Capítulo 2

Desafíos en la búsqueda de un liderazgo sostenible en el ciberespacio y el sistema internacional

DOI: https://doi.org/10.25062/9786287602526.02

Milena Elizabeth Realpe Díaz
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: En el presente capítulo se realiza un estudio en el que se evidencian las dificultades existentes para establecer un liderazgo claro y contundente tanto en el ciberespacio como en el sistema internacional, apelando a la *teoría del realismo de la disciplina de las relaciones internacionales* y al estudio de las amenazas y las nuevas formas de conflicto. Ciertamente, la conjunción de intereses económicos, políticos y geoestratégicos ha marcado las dinámicas en diversas dimensiones a escala nacional, regional e internacional, por lo que se observará cómo ello impide que, eventualmente, algunos acumulen recursos de poder en lapsos definidos, pero sin llegar a establecerse de forma genuina un proceso de liderazgo. Finalmente, se aborda cómo el ciberespacio es analizado como el escenario preferido de las nuevas formas de conflicto, y como el poder ciberespacial no se circunscribe al uso exclusivo de las Fuerzas Militares de una nación, sino que esta lo puede ejercer, un gran número de actores con la capacidad técnica y humana para su propia conveniencia en el dominio cibernético, ello podría obligar a los Estados a repensar el diseño de sus estrategias de seguridad y defensa nacionales.

Palabras clave: liderazgo, ciberespacio, amenazas, sistema internacional.

Milena Elizabeth Realpe Díaz
Teniente Coronel, Ejército Nacional de Colombia. Doctoranda, Estudios Estratégicos, Seguridad y Defensa, Escuela Superior de Guerra "General Rafael Reyes Prieto". Magíster, Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra. Magíster, Seguridad de la Información, Universidad de los Andes. Especialista, Seguridad de Redes de Computadores, Universidad Católica de Colombia, Especialista, Seguridad Física y de la Informática, Escuela de Comunicaciones del Ejército y Especialista, Seguridad de la Información, Universidad de los Andes. Ingeniera de Sistemas, Universidad Cooperativa de Colombia.
https://orcid.org/0000-0003-4345-6182 - Contacto: **milena.realpe@esdeg.edu.co**

Citación APA: Realpe Díaz, M. E. (2023). Desafíos en la búsqueda de un liderazgo sostenible en el ciberespacio y el sistema internacional. En S. Uribe-Cáceres & D. López Niño (Eds.), *Aproximación teórica a las nociones de la guerra y el liderazgo estratégico* (pp. 41-62). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602526.02

APROXIMACIÓN TEÓRICA A LAS NOCIONES DE LA GUERRA Y EL LIDERAZGO ESTRATÉGICO
ISBN impreso: 978-628-7602-51-9
ISBN digital: 978-628-7602-52-6
DOI: https://doi.org/10.25062/9786287602526

Colección Seguridad y Defensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes prieto"
Bogotá D.C., Colombia
2023

Introducción

Los cambios tecnológicos que han acompañado la evolución humana han sido, precisamente, la base para dar saltos que han llevado a la transformación del cuerpo humano, de su entorno y de las herramientas que la especie utiliza para facilitar su vida, maximizar los recursos de poder y generar cambios sociales, políticos y culturales que se amoldan a dichas transformaciones tecnológicas, y por lo cual se entra a lo que algunos han denominado el *posthumanismo*.

> Se puede entender que la condición posthumana se configura bajo la tensión entre la definición de los límites ontológicos de lo 'humano', lo 'animal' o lo 'artificial' y una política de emancipación que busca darle un sentido político a estas transformaciones. Esto significa vislumbrar el potencial tecnológico a partir del momento histórico 'singular' en que la configuración, a modo de 'enhancing', de nuestras características bío, psico y fisiológicas, nos permitirá, como especie, moldear un futuro proyectado, tanto para nuestra longevidad y nuestras aptitudes físico-cognitivas. (Cornejo, 2017, p. 222)

Si bien el eje central de la presente disertación no es una reflexión bioética, sí es necesario contextualizar que la tecnología tiene en la actualidad injerencia incluso en la biología, a través de la biotecnología, lo que se traduce en un inigualable poder para transformar la vida misma y crear nuevos mundos, diseñados en detalle según la conveniencia del gestor. Exactamente ello se aproxima a lo que hoy por hoy ha ganado popularidad: el *metaverso.*

Lo que antes parecía una idea de ciencia ficción, en la que la imaginación del autor William Gibson parecía romper todo límite, es hoy una realidad. En 1984 la publicación de la novela *Neuromante* dio los primeros atisbos de lo que hoy se conoce como ciberespacio relatando la vida de un *cibervaquero,* que en su tiempo

parecía inconcebible, pero en la actualidad cobra sentido y centra la atención de las grandes empresas tecnológicas, al abrir la posibilidad de vivir en un contexto diferente.

> La experiencia de máxima customización llegará muy probablemente en el metaverso, que podemos traducir como un espacio en creación 'más allá del universo'. Se trata de la próxima parada tecnológica, resultante de la mezcla de realidad virtual, redes sociales, videojuegos e internet de máxima velocidad. Ese mundo paralelo, digamos que, en otra dimensión, nos ofrecerá la posibilidad de ser quienes de verdad queremos ser, sin límites incluso para la Física. Hablamos de una hipótesis, por supuesto, de algo futurible, de uno de esos proyectos tecnológicos que vemos en el horizonte… Pero de momento Mark Zuckerberg ya ha anunciado la contratación de 10.000 personas para dar vida a ese metaverso. (Bueno, 2021, p. 6)

En este sentido, se hace necesario examinar qué sucede con las formas sociales que han tomado la forma de los Estados nación en las que se organiza la humanidad en la actualidad, así como en organizaciones intergubernamentales, organizaciones no gubernamentales (ONG), empresas transnacionales y grupos armados, que son los actores principales del sistema internacional tradicional.

