteligencia, tecnología y logística. China, Rusia, Corea del Norte e Irán y, por supuesto, Estados Unidos han mostrado avances en ciberguerra" (Herrero, 2013).

Los ataques Ciberneticos son constantes y están creciendo en frecuencia e intensidad. Pueden destruir estructuras físicas y sistemas operacionales, paralizar ciudades y generar millonarias pérdidas, inclusive costar vidas. Pero los instrumentos de todo este caos no son balas, bombas o tanques; son "bits y bytes". Así lo catalogó William J. Lynn III, el subsecretario de Defensa de Estados Unidos, al presentar la primera Estrategia para Operar en el Ciberespacio en el año 2011, también afirmó que es un programa con miras a proteger la nación de un potencial y devastador ataque en la red contra su infraestructura crítica, sistemas clave y otros intereses físicos y electrónicos (Marquéz, 2011). Para el Departamento de Defensa (Pentágono), "el ciberespacio es un campo de

operaciones igual a la tierra, mar, aire o espacio y, por ende, igualmente sujeto a ser escenario de maniobras defensivas y, si es necesario, ataques preventivos y represalias".

6. Estrategia para proteger los intereses geopolíticos del Estado Colombiano en su Quinto Dominio de la guerra

Al entender al ciberespacio como dimensión debido a que se trata de "un dominio que no es físico sino virtual", los Estados deben aún adoptarlo como una locación física específica con el fin de ser entendido como frontera. Esto, con el fin de direccionar objetivos nacionales específicos a la defensa del quinto dominio, en el camino a esta adaptación a los nuevos desafíos cibernéticos del sistema internacional se logrará revelar la incertidumbre y carencia de evidencias sobre la autoría de los posibles ciberataques de una figura independiente hacia un Estado o de un Estado a otro, lo cual posibilita vulnerar sus capacidades militares, he aquí el ámbito restringido en el que la defensa debería hacerse presente y no extendiendo la militarización hacia las consideradas "nuevas amenazas" (Aguilar, 2010, p. 181).

Las tecnologías de poder cibernéticas tienen límites internos y externos inagotables, observando esto desde la ciber geografía se puede identificar que el ciberespacio es entendido como una nueva dimensión de disputa del poder, las posiciones de intereses individuales de los usuarios desactivan los espacios culturales según región y extienden cada vez más la globalización como un mecanismo poderoso para su desenvolvimiento.

Esta nueva dimensión modifica los espacios culturales y establece un nuevo orden en la estrategia de poder, en la que los Estados que han logrado un avance tecnológico importante ejerzan el planeamiento estratégico geopolítico a nivel internacional. La reconstrucción de este nuevo tablero de soberanos inscribe a la ciber geografía en un estatus muy especial porque determina el acceso a flujos comunicacionales, mediciones

a la conexión en Red de los diversos países y la base de datos que estudia los intereses de las poblaciones (Prado, 2018).

Las unidades políticas que logran tener la soberanía tecnológica y efectivizar el control del tráfico de Internet y sus flujos informáticos tienen el dominio mundial. Así, la jerarquía de poder en el *heartland* cibernético ilustra la nueva historia insustancial e inconmensurable, la historia de una red de redes cuyo campo de batalla transcurre sin rostros ni nombres sino por medio de las arterias del nuevo cuerpo mundial: los cables de internet. Y cuyas armas podrían estar a un clic de desabastecer, perjudicar, vulnerar y deteriorar otras unidades políticas con fines e intereses políticos (Prado, 2018, p. 12).

La fuerza pública debe crear estrategias que protejan la Nación en su quinto dominio, aquellas comunidades que desarrollen este tipo de tecnología estarán en cambiando al mundo a obedecer sus propuestas, por lo tanto es menester de la fuerza encontrar estrategias que enfoquen a una Colombia que gobierne y no que sea gobernada.

En Colombia las Fuerzas Militares diseñaron como primera estrategia de defensa el Comando Conjunto de Ciberdefensa (CCOC) en el año 2012, el CCOC es una Unidad Militar fundada el 10 de octubre de 2012, con la misión de direccionar, planear, coordinar, integrar y sincronizar, a través de unidades y/o dependencias el desarrollo, la ejecución y conducción de actividades y operaciones cibernéticas conjuntas, combinadas, coordinadas e interagenciales con el fin defender las infraestructuras críticas cibernéticas que le sean asignadas, de acuerdo a su misión constitucional, ante las amenazas que atenten contra la seguridad y defensa del Estado Colombiano en el ámbito cibernético, dentro del marco de la legalidad soporte de la legitimidad institucional (Comando Conjunto Cibernético, 2017).

