Ética militar y ciberseguridad[1]

6

https://doi.org/10.21830/9789585377134.06

Lina María Patricia Manrique Villanueva[2]
Gladys Elena Medina Ochoa[3]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen

Este capítulo reflexiona sobre el concepto de ética militar aplicada a la ciberseguridad. Con este propósito, dialoga con los preceptos clásicos del arte de la guerra, específicamente: influencia moral, terreno y mando, contrastado con las necesidades contemporáneas de la ciberseguridad. El marco teórico adopta la teoría de la complejidad, lo cual implica aristas múltiples, que son susceptibles de ser estudiadas desde diferentes frentes epistemológicos. Con una metodología cualitativa, y usando el análisis de discurso, responde a la pregunta: ¿Cómo acercarse a una comprensión de la ética militar y la ciberseguridad en el contexto colombiano? Para ello, se analiza la campaña "Fe en la causa, comportamiento ético superior" del Ejército Nacional de Colombia. Como resultado del análisis, se constata el nivel de recordación de la campaña y la necesidad de continuar

1 Este capítulo presenta los resultados colaborativos de dos proyectos de investigación: (1) "Desafíos y nuevos escenarios de la seguridad multidimensional en el contexto nacional, regional y hemisférico en el decenio 2015-2025", del grupo de investigación Centro de Gravedad, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia, categorizado en B por Minciencias y con código de registro COL0104976, y (2) "Mujeres de arma, seguridad y defensa nacional. Un análisis desde sus percepciones", del grupo de investigación en Ciencias Militares, de la Escuela Militar de Cadetes "General José María Córdova", Colombia, categorizado en B por Minciencias y con código de registro COL0082556. Los puntos de vista pertenecen a las autoras y no reflejan necesariamente los de las instituciones participantes.

2 PhD en Estudios Políticos y Relaciones Internacionales de la Universidad Nacional de Colombia. Magíster en Nuevas Tecnologías de la Información y la Comunicación (Ntic) de la Universidad Nacional de Educación a Distancia de España. Magíster en Análisis de Problemas Políticos, Económicos e Internacionales Contemporáneos de la Universidad Externado-Science Po. Comunicadora social y periodista de la Pontificia Universidad Javeriana. Docente de la Escuela Superior de Guerra "Rafael Reyes Prieto", Colombia. Orcid: https://orcid.org/0000-0003-3646-4328 - Contacto: lina.manrique@esdegue.edu.co

3 Oficial de la Reserva Activa en el grado de Capitán de Navío de la Armada Nacional. Magíster en Gestión de Proyectos de la Universidad EAN Colombia y Universidad de Quebec a Chicoutimi, Canadá. Especialista en Auditoría de Sistemas de la Universidad Antonio Nariño. Ingeniera de Sistemas de la Universidad Central de Colombia, Auditor Interno Integral en Norma NTC ISO 9001:2015 y NTC ISO 21001:201. Fue Directora de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "Rafael Reyes Prieto". Orcid: https://orcid.org/0000-0001-8375-3195

fortaleciendo los discursos que afiancen cada vez más la credibilidad y la confianza en las instituciones, a partir del comportamiento ético superior. Entre las conclusiones se subraya que la guerra cibernética defensiva y ofensiva plantea serios problemas éticos para las sociedades que deben ser abordados con políticas y campañas, entre otras estrategias. Dado que las armas cibernéticas son tan diferentes de las convencionales, el público está mal informado sobre sus capacidades y pueden respaldar posiciones éticas extremas, en cualquier dirección. Las armas cibernéticas son difíciles de apuntar con precisión dada la interdependencia de la mayoría de los sistemas, por lo que el daño colateral a objetivos civiles es un peligro importante. Sin embargo, las políticas y las campañas sí pueden ser direccionadas adecuadamente para procurar claridad en medio del caos y la complejidad.

Palabras clave: digitalización; ética; guerra; militarismo; seguridad del Estado; tecnología.

Introducción

La velocidad de los avances tecnológicos superó la capacidad de regular el ciberespacio como un tercer entorno. Esto condujo a una brecha entre los hechos tecnológicos y los hechos jurídicos locales. En este contexto, el asunto de las guerras de cuarta generación se ha puesto de relieve en el año 2020, inolvidable también por la situación sanitaria mundial a raíz de la pandemia originada por la Covid-19, que nos ha volcado como ciudadanos a la virtualidad aplicada a la educación, el trabajo y las relaciones familiares, e inclusive a hacerle frente al mundo del *eCrime* o crimen electrónico. En este contexto, el presente capítulo emerge después del trabajo *Ciberparamilitarismo en Colombia: Agencias y complicidades mediáticas* (Manrique, 2019), editado por la Universidad Nacional de Colombia, y del libro *La seguridad en el ciberespacio: un desafío para Colombia* (Medina *et al.*, 2019), editado por la Escuela Superior de Guerra.

La pregunta principal de la investigación es la siguiente: ¿Cómo acercarse a una comprensión de la ética militar y la ciberseguridad en el contexto colombiano? Esta pregunta se formula desde la experiencia de los cursos de Ética en el Ciberespacio y, en general, teniendo en cuenta los aprendizajes para profundizar en los resultados de investigaciones previas, realizadas por las autoras, como investigadoras, académicas y editoras.