Así, al iniciar el estudio de estos actores, los autores clásicos, como Thomas Hobbes o John Locke, hacían un símil entre la condición natural del hombre y el comportamiento de los Estados. En tal sentido, el primero, desde una visión pesimista en términos antropológicos, indicaba que los Estados, así como el humano en estado de naturaleza, solo propenderían por su beneficio, pues son egoístas e individualistas (Aparicio, 2018). Allí reside la génesis de una de las teorías clásicas de la disciplina de las relaciones internacionales, que compondrá el marco teórico del presente escrito, al relatar con exactitud que, tanto en el sistema internacional tradicional —que se forjó desde 1648, con la Paz de Westfalia— como en el quinto dominio y en la posibilidad de vivir una realidad alterna en el metaverso, hay claras limitantes para consolidar el liderazgo de un solo actor o el de un grupo de estos.

Las dinámicas inherentes a la condición humana han llevado a forjar estrategias para concentrar poder y riquezas, y las cuales son susceptibles a la emergencia de las innovaciones tecnológicas. Es decir, si bien las revoluciones industriales han sido gestadas desde el propósito de evolucionar —especialmente, en el ámbito de los procesos productivos—, a la postre se han convertido en excelsas herramientas para la acumulación de recursos de poder. Su ambigüedad reside,

precisamente, en la interpretación y el uso que le dan las personas y las organizaciones a la tecnología, que, por un lado, puede ser una oportunidad para mejorar sustancialmente la calidad de vida, pero, por otro, puede marcar la mutación de una serie de amenazas que se hacen presentes en el ahora tan popular ciberespacio.

Es así como desde el acercamiento a las cualidades y las características de un líder y el estudio comparado del sistema internacional y del ciberespacio, se procurará evidenciar que estos contextos, si bien cuentan con líderes visibles en el interior de las unidades, no facilitan la consolidación de un líder que persuada a los demás a seguir un camino determinado, imponga orden y garantice, como podría suceder en un plano físico tradicional, la protección de derechos o de una normativa específica.

El autor destacado y líder en materia cibernética y conflictos en el ciberespacio es el coronel Crowther, quien, mediante la construcción de conocimiento, evidencia sus creencias sobre la comprensión del ciberespacio como un dominio de guerra que impacta notablemente en la revolución de los asuntos militares en las realidades digitales. Dichas creencias se encuentran basadas en estudiar y explicar el ciberespacio, su conformación, el dominio cibernético, las operaciones militares en el ciberespacio y el arte de la guerra en un mundo moderno, entre otros, todo lo cual demuestra que este quinto dominio, a diferencia de los dominios tradicionales de tierra, mar, aire y espacio, es un ambiente virtual creado por el hombre, quien, por tanto, tiene la posibilidad de liderarlo, transformarlo y expandirlo.

En consecuencia, el ciberespacio, por naturaleza, no es un espacio seguro ni protegido: de hecho, en él se ha incrementado de manera exponencial la superficie de ataque y, por tanto, es vulnerable a las amenazas o los ataques cibernéticos latentes o emergentes, lo que puede resultar en pérdidas significativas para los sectores económico, político, y social o constituir una seria amenaza para la defensa o los intereses nacionales. Por esto, el ciberespacio es analizado como el escenario preferido de las nuevas formas de conflicto, como es el caso de los conflictos híbridos (Luque, 2019) y como un dominio en, desde y a través del cual las operaciones militares crean efectos previstos y donde los objetivos militares fundamentales relativos a este dominio son esencialmente los mismos que en los otros dominios, y el objetivo principal es la libertad de acción en, a través y desde el ciberespacio, según como sea necesario para apoyar los objetivos de la misión.

Finalmente, se aborda la complejidad del poder ciberespacial considerando que este no se circunscribe al uso de las FF. AA. de una nación, sino que lo puede acceder un gran número de actores con la capacidad técnica. En el contexto

descrito, el desarrollo de capacidades en el ciberespacio se constituye en una prioridad estatal, la cual presume un rediseño de las estrategias de seguridad y defensa nacional. Este nuevo escenario se sirve como un medio y un fin en sí mismo, para alcanzar la modificación, mantenimiento o expansión del *statu quo* de los Estados y actores que, por excelencia, han dominado la agenda internacional.

Metodología

Desde un análisis cualitativo con el diseño de la teoría fundamentada, en la primera parte se hará un encuadre conceptual para contextualizar los ejes transversales de este trabajo: ciberespacio, sistema internacional y metaverso, entre otros. Posteriormente, desde una aproximación teórica se marcará la pauta para el análisis de la plausibilidad de una dinámica de liderazgo en estos espacios, de modo tal que, para finalizar, pueda examinarse hacia dónde se dirigen los actores primordiales a fin de garantizar su liderazgo en sus entornos inmediatos.

Se escoge específicamente el diseño de la *teoría fundamentada,* pues "el investigador produce una explicación general" (Hernández, 2014, p. 93) de un fenómeno, que se aplica a un contexto particular en el que se relacionan diversos aspectos.

De este modo, al usar diversas variables en el presente escrito, se busca hallar una relación entre ellas que permita explicar el fenómeno que se está presentando, para lo cual se usa de base una *teoría de la disciplina de relaciones internacionales,* a falta de una explícita que trate el fenómeno propuesto, dada su novedad.

Contexto general del ciberespacio y del sistema internacional

Como ya se advertía, fue en una novela de 1984 en la que se dio la primera aproximación a ese espacio que se abría en la virtualidad, y que se consolidó como el precedente por excelencia cuando se habla de ciberespacio.