El CCOC desde su creación viene adquiriendo y desarrollando habilidades y destrezas de Ciberdefensa, inteligencia y respuesta, ante una agresión que afecte los intereses nacionales. Para la consecución de este fin, el CCOC ha basado el desarrollo de su estrategia en personas, procesos y tecnología, considerando que el talento humano es el factor fundamental, así las cosas, el personal del Comando y de las Unidades

Cibernéticas de las Fuerzas requieren de un proceso continuo de capacitación y entrenamiento persistentes en todos los niveles de la estrategia de defensa" (Comando Conjunto Cibernético, 2017).

La convergencia[15] de los enemigos de los Estados cada vez es más notoria gracias al ciberespacio, por ello Colombia debe protegerse no solo de las guerras de guerrillas de las largas décadas del siglo XX, sino que además, debe desarrollar medidas contra las ofensivas de los grupos narcoterroristas que operan a través del ciberespacio, un solo hacker de manera simultánea puede atentar contra el Estado colombiano en cuestión de minutos.

La capacidad de monitorear y recolectar las comunicaciones digitales en el área de operaciones es un elemento clave para cumplir un papel importante en el ciberespacio como actor estatal. La incapacidad de observar lo que pasa a través del terreno digital es similar a la incapacidad de llevar a cabo la vigilancia aérea de un área física de operaciones. Para lograrlo, se requerirá el acceso a la infraestructura de comunicaciones digitales de esa ciudad, incluyendo las redes celulares e internet alámbrica (Commons, 2014).

A pesar de su alto contenido confidencial, la seguridad en Colombia debe abarcar todos los aspectos necesarios para que se catalogue La Estrategia Nacional de Ciberseguridad como el dominio que protegido por ciber fronteras mantiene vivo el Estado Colombiano.

El ciberespacio para el Estado colombiano de entonces ser visto como un espacio más allá de lo global, que proporcione una visión conjunta del ámbito de la ciberseguridad, los avances en materia de la estrategia. Las actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad colombiana actual y la tecnología e infraestructuras que forman que la conforman son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio uno de los principales riesgos para el continuo desarrollo.

15 La convergencia consiste en la aproximación entre actores del crimen organizado y actores terroristas o políticos y, bajo la interpretación de Moisés Naím, es importante resaltar el accionar de las redes del crimen transnacionales. Igualmente, el autor alerta que las organizaciones criminales no buscan acabar con el Estado –a diferencia de las organizaciones subversivas- sino infiltrarlo para desarrollar sus actividades ilícitas.

Determinar las amenazas y desafíos en el ciberespacio para Colombia, es construir la estrategia de defensa que contrarreste a los adversarios y las posibilidades que no pueden ser subestimadas a la hora de pensar en un ataque, elevándolas a estrategias que contrarresten el alto impacto ante cualquier ataque. Clasifica estas amenazas en categorías, permite discriminar uno a uno de los activos estatales tanto intangibles como tangibles y aquellos infractores que son potenciales enemigos del Estado activos en el ciberespacio. Los principios rectores de la Estrategia de Seguridad Nacional determinan los objetivos específicos y sus líneas de acción (Gobierno de España, 2019).

El Estado español en el presente año emitió la Estrategia Nacional de Ciberseguridad del Estado, estas líneas de acción se dirigen a: reforzar las capacidades ante las amenazas provenientes del quinto dominio. El Estado de España creó esto con el fin de adecuarse a este nuevo escenario cambiante, se proponen un conjunto de Líneas de Acción y medidas más dinámicas que permitan, si fuese necesario, una rápida adaptación del ecosistema de ciberseguridad nacional, basadas en un modelo de gobernanza con una considerable madurez, donde debe participar activamente el sector privado y el resto de la sociedad civil.

En este sentido, la estrategia se concibe como un documento vivo que ha de adaptarse a la evolución de la ciberseguridad, por lo que deberá ser objeto de revisión continua, como también los planes específicos y sectoriales que de ella se deriven. Se elaborará un informe anual de evaluación de la Estrategia donde figurará el grado de ejecución y cumplimiento de sus objetivos.