Marco teórico

Este capítulo se circunscribe dentro de la perspectiva de la teoría de la complejidad, en la medida en que la naturaleza de la ética militar y la ciberseguridad convoca campos epistemológicos diversos: la ética filosófica, las ciencias militares, la teoría de sistemas, la inteligencia artificial, el derecho y los enfoques contemporáneos de *big data*, entre otros. Además, implica un análisis a la luz de la teoría realista de las relaciones internacionales, las teorías del poder y las formulaciones de política pública en relación con el sistema de gestión de seguridad de la información y la seguridad digital.

En el corazón de la teoría de la complejidad se reconocen los aportes de Edgar Morin, que en los años 60 desarrolló en Francia sus investigaciones sobre la antropología del conocimiento (Morin, 1991, 2011) y desarrolló una nueva aproximación y reorganización de los conceptos que se habían trabajado desde 1940, atendiendo las tensiones entre positivismo y realismo *vs*. constructivismo; cartesianismo *vs*. no cartesianismo, entre otras tensiones filosóficas.

> La educación debe dirigirse a una antropo ética, teniendo en cuenta la triple condición humana: individuo, sociedad, especie. Hay un control de las tres esferas. […] La ética no podría enseñarse con lecciones de moral, sino que debe formarse en la mente a partir de la conciencia de que el ser humano es al mismo tiempo individuo, parte de una sociedad y de una especie. […] La expansión y la libre expresión de los individuos constituyen nuestro propósito ético y político para el planeta; ello supone a la vez el desarrollo de la relación individuo-sociedad en el sentido democrático y el desarrollo de la relación individuo especie en el sentido de la realización de la Humanidad. (Morin, 1991, p. 63)

Desde las teorías de los sistemas, a principios del siglo XX se incorporó el término *cibernética*. Esta surge en 1941 como investigación del Ejército norteamericano. Introduce el concepto de *feedback* para describir cómo se adapta un sistema al medio a partir de una finalidad predefinida. En 1949, la *Conference Macy*[4], aún con poca discusión y base epistemológica, tuvo gran importancia para legitimar estas nuevas corrientes de investigación referidas a la comple-

4 Estas reuniones, que se realizaron en Nueva York entre 1946 y 1953, contribuyeron al desarrollo de la cibernética y la ciencia cognitiva (The Macy Foundation).

jidad (Alhadeff-Jones, 2008). En el texto de Juliao (2017), este mismo hecho es citado de la siguiente manera:

> A partir de 1949, una serie de diez conferencias sucesivas, conocidas bajo el nombre de *Conferencias Macy* fue iniciada por Von Foerster, Wiener, Von Newmann, Savage, McCulloch, Bateson, Mead y Lewin. Pese a la poca profundización epistemológica, esos encuentros contribuyeron a legitimar la idea de la complejidad desde un fundamento pragmático sólido. (p. 158)

Las tradiciones de tres generaciones de estudiosos de la complejidad permiten afirmar que el abordaje contiene ambigüedades, por lo cual estas contribuciones basadas en las teorías contemporáneas relacionadas con la complejidad, así como las valoraciones críticas de su legitimidad epistemológica y ética, deben seguir los ciclos y dinámicas de retroalimentación (Alhadeff-Jones, 2008, p. 67)

De acuerdo con Clausewitz (2002, p. 7), la guerra constituye un acto de fuerza que se lleva a cabo para obligar al adversario a acatar nuestra voluntad. Partiendo de la concepción de Clausewitz de que la naturaleza de la guerra tiene un elemento esencial en ser instrumento de la política, la ética también debe ejercer una notable influencia sobre las decisiones que toman los líderes políticos, de modo que adquiere sentido la existencia de una ética militar que, en las democracias, orienta a los militares cuando se involucran con su asesoramiento y al recabárseles opinión por los responsables legítimos elegidos por los ciudadanos a la hora de tomar decisiones sobre la guerra y la paz (Moliner, 2015, p. 125).

Teniendo en cuenta que en el siglo XXI se ha desarrollado el mundo de la cibercultura, en torno a lo digital, lo que la voluntad de un Estado sobre otro puede pretender imponer obedece a la más variada naturaleza. Atraviesa lo económico, lo político, lo cultural, los recursos naturales y los recursos humanos. Es por esto que estas nuevas formas de guerra podrían tener consecuencias inusitadas e imprevistas.

Las llamadas guerras de cuarta generación o guerras híbridas incorporan elementos de inteligencia artificial y *big data* que constituyen nuevos desafíos estratégicos para las Fuerzas Armadas en Colombia. La inteligencia artificial ha supuesto un gran avance para la humanidad en diversos campos; sin embargo,

eso no implica que su actividad esté exenta de reflexión ética. Todo lo contrario. Existe un desafío en materia militar y de seguridad (Terrones, 2018, p. 141).

Para abordar teóricamente un asunto tan sustancial como la ética militar, acudimos a los postulados primigenios de Sun Tzu, un clásico sobre la guerra, lo cotejamos con autores contemporáneos y, finalmente, proponemos un análisis discursivo de la campaña: "Fe en la causa, comportamiento ético superior", del Ejército Nacional de Colombia.

Actualmente, existen fenómenos de naturaleza diversa, como el *hacktivismo*, el ciberterrorismo, el ciberespionaje, el ciberdelito y la ciberguerra, y en los que se identifican diferentes actores, desde personas hasta grandes organizaciones de acuerdo con ciertos niveles de especialización: "Los movimientos sociales están usando activamente internet para alcanzar sus metas, y nuevos movimientos están surgiendo en red, haciendo visibles los dilemas fundamentales de esta sociedad posindustrial, compleja o como queramos llamarla" (Melucci, 1998, p. 380). Entender la naturaleza, la legalidad y la legitimidad de este amplio espectro de actividades contribuirá a definir estrategias de ciberdefensa realistas, proporcionales y ajustadas a la Constitución y la ley.