> Fue el escritor de ciencia ficción (ciberficción) William Gibson (1948) quien creó el concepto de ciberespacio en su novela Neuromante (1984) para designar el escenario espacial que existía al interior de las computadoras y sus interconexiones, y que ahora define el espacio antropológico de la red informática en donde todos los usuarios de la red informática al ingresar al

> ciberespacio nos convertimos en cibernautas, y que a su vez conformamos la cibersociedad, caracterizada por sus formas alternativas de socialización para la apropiación social de las TIC, es así que el Ciberespacio es un elemento definidor del espacio virtual de relación entre los usuarios de Internet y de otras redes telemáticas o de computadoras. (Martínez et al., 2014, p. 45)

Ciertamente, resulta complejo encontrar una definición única y completa; empero, la ya suministrada reúne dos aspectos primordiales: lo técnico y lo antropológico. Si bien en un inicio se podría percibir que solo se trata de una dimensión netamente tecnológica, el hecho de que sea finalmente operado por humanos amerita la revisión desde la antropología, la sociología, etc. Justamente, al integrarse estos aspectos es cuando se debe revisar cómo se genera un liderazgo efectivo en el ámbito, entendiendo que las esferas de la vida se entremezclan; más aún, cuando las nuevas generaciones no conocen otro modo de interactuar que no sea a través de las herramientas allí dispuestas, y cuando cada vez convergen más escenarios, que usualmente eran *físicos,* a este plano *virtual,* en las que las relaciones entre Estados, líderes mundiales y organizaciones internacionales encuentran oportunidades y amenazas.

> Nuestro espacio privado y nuestro espacio público interactúan con el ciberespacio y sus servicios, con o sin nuestra autorización o conocimiento. Por eso, aunque no sea perceptible por nuestros sentidos, es real al ser un producto del desarrollo de las telecomunicaciones, de la informática, de la interactividad y del mensaje multimedia: 'La única forma de 'ver' el ciberespacio es mediante una 'realidad virtual', una 'realidad artificial' construida por el hombre'. (Pérez, 2013, p. 2)

En esa construcción, intencionalmente o no, se han dejado espacios que pueden ser cooptados por quienes indiscriminadamente buscan lucro, poder o la inestabilidad y consecuente caída de su contrario. Ello es posible dada la migración de los procesos hacia dicho entorno digital, lo que genera beneficios, pero también, vulnerabilidades; en especial, en lo concerniente a la infraestructura crítica cibernética.

De conformidad con el CONPES 3854 de 2016, la *infraestructura crítica cibernética* es la soportada por las tecnologías de la información y las telecomunicaciones (TIC), y de cuyo funcionamiento depende que el Estado pueda garantizar sus fines esenciales y la prestación de servicios a todos los ciudadanos. Si llegara a presentarse una falla en alguna de las plataformas digitales dispuestas para tal fin, se vería gravemente afectada la estabilidad económica, así como el funcionamiento

de las instituciones y el de la administración pública; incluso, dependiendo del alcance de la afectación, podría gestarse un ambiente de incertidumbre y caos.

Estos escenarios son previstos a escala nacional e internacional, pues actores internos o externos pueden provocar tales efectos, dependiendo de los intereses que busquen recabar. Es por ello por lo que resulta plausible que, en el contexto de actores poderosos, como los Estados, se haga un símil con el sistema internacional, entendiendo que la interdependencia y la globalización son dos preceptos que hacen que todo tenga alguna conexión y correlación; en especial, si atañe a lo público.

Así, Frederic Pearson y Martin Rochester (2003) se refieren al sistema internacional como ese patrón general que define las relaciones políticas, sociales, económicas, tecnológicas y geográficas que configuran la agenda mundial o, como ellos también lo simplifican, "el escenario general en que ocurren las relaciones internacionales en un momento dado" (p. 37).

En este sentido, hoy por hoy esas interacciones a través de las fronteras se están dando en un momento en el que no es necesario tomar un avión para asistir a una cumbre presidencial, sino que las plataformas tecnológicas permiten conexiones en tiempo real; especialmente, después de la pandemia. Asimismo, no es necesario disparar un misil ni movilizar tropas para que un conflicto explote o escale, sino que, desde un ataque a la infraestructura crítica cibernética, pueden ocasionarse consecuencias aún más nefastas que las de un enfrentamiento de trincheras.

Ahora bien, cabe preguntarse quiénes tienen el control de esos dos espacios: el ciberespacio y el sistema internacional. Cabe preguntarse quién lidera y por qué. Esto, siguiendo a Hoojberg et al. (1997), quienes establecen que hay tres ejes de complejidad en el liderazgo: el *cognitivo,* el *social* y el *conductual.* Por ello, para responder a los cuestionamientos planteados se abordará, entre otras cuestiones, cómo, desde el conocimiento, la regulación de las interacciones y el control de los comportamientos de quienes interactúan en el ciberespacio, se puede pensar en la consolidación de un líder.

Realismo: la explicación y prescripción de un mundo particular

Si bien las interacciones entre las unidades y diversas formas de organización humana se han estudiado desde tiempos antiquísimos, fue con las guerras mundiales cuando surgieron los estudios formales que buscaban no solo entender qué

había ocasionado tal desastre, sino prevenir y prever el posible estallido de una nueva conflagración de tal nivel. Fue así como en 1919, en Gales, se creó la primera Facultad de Relaciones Internacionales y se inició el estudio riguroso de las interacciones entre los Estados (Frasson-Quenoz, 2014).

Con el fin de la Primera Guerra Mundial, se pensaba que las probabilidades de una segunda guerra del mismo tipo eran, por demás, nulas, al haberse presenciado la pérdida extraordinaria de vidas humanas, infraestructura y recursos económicos. Por ello, el liberalismo surgió como la otra teoría clásica que insistía en la capacidad de paz del hombre y en la cooperación como las mejores herramientas, no solo para reconstruir a Europa tras la guerra, sino como base para la interacción de los actores y, esencialmente, los Estados.