Por otro lado, a la vista del incremento de las amenazas y desafíos a la ciberseguridad y cómo los afrontan países de nuestro entorno, resulta cada vez más urgente dotarse de recursos económicos, humanos y materiales para hacer frente a los mismos. Una de las acciones especialmente relevantes en este marco es que el Centro de Operaciones de Ciberseguridad de la Administración General del Estado se encuentre adecuadamente dotado.

El Estado necesita una transición de un modelo de ciberseguridad de carácter preventivo y defensivo hacia un esquema que incorpore

elementos de mayor fuerza disuasoria que obedecen a un contexto global de mayor competencia geopolítica. El empleo del quinto dominio como mando de confrontación, de forma independiente o como parte de una acción híbrida, es un rasgo ampliamente reconocido. La disuasión en ciberseguridad requiere la obtención y potenciación de capacidades de ciberdefensa, como elemento fundamental de la acción del Estado.

De esta forma, debido la rápida evolución de las ciberamenazas se debe tener una aproximación más proactiva de la ciberinteligencia. Su integración en el esquema conjunto de la ciberseguridad es un elemento clave para el conocimiento de la situación y la necesaria alerta temprana que permita anticiparse a las acciones de los potenciales adversarios a través del conocimiento de sus capacidades, técnicas, tácticas e intenciones (Gobierno de España, 2019).

Por lo tanto, es necesario fomentar el empleo de mecanismos y medios que permitan una oportuna investigación y persecución de los autores para incrementar las posibilidades de atribución. A todo lo anterior se une la necesidad de una mayor implicación de toda la sociedad mediante el fomento de una cultura de ciberseguridad, para evolucionar desde la concienciación al compromiso, en el entendimiento de que el ciudadano es corresponsable de la ciberseguridad nacional.

No obstante, Colombia debe promover un ciberespacio abierto, plural, seguro y confiable tanto en sus relaciones bilaterales como en las organizaciones multilaterales, regionales e internacionales, y en los foros y conferencias, donde la ciberseguridad ocupa un lugar destacado y de esta manera abogar por la creación de un marco internacional para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, en el que se apliquen los principios de La Carta de Naciones Unidas en su totalidad, el Derecho Internacional, los Derechos Humanos y el Derecho Humanitario Bélico, así como las normas no vinculantes sobre el comportamiento responsable de los Estados.

Consciente de la importancia del multilateralismo, se considera relevante el papel de Naciones Unidas para avanzar en la construcción de consensos que, junto a la adopción y puesta en marcha de medidas de fomento de la confianza, la colaboración y participación de todos los

actores implicados (Estados, sector privado, sociedad civil, usuarios y academia), constituyen la base para lograr seguridad y estabilidad en el ciberespacio y avanzar hacia su regulación.

Conclusiones

El resultado del estudio arroja la enorme importancia que debe dar el Estado de Colombia al quinto dominio, tener la capacidad de adaptarse al nuevo entorno que se vive hoy en el siglo XXI, si quiere prolongarse en el tiempo debe importarle. Se aproxima la segunda década y el desafío de controlar los estados alrededor del mundo desde todos sus dominios es mayor, las modernas ofensivas serán numerosas y la vulnerabilidad será a gran escala. El pasado demostró que los niveles de poder coexisten entre sí, pero que la naturaleza de la guerra los cambia, transforma, crea, a consecuencia de la astucia e inteligencia humana.

La necesidad de controlar el Estado colombiano debe ser prologarse en el tiempo y generar una estrategia que le de prospectiva a su intensión, de esta manera debe cuidar los recursos, expedirse en busca de nuevos territorios que proporcionen a los ciudadanos mayor supervivencia y ser reconocido en el orden mundial como potencia, garantizando contrarrestar los enemigos tanto internos como externos a través de la seguridad que proporciona a la vez desarrollo económico, religioso, cultural, político, de innovación y emprendimiento, es decir abarcando aspectos multidimensionales que le permitan existir.

El quinto dominio es entonces adaptar la geopolítica tradicional a la moderna, es proporcionarle a Colombia nuevas herramientas que le permita entender que el interés nacional abarca la existencia de su estado por sí mismo y que todo lo que se desprenda de ello será el resultado de haber entendido la importancia de su origen y de haber puesto en marcha sus capacidades de dominio.