En esos escenarios se ha tenido una respuesta progresiva e integral desde los Estados con la creación de Equipos de Respuestas a Incidentes Informáticos (Csirt). Hoy en día, paralelo a esto la Otan nos habla de dos aspectos trascendentales de tendencias mundiales en ciencia y tecnología: las *tecnologías disruptivas* y las *tecnologías emergentes*. Por un lado, encontramos cinco tecnologías disruptivas: la inteligencia artificial, la *big data* y la analítica avanzada, los sistemas de armas hipersónicas, los sistemas autónomos y las tecnologías espaciales. Por otro lado, podemos identificar tres tecnologías emergentes, mucho más nuevas y avanzadas que las disruptivas: las tecnologías cuánticas, las biotecnologías y tecnologías de mejora humana, y los materiales novedosos y de fabricación avanzada. Estos se aplican en los cinco dominios, de manera que existen interdependencias con las otras, convergencias y sinergias que conservan la inteligencia artificial como eje articulador.

Métodos

Este capítulo se aborda con metodología cualitativa. Se propone una revisión analítica de carácter narrativo sobre la ética militar y su relación con el ciberespacio, a la luz de conceptos clásicos como los de Sun Tzu y Clausewitz, y un análisis crítico del discurso de un estudio de caso: "Fe en la causa, comportamiento ético superior". Para ello se realiza una revisión de literatura a partir de un corpus de 25 documentos, entre artículos publicados en revistas indexadas, libros de ética, ética militar y documentos contemporáneos sobre ciberseguridad y ciberdefensa. Luego, se realiza un análisis de resultados en Youtube del video de la campaña "Fe en la causa, comportamiento ético superior", del Ejército de Colombia, que inició como una campaña y derivó en una cartilla orientada al comportamiento ético superior. Finalmente, se incluye un apartado de conclusiones y se presenta una recomendación para revisiones futuras.

En cuanto a la metodología de análisis crítico del discurso, se retoma el proceso sugerido por Neyla Pardo Abril, heredera de la tradición de Teun van Dijk. Pardo Abril ofrece las siguientes herramientas: (1) reconocer un fenómeno social para recolectar un corpus del que se obtienen datos relevantes para la investigación; (2) tomar decisiones sobre las categorías y los recursos analíticos; (3) sistematizar y procesar los datos para obtener redes semánticas; (4) esclarecer estrategias y procesos discursivos, y (5) analizar desde una perspectiva cultural cognitiva para interpretar representaciones de un fenómeno sociocultural (Pardo, 2007).

Factores fundamentales de la ética militar en el ciberespacio

A continuación se revisan los factores fundamentales de la guerra y se actualizan con el contexto actual de las guerras de cuarta generación, aplicadas al contexto colombiano, para llevar a una reflexión sobre la ética militar y la ciberseguridad.

En el capítulo de "Estimaciones, valoraciones, planes o cálculos" de *El arte de la guerra*, Sun Tzu hace los siguientes planteamientos:

1. Influencia moral

"La guerra es un asunto de importancia vital para el Estado; la providencia de vida o muerte; el camino a la supervivencia o la ruina" (Tzu, 2007, p. 91). Luego, invita a apreciarla según cinco factores fundamentales: el primero, la influencia moral; el segundo, el clima; el tercero, el terreno; el cuarto, el mando, y el quinto, la doctrina. Si vamos a reflexionar sobre las guerras del siglo XXI, es necesario analizar estos tres puntos que se conectan directamente con la ética militar en el ciberespacio: (1) la influencia moral de las guerras de cuarta generación, (2) el terreno, que ya no es un espacio físico, sino el ciberespacio, y (3) el mando.

> Con *influencia moral me refiero* a lo que motiva a la gente a estar en armonía con sus líderes, a fin de que les puedan acompañar en vida y muerte sin miedo a morir.
>
> Chang Yu: Cuando alguien trata a la gente con benevolencia, justicia y rectitud, y deposita en ella la confianza, el Ejército estará espiritualmente unido y estará feliz de servir a sus líderes. El libro de las mutaciones dice: 'Con la alegría de superar dificultades, la gente se olvida del peligro de la muerte'. (Tzu, 2007, p. 92)

De la reflexión sobre el trato benevolente, justo y recto se deriva la capacidad de los mandos de obtener confianza de las filas. Cuando los líderes emanan virtudes, es la influencia moral lo que lleva a la gente a estar de acuerdo con sus superiores. El nivel de sacrificio del soldado profesional es muy alto en términos de entrenamiento, disciplina, entrega, esfuerzo físico y mental, por lo cual solo una influencia moral poderosa derivada del liderazgo de sus comandantes puede mantener en alto la moral de las filas y su compromiso férreo con la patria y con su propia familia.

¿Cómo se relaciona este principio con la actuación ética militar en el ciberespacio?

La situación de armonía en el contexto del ciberespacio responde a un uso adecuado de este, dentro de los protocolos de netiqueta y de uso legal y legítimo de las redes. Los escenarios de ataques en el nuevo entorno pueden llegar a reducir la cantidad de hombres para resistir un ataque y entran en

juego otras variables propias de la cuarta revolución. En ese sentido, las batallas ocurren en nuevos escenarios.