Sin embargo, se desencadenaron incidentes relacionados con los intereses expansionistas de los alemanes, los italianos y los japoneses (Venatici, 1978), que evidenciaron cómo el idioma del trabajo mancomunado no estaba siendo interpretado por todos desde la misma perspectiva. Fue entonces cuando el Realismo, como paradigma clásico, tomó el control de la explicación y prescripción de lo que sucedía en el sistema internacional, no solo hacia fines de la década de 1930, sino a lo largo de una historia que evidencia la actuación individualista y beligerante de algunos países.

En tal contexto, en el estudio de las relaciones internacionales como disciplina científica, toman fuerza los principios propuestos por Hans Joachim Morgenthau. En primer lugar, este autor clásico prescribe una teoría de política internacional con capacidad explicativa y prescriptiva, pues, para él, el realismo no puede tratarse solamente de explicar el mundo, sino que también debe generar líneas de comportamiento idóneo para los gobernantes (Frasson-Quenoz, 2014).

De igual modo, identifica que la motivación de los actores, de los políticos, es el interés en términos de poder, que es el elemento esencial de la política en general. Asimismo, reflexiona sobre la moralidad y la política entendiendo que los valores morales pueden ser incompatibles con las necesidades, por lo que, en últimas, se les dará prioridad a estas.

Una de las premisas de mayor importancia en este autor fue que el sistema internacional es anárquico y competitivo, y fundaba su análisis en una naturaleza humana esencialmente pesimista. El egoísmo y el instinto de dominación son lo que puede describir el sistema internacional como lo que es, y no como debería ser, que es la principal crítica de este autor al liberalismo clásico (Frasson-Quenoz, 2014).

En este orden de ideas, esa naturaleza anárquica del sistema, como idea central del Realismo, es la clave para comprender las limitaciones existentes a la hora

de establecer liderazgos claros; además, a diferencia de un Estado que posee el monopolio del uso de la fuerza porque todos los ciudadanos concuerdan en ceder parte de sus derechos y libertades para obtener el bien mayor de la protección y la salvaguarda de sus intereses primarios, en la arena internacional no sucede así.

Si bien los otros enfoques teóricos han resaltado, a través de ejemplos históricos, la funcionalidad de la cooperación y de las instituciones internacionales, entre otros, no es posible omitir que las relaciones potencialmente violentas también han transformado de manera profunda al sistema internacional. Las guerras mundiales y conflictos como los devenidos con la disolución de Yugoslavia y la Unión Soviética, etc., dan cuenta de cómo los intereses particulares de cada Estado priman por sobre la posibilidad de establecer relaciones de líder y seguidores, pues de este modo no se tendría control de los recursos ni posibilidades de conquistar una determinada meta.

Así, antes que, entre todos, construir un camino que lleve al bienestar general de los humanos, cada uno, desde su propia perspectiva, cultura, religión, historia y objetivos, da pasos hacia lo que ha prescrito para sí, incluso si ello implica el debilitamiento o la eliminación del otro. De la misma forma, es necesario tener en cuenta que, progresivamente, los Estados ya no son los únicos actores con capacidad de actuación, sino que las organizaciones intergubernamentales, las ONG, las empresas transnacionales y los grupos armados han sido los que han protagonizado varios de los fenómenos recientes.

Especialmente desde la ilegalidad, hay grupos armados que han adquirido capacidades extraordinarias para desestabilizar naciones enteras. Es por ello por lo que en el acápite siguiente se hará una aproximación a todas las amenazas que desde el ciberespacio emergen y se fortalecen por asuntos inherentes a la incapacidad para identificar plenamente a los actores, la posibilidad de desarrollo de tácticas y estrategias variadas e innovadoras y las fallas propias de un sistema creado por humanos.

Amenazas cibernéticas en un mundo hiperconectado

El secretario general de las Naciones Unidas advirtió que "la guerra cibernética se había convertido en una amenaza de primer orden para la paz y la seguridad internacionales y que, los ataques cibernéticos masivos bien podrían convertirse en el

primer paso de la próxima gran guerra" (ONU, 2018). Sin embargo, existe un acuerdo generalizado entre los países firmantes de la Carta de las Naciones Unidas, cuyos preceptos se aplican en su totalidad a las TIC, junto con la obligación por parte de los Estados, de resolver las disputas por medios pacíficos. De ahí que el comportamiento de los Estados en el ciberespacio, en relación con el mantenimiento de la paz y la seguridad internacionales, esté pasando a ocupar un sitio destacado en la agenda internacional (OEWG, 2021).

La consolidación del ciberespacio como una temática que se ha convertido en tendencia general para la mayoría de los países del mundo ha venido desencadenando la expansión de la nueva superficie de ataque para el espectro de seguridad nacional. Esto, como consecuencia de que cuanto mayor sea la intensidad de la actuación de los humanos en el ciberespacio, mayor será el potencial para una eventual provocación de los conflictos en el ciberespacio. Esta amenaza no se limita a la ciberseguridad nacional, sino que también tendrá un impacto en la seguridad y defensa de los Estados. En tal contexto, es preciso mencionar que el dominio del ciberespacio fue una carrera iniciada por las grandes potencias, como Rusia, Estados Unidos y China, y es por ello por lo que son un punto de referencia para la creación de instrumentos que salvaguarden la seguridad y defensa nacional en el ciberespacio (Gaitán, 2018).