La posición geográfica que tiene Colombia es ventajosa en todos sus niveles poder, en comparación con los Estados vecinos y del mundo, tener dominado el ciberespacio como nuevo elemento geopolítico es

permitirle a Colombia dejar el pasado de una nación tercermundista y potencializarla a través de cada uno de sus ciudadanos por medio de Internet, los celulares, la inteligencia artificial, plataformas, drones, censores, laboratorios y todas las áreas multidisiciplinas.

No puede seguir concibiendo el ciudadano normal, que el quinto dominio es solo para los ingenieros de sistemas o los ciber-soldados pertenecientes al ciber-comando conjunto colombiano, concientizar a cada persona es parte de la estratégica y de los modos innovadores, España por su parte brinda elementos diferenciadores geopolíticos, que quizás aunque no son motivo de este estudio y en principio parecen polémicos, inspiran a que sean aplicados en Colombia; los ciudadanos, sus libertades y su privacidad son parte del interés nacional; su información está por debajo primando siempre la existencia del Estado, de ahí que detectar amenazas y saber cómo y cuándo proceder o a que fuerza acudir, despertará y exacerbará el nacionalismo que a Colombia tanto le hace falta, mientras que cada uno de sus ciudadanos comprenda y se involucre en el quinto dominio ya sea como cibernauta, como empresa o como amenaza.

Potencializar los emprendedores que salgan a someter el mundo a través del quinto dominio es expansión en simultaneo, incentivarlos es una obligación por parte del Estado, es desarrollo en otro nivel, es aumentar las capacidades de dominio desde la ciberdefensa y ciberseguridad para accedan y se expongan al mundo con la tranquilidad que su ciberfuerza los custodia, llegar a otros territorios por parte de empresarios que si entienden la dinámica intangible del nuevo concepto de comercio, permite diferenciar dos modos ya nombrados, una ciberfuerza, independiente a las tres tradicionales y incentivos económicos a empresarios con necesidad expansiva (evaluando a millones de empresas que busquen mercados y generen expansión en el quinto nivel).

Sin embargo, tener políticas defensivas actualmente solo ha demostrado que perdamos territorio tanto terrestre como marítimo, la necesidad de crear el modo de ofensiva es inminente para lograr expansión a otros lugares, ya que todos los territorios pueden ser invadidos en simultaneo, ofensivas disfrazadas de legalidad que permitan ir tras nuestros

intereses. El ciber comando conjunto es solo un piloto de dominar el quinto dominio desde todos sus ángulos y su política es netamente defensiva, su labor y estructura es impecable al detectar, frenar, identificar, reaccionar frente a las amenazas.

China, proporciona al estudio su Intranet, si bien es cierto que el quinto dominio transformó el concepto de fronteras, China demuestra que las ciber fronteras son posibles y que la Intranet permite el control de visitantes al estado colombiano desde este nuevo aspecto geopolítico, todas las convergencias delictivas, como las transacciones, delincuencia transnacional, o violaciones a la soberanía como se evidencia cuando llegó UBER a modo ejemplo, requieren la atención del control de quién entra y quién sale, y qué efectos ocasiona la entrada de personas o empresas al territorio en este nivel de poder. Lo que lograría sería tener mucha más capacidad de dominio y de adaptabilidad de las normas legales a las costumbres modernas, posibilidad de detección temprana de alarmas y tipificar delitos teniendo absoluto control para poder judicializar en caso de violaciones a las normas del quinto dominio y el libre tránsito dentro de la Intranet.

El riesgo de no entender y no crear una estrategia de dominio en el quinto nivel es repetir el pasado magnificándolo a los tiempos modernos; dejar el espacio vacío es, sin duda, no entender que hay un nuevo escenario geoestratégico que se debe controlar y dominar; es arriesgar a Colombia y sus próximas generaciones a la merced de Estados que sí comprendieron la necesidad de entenderlo y del acceso que tiene cualquier ciudadano del mundo. Subestimar a cualquier persona en pijama desde su casa, es un riesgo como también es un riesgo no educar la población en prospectiva y proyectar el estado entero. La amenaza del enemigo siempre estará a la orden del día cada vez es más difícil detectarla si el quinto dominio no se tiene como prioridad, por tanto, es hoy y no mañana que el Estado de Colombia debe adaptarse y tomar en serio conceptos como geoestrategia, geopolítica; entendiendo que no es solo seguridad y defensa nacional o ciberseguridad, que el quinto dominio es geopolítica y la estratégia está planteada.