> En 2019, en Davos, Suiza, el director general de la Red de Centros para la Cuarta Revolución Industrial del Foro Económico Mundial (Wef, por su sigla en inglés), Murat Sonmez, confirmaba junto al presidente Iván Duque que Medellín había sido elegida como la sede del primer Centro para la Cuarta Revolución Industrial en la región —no solo para Colombia— para toda América Latina. A nuestro país se suman en esta segunda fase de Centros: Emiratos Árabes Unidos, Israel, Sudáfrica y Noruega. En un primer grupo, el Foro Económico Mundial consolidó los Centros para la Revolución Industrial en Estados Unidos, China, Japón e India. (Constaín, 2019)

La ciudad elegida para este reto de innovación tecnológica es Medellín, donde ya se está trabajando para aprovechar la cuarta revolución industrial en inteligencia artificial, internet de las cosas y blockchain (Presidencia de la República, 2019).

Además de los retos de innovación, para el desarrollo tecnológico y la necesidad de responder a la pregunta: ¿Cómo se llevará a cabo los nuevos combates, en contexto de la cuarta revolución industrial?, es necesario fortalecer la capacidad de investigación. Lo que resulte transgresor en términos de protección de datos, será investigado dentro de los términos que plantea la Ley 1581 de 2012 de protección de datos. La comprensión de lo bueno, lo justo y lo correcto dentro del ciberespacio amerita tiempo de reflexión y estudios de caso para poder dilucidar este sentido, incluida también la comprensión del ordenamiento jurídico.

2. Terreno

> Con *terreno* me refiero a las distancias, si este es fácil o difícil de atravesar, si es amplio o estrecho, así como qué posibilidades de vida o muerte ofrece.
>
> Mei Yao-Ch'en: […] Cuando se usan tropas, es esencial saber de antemano las condiciones del terreno. Conociendo las distancias, uno puede planear indirecta o directamente. Si se conoce el grado de facilidad o dificultad para atravesar el territorio, pueden estimar las ventajas de usar la infantería o la caballería. Si se sabe dónde el terreno es angosto y dónde amplio, se puede calcular cuántos efectivos emplear. Si se sabe dónde se iniciará la batalla, se sabe cuándo concentrar o dividir sus fuerzas. (Tzu, 2007)

¿Cómo se relaciona este principio con la actuación ética militar en el ciberespacio?

En el ciberespacio se ha diluido la frontera espacio-temporal, por lo cual se puede mantener comunicación directa entre dos puntos del planeta aunque los husos horarios sean diferentes. Este hecho tecnológico nos lleva a lo que McLuhan denominó la *aldea global*. Además, geográficamente el hecho de los servidores y los *data set* en diferentes países, que responden a normativas y posturas políticas diferentes, constituyen un desafío contemporáneo. Es en este terreno intangible y volátil, donde se puede rastrear una IP o la huella digital, en el que ocurren las nuevas guerras en el siglo XXI.

En el campo de la guerra, la tierra es considerada el primer dominio; el segundo dominio, el mar; el tercer dominio, los ríos, el cuarto dominio, el aire, y ahora, el quinto dominio es el ciberespacio. "El ciberespacio es el quinto dominio de la guerra. Los Estados, además de defender la tierra, el mar, los ríos y el aire, ahora luchan contra los ataques cibernéticos" ("El ciberespacio es el quinto dominio de la guerra", 2020).

El ciberespacio es transversal a los otros ámbitos. En realidad, se comporta como un supraespacio con gran presencia e influencia en el resto de ámbitos. Esta transversalidad hace que el ciberespacio deba ser considerado de manera especial en todos los aspectos conjuntos (doctrina, planeamiento y conducción de operaciones, orgánica, etc.). En primera instancia, el reconocimiento del ciberespacio como un dominio de operaciones, así como la tierra, el mar, el aire y el espacio, ha dado lugar al desarrollo de una nueva ciencia militar y, a partir de ella, de conceptos como el de *ciberseguridad* y *ciberdefensa*. Toda esta situación de riesgos, vulnerabilidades e incidentes en el ciberespacio ha generado una respuesta progresiva e integral desde los Estados en la creación de Equipos de Respuestas a Incidentes Informáticos (Csirt). Asimismo, acompañando la creación de estos entes, se han desarrollado y actualizado diferentes estrategias nacionales en ciberseguridad, las cuales no tienen otro fin más que aprehender las dinámicas actuales que supone el ciberespacio para la seguridad y la defensa (Banco Interamericano de Desarrollo [Bid], 2020).

En el contexto de la ciberdefensa, hoy en día ya se habla de que esta debe interactuar con otras disciplinas, como lo expone la guía de ciberdefensa de la Junta Interamericana de Defensa. Temas como la creación de centros de operaciones cibernéticas donde se enmarcan los tres principales tipos de ciberoperaciones: las defensivas, de explotación y ofensivas, que de acuerdo con su naturaleza, objetivo y entorno pueden ser pasivas, activas o de respuesta.

3. Mando

> Con mando me refiero a las cualidades de inteligencia, sinceridad, humanidad, coraje y severidad del general.
>
> Li Ch'üan: Estas son las cinco virtudes del general. Si es así, su ejército lo llamará "El Respetado".
>
> Tu Mu: […] Si es sabio, un comandante es capaz de reconocer las circunstancias cambiantes y actuar convenientemente. Si es sincero, sus hombres confiarán en las recompensas y castigos. Si es humanitario, amará al prójimo, simpatizará con los otros y apreciará su labor y esfuerzo. Si es valiente, vencerá aprovechando sin vacilar las oportunidades. Si es estricto, sus tropas serán disciplinadas porque están fascinadas con él y temen su castigo. (Tzu, 2007, p. 94)

¿Cómo se relaciona este principio con la actuación ética militar en el ciberespacio?