En la actualidad, el ciberespacio se configura como un dominio artificial creado y modificado por el hombre, en el cual no existe la perfección absoluta y, en consecuencia, se sirve como un mundo paralelo en el que pueden desenvolverse los humanos. De tal forma, todas las actividades humanas que se realizan en el mundo real también son realizables en el ciberespacio, con sus aciertos y desaciertos, sus acuerdos y desacuerdos e, incluso, las múltiples fricciones y controversias que surgen de la diaria convivencia en sociedad, todo lo cual ocasiona relaciones de enemistad que podrían confluir en la consolidación de amenazas o ataques en o a través del ciberespacio o, en el peor de los casos, en conflictos o guerras de tipo cibernético. Las amenazas en el ciberespacio se clasifican como amenazas reales, por lo que enfrentarlas requiere una estrategia de defensa eficaz y con alta capacidad de disuasión (Nur, 2022). Sin lugar a duda, si se observa más allá de la falta de consecuencias físicas, los ataques cibernéticos pueden causar un daño enorme al socavar la cohesión social y la confianza en las instituciones gubernamentales, dado el crecimiento constante de la convergencia tecnológica, la velocidad de trasmisión y el empoderamiento del individuo dentro del dominio cibernético. De acuerdo con el reporte presentado por la UNESCO respecto al Foro de la Cumbre Mundial sobre la Sociedad de la Información 2021, se establece que

> Las sociedades se han transformado gracias a las tecnologías de la información y la comunicación de una forma que no podía ni imaginarse hace una década y media. En muchos casos, estas tecnologías han cumplido su promesa de desarrollo y de ampliación espectacular de la inclusión y la participación en la sociedad. Sin embargo, ha aumentado la conciencia de nuevos riesgos, como la desinformación y el discurso de odio, la vigilancia digital, la privacidad de los datos y, ahora, el auge de la inteligencia artificial, todo lo cual tiene importantes implicaciones para los derechos humanos y las libertades fundamentales. (UNESCO, 2021)[1]

El futuro de los conflictos digitales en la geopolítica tendrá amplias implicaciones para los actores públicos y privados y para la sociedad civil. Por esto, en Colombia, desde 2011, se ha venido hablando de la importancia de una estrecha cooperación no solo en el ámbito nacional, con la participación de las múltiples partes interesadas[2], sino en el plano internacional, lo cual será imprescindible, pero no suficiente, a fin de prevenir y resolver futuros conflictos geopolíticos digitales. La construcción de las relaciones políticas, sociales, económicas e incluso militares en este mundo hiperconectado no solo requiere hacer uso de los medios tradicionales, sino que obligará también a acudir a las herramientas y medios que ofrece el ciberespacio, de manera que permitan adaptarse a la nueva realidad digital.

Nuevas formas de conflicto

La existencia de un mundo paralelo en forma de metaverso desencadenará una expansión del espectro de seguridad, dadas las condiciones de anonimidad y clandestinidad que permiten actuar con libertad y, en ocasiones, evadiendo las leyes y normas. Para hacer frente a estas amenazas, además de la cooperación, se hace necesario construir una estrategia de defensa del país para la sociedad en general, además de seguir fortaleciendo las capacidades de ciberseguridad y ciberresiliencia del país.

En lo que atañe a Colombia, mediante el documento de política pública CONPES 3701 de 2011 se estableció que la defensa nacional estaría a cargo de las

---

1 En primera instancia, los efectos de los conflictos o ataques en el ciberespacio no tienen una percepción en la dimensión física, no obstante, en la escalada del conflicto sí se pueden apreciar afectos cuando se impacta la infraestructura crítica cibernética, teniendo efectos en la supervivencia física de las personas.

2 Múltiples Partes Interesadas: cinco actores: Gobierno, Empresa Pública y Privada, Fuerza Pública, Academia y Sociedad Civil. (CONPES 3854, 2016).

FF. MM. y, en particular, del Comando Conjunto Cibernético (CCOCI), basándose en los postulados según los cuales para la defensa nacional se debe involucrar a las múltiples partes interesadas: las entidades de gobierno territorial, empresas públicas y privadas, la Fuerza Pública, propietarios y operadores de infraestructura crítica, la academia y la sociedad civil, haciendo uso de tecnologías modernas y de procesos adecuados, pero, sobre todo, bajo el liderazgo de personas capaces de transformar la cotidianidad innovando bajo las nuevas condiciones de una actualidad digital para hacer propuestas que revolucionen el devenir en el ciberespacio.

Este es el caso del coronel Crowther, quién, mediante la construcción de conocimiento, evidencia sus creencias sobre el componente cibernético, lo que cada vez adquiere más fuerza y se convierte en un referente cuando se trata de influir en las personas a través del conocimiento, y la academia, e incluso, en la trasformación de los asuntos militares, por medio de temas relacionados con ciberseguridad y ciberdefensa. Sus creencias se basan en estudiar y explicar el ciberespacio, su conformación, el dominio cibernético, las operaciones militares en el ciberespacio y el arte de la guerra en un mundo moderno, entre otros, demostrando que el dominio cibernético, a diferencia de los dominios tradicionales de tierra, mar, aire y espacio, es un ambiente virtual creado por el hombre y, por tanto, brinda la posibilidad de liderarlo, transformarlo y expandirlo.

En consecuencia, una variable fundamental en este nuevo escenario es el ser humano, quien interactúa a través de su identidad real o de múltiples identidades digitales. Crowther (2017) establece que el ciberespacio tiene tres capas: una *red física*, que está enmarcada en el *hardware;* una *red lógica,* consistente en el *software* que hace operable la red, y una *ciberpersona,* la cual son los humanos que están liderando y operando en el ciberespacio con su identidad real y sus múltiples identidades digitales. Bajo este concepto, tanto la capa física como la de personas existen dentro de los Estados y, por lo tanto, se hallan sujetas a sus leyes y políticas. Eso permite sentar unas bases para comprender la nueva realidad. El elemento humano es una parte fundamental del dominio cibernético que no puede ni debe ser ignorada. Debido a que los humanos construyeron la arquitectura cibernética, esta se presume inherentemente imperfecta. Bajo sus preceptos, el imperativo fundamental para madurar la comprensión del ciberespacio es tratarlo como un lugar, y no solo como una misión. Es decir, el ciberespacio es un dominio en, desde y a través del cual las operaciones militares crean efectos previstos. De igual forma, los objetivos militares fundamentales relativos a dicho dominio son esencialmente los mismos que en los otros dominios, y el objetivo principal es la

libertad de acción en, a través y desde el ciberespacio, según como sea necesario para apoyar los objetivos de la misión.