Se habla de guerra informática o ciberguerra porque el ciberespacio es ya un dominio bélico, como lo reconoce la Organización del Tratado del Atlántico Norte (Otan) (Moliner, 2015, p. 166), donde se desarrollan ciberataques y ciberdefensa, que provocan daños físicos y que ponen en peligro, a menudo, con consecuencias muy serias, las vidas humanas. El mando, en el contexto de la ética militar en el ciberespacio mantiene esos valores que se esperan de las cúpulas: inteligencia, sinceridad, humanidad, coraje y severidad.

Partiendo de la ilustración que nos trae la Constitución Política de Colombia en el artículo 217.°:

> La Nación tendrá para su defensa unas Fuerzas Militares permanentes constituidas por el Ejército, la Armada y la Fuerza Aérea. Las Fuerzas Militares

> tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional. La Ley determinará el sistema de reemplazos en las Fuerzas Militares, así como los ascensos, derechos y obligaciones de sus miembros y el régimen especial de carrera, prestacional y disciplinario, que les es propio.

En el desarrollo de tecnologías en el ciberespacio encontramos: el análisis en el dominio humano, que genera, por un lado, la implementación de tecnologías de datos, como la *big data* y las analíticas avanzadas a partir de algoritmos, la inteligencia artificial para la predicción de comportamientos humanos, pero también, por otro lado, una preocupación por su ciberseguridad. Por esta razón son de utilidad programas como *DarkTrace*, que, a partir de inteligencia artificial, los datos, el *machine learning* o "aprendizaje de máquina", *deep learning* y, en general, todo este ecosistema permiten construir estructuras automatizadas de ciberseguridad que abarcan desde infraestructuras críticas, como las que rastrea el programa *Industrial Immune System*, hasta la seguridad personal, en programas como el *DarkTrace Antígena* o el australiano *Shapes Vector*.

Los sistemas de información que se apoyan, sobre todo, en la inteligencia artificial y en las grandes cantidades de datos para el perfeccionamiento de las operaciones conjuntas en el terreno: *Aktek* con su software *Fusión* es un ejemplo de ello. A través de sistemas satelitales y un cruce de información en el terreno, permiten el entrelazamiento de este flujo de datos y el entrenamiento avanzado de redes neuronales en el ciberespacio para que responda a un mejor diseño operacional en cualquiera o todos los otros dominios (Otan, 2020). Para el caso colombiano, los principales desarrollos en el campo de estudio de la inteligencia artificial y el *machine learning* se están realizando en algunas universidades públicas de Colombia.

Por último, la computación cuántica es un reto para la seguridad informática. De un lado, tenemos la seguridad de los datos cuánticos, es decir, la seguridad de datos representados en *giga bits* con altísimas velocidades de transporte y, por el otro lado, se presentan procedimientos de seguridad cuánticos de los datos haciendo especial énfasis en términos de criptografía y encriptación de estos (Rieffel, 2011).

Estos avances tecnológicos que se están dando en este momento, en especial aplicados a la seguridad y la defensa, se caracterizan por su gran velocidad

de cambio, lo cual trae consigo realidades que plantean ciertos retos: ¿cómo manejar la batalla contra la obsolescencia programada en los equipamientos de defensa y seguridad? ¿Cuál puede ser el alcance del derecho y de la ética en algunos contextos? En general, el desplazamiento de nuestras fuerzas al ciberespacio y las nuevas dinámicas en los campos de batalla suponen el uso de estas tecnologías disruptivas y emergentes.

Como conclusión tenemos que últimamente el quinto dominio, la ciberseguridad y la ciberdefensa son un tema que nos ha ocupado, no solo por ser transversal, sino por su desarrollo exponencial y constante. Sin embargo, podríamos decir que no es lo único que nos ocupa y que debemos prestar especial atención a estas cinco tecnologías disruptivas y a estas tres tecnologías emergentes que guardan correlaciones e interacciones entre ellas implementadas en la defensa. Estas tecnologías y su uso traen retos para nuestro futuro, los cuales están basados en el camino que marcan los avances tecnológicos y que, de alguna forma, nosotros como colegios y escuelas de la seguridad y la defensa para cada una de nuestras Fuerzas Armadas y países debemos afrontar a partir de la investigación científica, de la colaboración y la cooperación multilateral (Otan, 2020).

En este contexto cabe mencionar dos aspectos cruciales para el contexto colombiano: la ciberinteligencia y las campañas para posicionar el discurso de la ética militar.

Ciberinteligencia: inteligencia y contrainteligencia

De acuerdo con Sullivan (1995),

> el concepto de guerra se está expandiendo en dos direcciones, como mínimo. Por una parte, ya no es posible concebir la guerra simplemente como el combate entre los ejércitos de una nación-Estado o grupo de naciones-Estado; por otra parte, se está ampliando el concepto de guerra respecto a su relación con el combate convencional. (p. 35)

Desde este punto de vista, se pueden ver reflejados tanto los avances en materia de contrainteligencia como su alcance, así como desde la ciberdefensa en el informe de gestión correspondiente a la Armada de la República de Colombia (Arc Ig, 2019):

> También se adelantaron actividades relacionadas con la Seguridad Naval, ligadas estas a la protección de la Fuerza, contrarrestando así de forma efectiva la posible materialización de riesgos como la fuga de información (espionaje), subversión y sabotaje; así mismo, se desarrollaron actividades de evaluación y prevención, encaminadas a garantizar la eficiencia y efectividad en el planeamiento, desarrollo y retroalimentación de las Operaciones Navales que desarrollan las diferentes Unidades de la Armada Nacional, situación que permitió preservar el centro de gravedad institucional que es la Legitimidad del actuar de las instituciones militares. (Agudelo, 2020).

Para hacer frente al espionaje y la subversión, el Estado realiza actividades que puedan garantizar la seguridad. Para el caso colombiano, el principio de seguridad es abordado normativamente por la Ley estatutaria 1581 de 2012, de protección de datos personales, la cual considera la seguridad como uno de los principios rectores:

> Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. (Ley 1581 de 2012)

Para retomar el asunto de los riesgos éticos en la aplicación militar, mediada por tecnologías digitales, y para este caso, por inteligencia artificial:

> Son tres los retos éticos en la aplicación militar de la inteligencia artificial:
>
> 1. *El principio ético de reducción del riesgo innecesario a los combatientes propios*
>
> El jefe militar tiene la obligación de proteger a sus hombres reduciendo al máximo las posibles bajas en vidas humanas o en heridas físicas, pero también debe velar por minimizar el riesgo ético de la pérdida del principio de humanidad y la integridad moral que, incluso en las terribles condiciones de violencia en la guerra, deben mantener los combatientes. (Moliner, 2015, p. 179)
>
> […].
>
> 2. *El principio ético y legal de la discriminación entre combatientes y no combatientes*
>
> En el combate, elemento esencial y definitivo de la función del militar, se produce destrucción y se utiliza la fuerza letal. Por ello, el principio de discri-

> minación de combatientes y no combatientes, así como el evitar las bajas de civiles (los daños colaterales) es un elemento esencial de las reglas éticas de la guerra y del Derecho Internacional Humanitario. (Moliner, 2015, p. 181)
>
> […].
>
> *3. El principio de la prevención*
>
> *El principio de la prevención* exige que los científicos no dejen su investigación si algo malo o inapropiado ocurre, sino que desde el inicio hagan un esfuerzo para "prevenir los potenciales malos efectos que podrían venir de sus inventos" (Singer, 2009). (Moliner, 2015, p. 127)

Una campaña en Colombia: "Fe en la causa"

En el caso colombiano se destaca una campaña titulada: "Fe en la causa, comportamiento ético superior". Es la fuerza interior que inspira a los integrantes del Ejército Nacional para lograr la victoria de manera irreprochable. La campaña fue planteada en los siguientes términos:

> **Reto**
>
> Empoderar a cada integrante del Ejército Nacional, como el principal activo de la institución, para garantizar el cumplimiento transparente de la misión.
>
> **Estrategias**
>
> 1. Generar y difundir la doctrina referente al concepto Fe en la Causa, Comportamiento Ético Superior, determinando una política unificada, "centrada en el hombre", que defina las directrices, para los diferentes grupos objetivos.
> 2. Implementar acciones encaminadas a la interiorización del concepto Fe en la Causa, Comportamiento Ético Superior, de manera coordinada con Jefaturas, Direcciones y Unidades Operativas Mayores del Ejército.
> 3. Establecer mecanismos comunicacionales, a fin de garantizar la unidad de mensaje, la optimización de recursos disponibles y el soporte institucional requerido para el posicionamiento y sostenimiento de la campaña. (Ejército Nacional de Colombia, 2011)

Esta campaña logró un nivel de recordación o *top of mind* significativo, que se deduce del comportamiento de las analíticas de Youtube.

El asunto de la "Fe en la causa" se conecta con la convicción de las Fuerzas de la causa justa, como se analizaba arriba con Sun Tzu: "Cuando alguien trata a la gente con benevolencia, justicia y rectitud, y deposita en ella la confianza, el Ejército estará espiritualmente unido y estará feliz de servir a sus líderes".

Uno de los comentarios en torno al video resulta llamativo, y se considera un hallazgo para este análisis. Se transcribe a continuación:

> Fernández
>
> Hace 2 años (editado)
>
> Me acuerdo cuando estaba en instrucción nos mostraron este video, me llené de moral. Hoy día ya salí de prestar servicio y pienso continuar en la Fuerza. (Fernández, 2018)

La heroización (Pardo, 2007) es una de las categorías que propone la profesora Neyla Pardo y que se puede apreciar en este testimonio disponible en internet. Hay un reconocimiento de la necesidad del soldado de obtener moral y luego, una vez vivida la experiencia, una voluntad personal de continuar en las Fuerzas Militares.

El enfoque

> centrado en el hombre como "antropocéntrico" permite inferir los siguientes aspectos, desde el análisis del discurso, teniendo en cuenta las siguientes categorías: enfoque, encuadre, coherencia, cohesión y estilo. […]. Diversos aspectos de cohesión y coherencia han sido estudiados extensamente desde una variedad de perspectivas. Usamos el término *coherencia* para referirnos a las relaciones representacionales y el de *cohesión* para las indicaciones textuales desde las cuales se debería construir representaciones coherentes. […]. El modelo clasifica la *cohesión* y la *coherencia* en locales y globales, guiadas por la gramática y guiadas por el vocabulario, cada una con sus propias especificaciones semánticas (por ejemplo: referencial, espacial, aditiva, temporal y causal). (Louwerse, 2004, p. 41)

Asimismo, cabe anotar que los asuntos de coherencia y cohesión son vitales para la efectividad de la campaña, como puede constatarse en la literatura de estudios críticos del discurso.