El resultado es negar la libertad de acción a los adversarios en los momentos y lugares de nuestra elección. La capacidad para hacer ambas cosas proporciona superioridad militar cibernética (USAFT, 2011). Así las cosas, el coronel Crowther, líder estudiado en este análisis, ha sido capaz de abordar diferentes tipos de público, con edades y razas diferentes impactando contundentemente en los cambios en temas asociados al dominio cibernético. Este tipo de liderazgo es definido muy bien por Yulh (2010) cuando establece que el liderazgo es el "proceso de influir en otros para entender y estar de acuerdo sobre lo que hay que hacer y cómo hacerlo, y el proceso de facilitación de los esfuerzos individuales y colectivos para lograr objetivos comunes" (p. 8).

El mundo actual, marcado por la Cuarta Revolución Industrial, requiere contar con líderes VUCAH (por las iniciales en inglés de *Volatile, Uncertain, Complex, Ambiguous and Hyperconnected* [volátil, incierto, complejo, ambiguo y, ahora, hiperconectado]) para enfrentar un escenario caracterizado por la inestabilidad. El ciberespacio exige a los líderes enfrentarse a cambios inesperados, impredecibles y en ocasiones turbulentos, donde cada uno hace parte integral del propio contexto de cambio, en el que cabe incluir la perspectiva teórica del Realismo, para poder explicar y prever las posibles actuaciones de quienes, racionalmente, perseguirán sus intereses particulares en términos de poder, incluso si ello implica disminuir las capacidades de un par.

En este ambiente, un líder contemporáneo requiere actuar de manera diferente de la de un líder tradicional: el rol de un líder moderno exige convertirse en agentes de cambio exitosos, con una amplia capacidad para adaptare a las transformaciones continuas y los cambios disruptivos, con el conocimiento adecuado para hacer frente a la incertidumbre, con capacidad para responder a los cambios y recuperarse a su estado normal, pese a cualquier situación. Es decir, con capacidad de resiliencia para no dar campo a la ambigüedad; con la habilidad de comunicar con claridad y sencillez para combatir la complejidad y, sin lugar a duda, con la suficiente capacidad emocional para manejar las nuevas generaciones de alfas, *millenials* y *centenials* (IBERDROLA, 2022), que se encuentran altamente influenciadas por todo lo que experimentan, ven, escuchan y lo que creen que es verdad; es decir, sus propias creencias, con el sesgo propiciado por la explosión de información, no necesariamente cierta.

Si bien en los liderazgos tradicionales el uso de símbolos no siempre es tan evidente y llamativo, al hablar de liderazgo complejo este tipo de identidades se difuminan aún más, por la diversidad del ambiente en el que se desarrolla. Una máxima de Crowther (2018), y que simboliza su pensamiento, es definir que los líderes con más recorrido y experiencia deben comprender cómo los seguidores más jóvenes perciben y usan la tecnología. Aunque los líderes militares entienden la importancia de la cibernética y la información, no todos comprenden el alcance de las oportunidades y los desafíos que ofrece el ciberespacio.

Es por lo anterior por lo que este líder, a través de sus enfoques, ha permitido comprender y analizar que los servicios militares deberán gastar más recursos en entrenar y equipar, no solo a las fuerzas cibernéticas, sino a todas las fuerzas que dependen de tecnología y en ese ambiente estarán sirviendo bajo un enfoque cibernético continuo.

Las naciones y sus capacidades de defensa en el ciberespacio

En los nuevos escenarios estratégicos nacionales e internacionales, el ciberespacio es analizado como el escenario preferido de las nuevas formas de conflicto, como es el caso de los conflictos híbridos (Luque, 2019). El dominio cibernético, a diferencia de los dominios tradicionales, presenta grandes diferencias que merecen ser estudiadas e investigadas desde perspectivas distintas y avanzadas; especialmente, cuando nos enfrentamos a situaciones nunca antes vistas. Durante el Simposio Internacional de Seguridad y Defensa, en Perú, en 2005, El PhD Kevin Newmeyer afirmó que, a diferencia de los otros dominios, en los cuales prevalece una potencial posibilidad de conflicto, el ciberespacio ha sido moldeado completamente por el hombre con fronteras inciertas y algunas normas para la política de gobernación.

En dicho ámbito, las naciones buscan controlar cada vez más el dominio ciberespacial generando *poder ciberespacial,* entendido como el potencial para usar el dominio cibernético a fin de lograr los resultados deseados (Nye, 2011, p. 123). La complejidad del poder ciberespacial se configura porque este no se circunscribe al uso de las FF. AA. de una nación, sino que se lo puede ejercer, según una voluntad, por un gran número de actores con la capacidad técnica y humana para su propia

conveniencia en el dominio cibernético, lo que podría ser una evidencia de la proyección correcta del paradigma realista de las relaciones internacionales.

Por su parte, el general de división Evergisto de Vergara y el contralmirante Gustavo Adolfo Trama, de la reserva activa de Argentina, señalan que

> Todas las acciones que se desarrollen en este campo afectarán al componente armado del poder nacional desde varias perspectivas. La primera de ellas es el uso de la fuerza convencional militar como respuesta a un ataque cibernético masivo. La segunda implica el uso del poder militar convencional de los países ante el ataque cibernético a infraestructuras civiles (p. 11).

De igual modo, las operaciones en el ciberespacio están cambiando las características de la guerra. Aunque la naturaleza de la guerra es constante, las características de la guerra pueden cambiar cada vez que se introduce una nueva arma o un nuevo enfoque táctico. Las operaciones en el ciberespacio ahora permiten adquirir y compartir más información y ejercer un mejor mando y control en el campo de batalla, lo que teóricamente reduce la *niebla de guerra* al agregar fidelidad a la comprensión del comandante del espacio de batalla.