Los conceptos clave de la teoría de la guerra justa se incluyen en las categorías de criterios para ir a la guerra (*jus ad bellum*) y luchar justamente durante

la guerra (*jus in bello*): (1) el propósito es correcto, (2) la autoridad está debidamente constituida y (3) último recurso. En pocas palabras, la guerra no puede considerarse justa a menos que siga una búsqueda exhaustiva de negociaciones y otros medios de resolución de conflictos (Arquilla, 1999, p. 381) .

La campaña: "Fe en la causa"

Esta campaña fue lanzada por el Ejército Nacional en el año 2011, con la presencia del señor Almirante Comandante General de las Fuerzas Militares, el señor General Comandante del Ejército, el Estado Mayor del Ejército y los señores Comandantes de las Unidades Operativas Mayores, Menores y Tácticas (Ejército Nacional de Colombia, 2011). Los resultados del éxito de la campaña se pueden medir con apoyo de las herramientas de analíticas que ofrecen las plataformas, en este caso Youtube.

La campaña incluye un desarrollo web, videos en Youtube, cartilla, evento de presentación y sostenibilidad de la campaña en el tiempo. Uno de los videos ofrece el siguiente *copy* en la locución:

> Esta es la historia de un compromiso […] llenando de valor, honor y gloria a nuestros comandantes y todas nuestras tropas. Este compromiso es Fe en la causa […]. Este compromiso ha representado por años sacrificio, espíritu, convicción, pasión, fuerza, transparencia, disciplina, actitud de combate y, sobre todo, victoria.

De las categorías desarrolladas por la profesora Neyla Pardo: *honorificación*, categoría que confiere honor; *espacialización*, que se refiere al terreno y la geoespacialidad, y *heroificación*, que le confiere reconocimiento heroico al sacrificio. Estas tres categorías aplican para el análisis discursivo del video. Para una mirada más global, también resulta interesante la interacción de los cibernavegantes en Youtube.

Resultados

Frente a la pregunta sobre ¿cómo acercarse a una comprensión de la ética militar y la ciberseguridad en el contexto colombiano?, hemos considerado de valor el estudio de los postulados clásicos, en clave de las comprensiones

contemporáneas. Se adopta la perspectiva del pensamiento complejo y se concluye que hay una coherencia entre los postulados clásicos del arte de la guerra, en concreto: influencia moral, terreno y mando, que siguen siendo perfectamente válidos y aplicables al terreno de las guerras de cuarta generación, que requieren del estudio concienzudo de las apuestas de la ética militar en el ciberespacio.

En lo que se refiere al análisis de la campaña "Fe en la causa, comportamiento ético superior", se realizó un análisis de las analíticas de Youtube del canal oficial del Ejército. El análisis de vistas en Youtube, en síntesis, logró los siguientes resultados (tabla 1):

Tabla 1. Analíticas de la campaña "Fe en la causa, comportamiento ético superior"

Características	**Video de Youtube**	
		año
Fecha de publicación	Diciembre 30 del 2010	2010
Vistas	311.029	
Me gusta	1.378	7 de diciembre del 2020
No me gusta	53	
Canal	Ejército Nacional	
Suscriptores	95.100	7 de diciembre de 2020
Duración:	**5'03"**	

Fuente: elaboración propia a partir de analíticas de Youtube (Ejército Nacional de Colombia, 2010).

De los resultados de este análisis de contenido se pudo determinar que la campaña "Fe en la causa" tuvo un impacto significativo. El canal de Youtube cuenta con 95.100 suscriptores. El video, con una duración de cinco minutos, obtuvo 311.029 vistas y un total de 1.378 me gusta al 7 de diciembre de 2020. Se pudo constatar que tuvo un alcance más allá del Ejército, como evidencia su resonancia en la Fuerza Aérea Colombiana.

La aplicación del algoritmo logró que fuera visible. La inteligencia artificial, aplicada al ámbito de las Fuerzas Armadas, es una revolución tecnológica de difícil previsión, que ha de significar una mayor eficiencia, una mayor efectividad y una mayor seguridad en todos los órdenes. Para los Ejércitos es clave la superioridad tecnológica y el combatiente potenciado intelectual y físicamente, capaz de emplear las nuevas tecnologías con rigor científico y ético (Fuente, 2019).

A continuación, la tabla 2 presenta el análisis del discurso del video "Fe en la causa".

Tabla 2. Análisis del discurso del video "Fe en la causa, comportamiento ético superior"

Principios éticos	**Youtube**
	Imagen
Valor	Helicóptero aterriza, toma aérea.
Honor	Cinco soldados armados, listos a disparar.
Sacrificio	Soldado herido, transportado en helicóptero.
Espíritu	Primer plano del rostro de un soldado.
Pasión	Primer plano de soldado hablando.
Transparencia	Dos soldados, uno usa intercomunicador.
Disciplina	Plano americano de soldado armado en operativo.
Actitud de combate	Plano medio de armamento.
Victoria	Plano medio de un capturado sometido.

Fuente: elaboración propia a partir de imágenes de Youtube (Ejército Nacional de Colombia, 2010).

Este estudio también permite identificar los esfuerzos de diferente naturaleza en materia de ciberseguridad, orientados a la ciberinteligencia para el desarrollo tanto de la inteligencia como de la contrainteligencia en las Fuerzas, lo cual supone un reto mayúsculo al estudiar en profundidad los aspectos jurídicos y técnicos de las diversas capas de la web.