Así, el ciberespacio permite un uso más preciso y eficaz de las personas y de las capacidades logísticas involucradas poniendo a la persona o el dispositivo correcto en el lugar correcto, en el momento correcto. Estas capacidades requieren que los gobiernos y sus FF AA. modifiquen sus prácticas. También pone de manifiesto la necesidad de que los líderes y las organizaciones hagan un mejor trabajo al seleccionar y utilizar nuevas tecnologías. Las leyes y las políticas deben actualizarse para aprovechar la nueva tecnología, teniendo también en cuenta un entorno internacional que funciona desde tendencias geopolíticas y geoestratégicas complejas.

Todo esto ha llevado a la humanidad —y en especial, al componente militar— a reflexionar sobre el uso intensivo de las tecnologías digitales como una tendencia que permanecerá en la vida cotidiana, por lo que conceptos como la ciberseguridad y ciberdefensa, aplicados por parte de los individuos, organizaciones y Estados, son sobremanera importantes para garantizar y capitalizar el beneficio de la conectividad y disponibilidad de información de manera segura, a fin de brindar un entorno de mayores posibilidades de desarrollo, así como de bienestar social y fortalecimiento de la democracia en una nación.

Los puntos de vista tradicionales y jerárquicos del liderazgo son cada vez menos útiles, dadas las complejidades del mundo moderno. La teoría del liderazgo

debe transitar hacia nuevas perspectivas que den cuenta de las complejas necesidades de adaptación de las organizaciones y los Estados capaces de afrontar los retos que impone el dominio cibernético, y en este contexto el coronel Glenn (Alex) Crowther, distinguido veterano y especialista en políticas cibernéticas, define que el ciberespacio, por naturaleza, no es un espacio seguro ni protegido y, por tanto, es vulnerable a las amenazas o ataques cibernéticos latentes o emergentes, lo que puede resultar en pérdidas significativas para los sectores económico, político y social o constituir una seria amenaza para la defensa o los intereses nacionales.

Por consiguiente, los Estados, cada vez más dependientes de la tecnología, enfrentan el desafío de una amplia variedad de actores estatales y no estatales en el ciberespacio, que ya es enorme y se halla en constante crecimiento, sin ser claros cuáles intereses en términos de poder gestionarán. La integración de capacidades nacionales a través de sus departamentos de defensa, de seguridad y justicia tienen que operar en este entorno como los tres actores principales del gobierno, que, adicionalmente, deben buscar asociaciones al sector privado, que opera casi todo internet. Por lo tanto, el desarrollo de capacidades en el ciberespacio se constituye en una prioridad para la defensa y seguridad de Colombia, cada vez más dependiente de la tecnología, al tiempo que el despliegue de operaciones militares en el ciberespacio es una necesidad para el avance de los modelos de defensa actuales (Sánchez, 2006).

Alinear dichas estrategias a escala nacional e internacional en un mundo hiperconectado resulta un poco complicado con las teorías tradicionales, por cuanto es una dinámica que trasciende las capacidades de los individuos solos; por eso se hace necesaria la generación de nuevos líderes capaces de articular la complejidad de los sistemas y establecer lineamientos y postulados que permitan teorizar y conceptualizar sobre temas relacionados con el ciberespacio, lo que hasta hoy evidencia tener ambigüedad.

En este contexto, Crowther (2017) ha permitido a la comunidad académica abordar la comprensión del ciberespacio como un dominio de guerra que impacta notablemente la revolución de los asuntos militares en las realidades digitales. El liderazgo ejercido se difunde y materializa en sociedades de diferentes naciones a través de la construcción de documentos de gran interés y relevancia internacional que basan su fundamentación en organismos como el Centro de Excelencia en Ciberdefensa de la OTAN y otras múltiples organizaciones y naciones que han tomado ventaja en el desarrollo de la carrera por el desarrollo de capacidades en el ámbito cibernético.

En este contexto, Crowther, cuyo currículum suma más de 30 años de servicio en el Ejército de Estados Unidos, e incluye ocho giras en el extranjero, con una extraordinaria formación académica y admirable experiencia, ha encontrado que, en este nuevo escenario de confrontación, una vez las sociedades entiendan la naturaleza de las amenazas que enfrentan, se hará necesario movilizar activos no gubernamentales adoptando un enfoque de *toda la sociedad* para reducir el riesgo de la nación. Aquí se evidencia con total claridad cómo, a pesar de la creencia generalizada de que el papel del líder es "manejar el conflicto", lo que significa "reducirlo", por el contrario, el conflicto experimentado en la tensión dinámica entre dos sistemas es en realidad la clave para la innovación y la adaptabilidad en las organizaciones, una clara característica del liderazgo complejo.

Conclusiones

El dominio cibernético fue creado por el hombre, y en ese contexto, tal y como ha sucedido con las formas tradicionales de organización e interacción, se vienen expandiendo las relaciones humanas a entornos digitales no convencionales. Asimismo, con el uso de internet y las tecnologías, se ha incrementado de manera exponencial la superficie de ataque, y con ello, los riesgos asociados a este dominio generan la necesidad de cambiar técnicas, tácticas y procedimientos aplicados en el ámbito de la defensa.

Los conflictos actuales se rigen por métodos de guerra asimétrica, con múltiples vectores y actividades que se habilitan con mayor intensidad en el ciberespacio. En este contexto, se requiere contar con personas capaces de innovar, proponer y, sobre todo, liderar cambios revolucionarios en las estructuras organizacionales estatales y no estatales, en la generación de políticas, programas, estrategias y doctrina, en el desarrollo y producción tecnológica, cambios de estrategias en la Fuerza Pública que permitan el ágil desarrollo de medidas y contramedidas que hagan uso del dominio cibernético, u otros que puedan identificarse en el futuro.

La incertidumbre propia del anárquico panorama internacional, según lo concibe la teoría del realismo de la disciplina de las relaciones internacionales, y los rápidos cambios que se están produciendo en todos los ámbitos están teniendo una gran repercusión en las políticas de seguridad y defensa, tanto nacionales como internacionales (Gil, 2017), lo cual obliga a que se adelanten acciones preventivas y de desarrollo de capacidades que puedan responder a un eventual conflicto en

este dominio. A tal efecto, el desarrollo de capacidades en el ciberespacio debe ser prioritario para la seguridad de cualquier país dependiente de tecnología.

Tal y como sucede en el sistema internacional, no son claras las intenciones ni los intereses, en términos de poder, de los actores del dominio; menos aún, cuando el anonimato propio del entorno digital impide identificar de donde provienen los ciberataques o las diversas amenazas emergentes del medio. De hecho, para los fines de la política tradicional, este escenario se sirve como un medio y un fin en sí mismo, para alcanzar la modificación, mantenimiento o expansión del *statu quo* de los Estados y actores que, por excelencia, han dominado la agenda internacional.

Ante este panorama, ciertamente complejo, es perentorio que cada institución, organización y Estado prevean la formación de líderes en las nuevas generaciones que desarrollen las habilidades y competencias propicias para garantizar los intereses nacionales, procurando siempre que se incluyan la ética y la moral en dicha toma de decisiones, bien sea en una dimensión física o en una cibernética.

Referencias

Aparicio, Z. (2018). El pesimismo antropológico en Hobbes desde una visión poliana. *Mercurio Peruano. Revista de Humanidades,* (531), 51-62. https://doi.org/10.26441/MP531-2018-A2

Bueno, C. (2021). Estoy en el Metaverso, ahora vuelvo. *Digital 4.0. Factoría & Tecnología,* (93), 6-26.

CONPES 3701. (2011, 14 de julio). *Lineamientos de Política para la Ciberseguridad y Ciberdefensa.* Departamento Nacional de Planeación. https://bit.ly/2UhnzYC

CONPES 3854. (2016, 11 de abril). *Política Nacional de Seguridad Digital.* Departamento Nacional de Planeación. https://bit.ly/3brazVR

Cornejo, S. (2017). La relación naturaleza y ser humano, tecnología y biología bajo la luz del posthumanismo. *Revista Antropologías del Sur, 4*(8), 215-232.

Crowther, G. (2017). *The Cyber Domain. The Cyber Defense Review, 2*(3), 63-78. https://www.jstor.org/stable/26267386

Crowther, G. (2018). *National Defense and the Cyber Domain.* The Heritage Foundation. https://www.heritage.org/sites/default/files/2019-10/2018_IndexOfUSMilitaryStrength_National%20Defense%20and%20the%20Cyber%20Domain.pdf

Frasson-Quenoz, F. (2014). *Autores y teorías de relaciones internacionales: Una cartografía.* Universidad Externado de Colombia.

Gaitán, A. (2018). *Ciberguerra. La consolidación de un nuevo poder en las relaciones internacionales contemporáneas.* Universidad Santo Tomás.

Iberdrola. (2022). *Tipos de liderazgo empresarial.* https://www.iberdrola.com/talento/tipos-de- liderazgo

Libicki, M. (2009). *Cyberdeterrence and cyberwar.* RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Luque, J. (2019). *Los nuevos conflictos bélicos del siglo XXI: las amenazas híbridas.* [Programa de Doctorado en Ciencias Sociales]. Universidad de Murcia. https://repositorio.ucam.edu/bitstream/handle/10952/4239/Tesis.pdf?sequence=1&isAllowed=y

Martínez, L., Leyva, M., & Félix, L. (2014). Qué es el Ciberespacio. En L. Martínez, P. Ceceñas, & V. Ontiveros (Eds.). *Virtualidad, ciberespacio y comunidades virtuales,* (pp. 44-93). Red Durango de Investigadores Educativos, A. C.

Newmeyer, K., Cubeiro, E., & Sánchez, M. (2015). Ciberespacio, Ciberseguridad y Ciberguerra. En *II Simposio Internacional de Seguridad y Defensa de Perú* [Simposio]. Escuela Superior de Guerra Naval de Perú.

Nur, A., Ferdion, M., Ari, D., Abdillah, I. (2022) Indonesian StateDefense as an Effort to Counter the Cyber space Security Threat of Metaverse. *International Journal of Arts and Social Science.* https://www.ijassjournal.com/2022/V5I8/414665868.pdf

Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. I*nternational Security. 1*(1), 44-71.

OEWG. (2021). *Open-Ended Working Group OEWG. Reporte Final 2021*. https://dig.watch/resource/oewg-2021-report

ONU, (2018). Documento S/2018/404 (2018, Annex, 3).

Pearson, F., & Rochester, M. (2003). *Relaciones internacionales. Situación global en el siglo XXI.* Mc Graw Hill.

Pérez, V. (2013). El ciberespacio: ¿una realidad en construcción? En P. Irala, & V. Pérez (Eds.). *Cibermedios. Palabra, imagen y tecnología,* (pp. 2-5). Ediciones Universidad San Jorge.

UNESCO. (2021). Informe de la Directora General sobre la aplicación de los resultados de la Cumbre Mundial Sobre la Sociedad de la Información (CMSI). En *Conferencia Anual 41ª reunión* [Conferencia]. UNESCO. Paris, Francia. https://unesdoc.unesco.org/ark:/48223/pf0000379370_spa

USAFT. (2011). *Cyberspace – The Fifth Operational Domain.* https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx

Venatici, C. (1978). *Los orígenes de la Segunda Guerra Mundial.* https://revistamarina.cl/revistas/1978/6/venatici.pdf