Discusión

Si bien la campaña fue lanzada por el Ejército Nacional, las demás fuerzas sintonizaron con sus propósitos. Un ejemplo es la apropiación realizada por la Fuerza Aérea Colombiana (Fac). Uno de los puntos de discusión es revisar si las acciones de campañas deben dirigirse de modo unívoco para cada Fuerza o si, eventualmente, en algunos casos se puede lograr una articulación, como ocurrió en este caso, según se puede inferir de una articulación con la Fac.

En ese sentido, es un reto en términos comunicativos articular los conceptos para lograr mayor alcance de la temática. Respecto a la integración de las Fuerzas en torno a esta campaña se encontró lo siguiente:

> A partir del lanzamiento de la campaña Fe en la Causa […] ¡Con todas nuestras Fuerzas!, realizada por el Comandante General de las Fuerzas Militares, señor General Alejandro Navas Ramos, en Bogotá, la Fuerza Aérea Colombiana se integra con su slogan "Somos la Fuerza", al igual que Ejército y Armada Nacional en un mismo propósito, en una misma Causa. ¡Colombia!
>
> "¡Con todas nuestras Fuerzas!" es la adición que se le hizo a esta campaña, para integrar a las tres fuerzas militares bajo un mismo propósito, corroborando el gran acierto que ha significado para el país trabajar unidos potencializando fortalezas. […] Con frases motivantes, esta campaña reafirma el trabajo, la disciplina, el compromiso, la ética y el valor, entre otros, de las Fuerzas Militares de Colombia, buscando fortalecer esos lazos de confianza, fraternidad, apoyo y credibilidad del pueblo colombiano para con sus Héroes. Soldados de tierra, mar y aire que día a día continúan su marcha, su crucero y su vuelo con ¡Fe en la Causa! (Marín, 2019)

Asimismo, también se encuentra la siguiente información respecto a los propósitos y alcances de la campaña:

> Los hombres y las mujeres que integran la institución son el bien más preciado que esta posee, y se convierten en los únicos garantes del cumplimiento transparente de los objetivos propuestos en el Plan de Campaña. Por esto, es imperativo realizar una estrategia soportada en principios, valores y demás componentes de la cultura institucional, para fortalecer el liderazgo, la vocación militar, el respeto por la dignidad humana y el manejo efectivo de la comunicación organizacional.

> Por lo anterior, nace la campaña institucional "Fe en la causa, comportamiento ético superior", como una fortaleza que permite seguir empoderando en cada miembro de la institución la vocación de servicio, los principios y los valores, con el propósito de conseguir el objetivo final: la victoria de manera transparente, entendida como el sagrado cumplimiento de la misión constitucional.
>
> Es importante entender que el compromiso, el prestigio y la imagen alcanzada por la Fuerza, reflejado entre otras por los índices de favorabilidad, denotan una obligación perenne de seguir avante, dándole al país la defensa y la seguridad que necesita a través de un Ejército eficaz, eficiente, transparente y respetuoso de las leyes y la normatividad imperante. Esta campaña institucional será parte de nuestra cultura organizacional y en ella interactúan de manera coordinada las diferentes jefaturas y direcciones del Cuartel General del Comando del Ejército y los Comandos de las Unidades Operativas Mayores, Menores y Tácticas.
>
> Para garantizar la interiorización del concepto "Fe en la causa, comportamiento ético superior", se aplicarán técnicas de comunicación informativa y persuasiva, a través de mensajes precisos para cada grupo objetivo, con miras a fortalecer la actitud de servicio en los integrantes de la Fuerza. No se ahorrarán esfuerzos para el logro de los objetivos previstos en esta campaña, que busca generar la interiorización del concepto "Fe en la causa, comportamiento ético superior", en todos y cada uno de los integrantes del Ejército Nacional. (Pérez, 2001, p. 515)

En términos de narrativa interna, la campaña "Fe en la causa" ha logrado resultados significativos, por lo cual a futuro resulta valioso emprender nuevas estrategias de comunicación interna. No obstante, el reto narrativo hacia la opinión pública es mayúsculo, ya que las narrativas mediáticas están contrastando y cuestionando diariamente los discursos, que desde el punto de vista corporativo, se logran posicionar con esta campaña.

Las responsabilidades frente a las amenazas cibernéticas deben ser una triada entre el sector privado, el gobierno y la academia. Ya que una debilidad latente del país es el cuidado de nuestras infraestructuras críticas, las cuales requieren hoy en día contar con mayores seguridades, a través de unos roles y responsabilidades adecuados, protegidos por una legislación pertinente que permita tener márgenes de acción óptimos, visualizar y a su vez cumplir la confidencialidad, la integridad y la disponibilidad requerida para estos servicios críticos del país.

La responsabilidad del Ministerio de Defensa frente a la protección de estas infraestructuras críticas obliga a contar con los mecanismos adecuados no solo tecnológicamente, sino estructurales para hacer frente a las amenazas de ciberataques y ciberterrorismos que se puedan presentar. No solo en la detección, sino también en la defensa.

Conclusión

En el contexto colombiano se está hablando de la cuarta revolución industrial desde 2019, en el contexto del Foro Económico Mundial. Este escenario constituye un desafío en materia de ética militar y ciberseguridad porque llama a identificar cuáles son los logros conceptuales, epistemológicos y tecnológicos y a continuar con el trazado de la ruta por seguir, con proyección a las próximas décadas. ¿Cómo acercarse a una comprensión de la ética militar y la ciberseguridad en el contexto colombiano? Es una pregunta parcialmente resuelta en esta revisión bibliográfica, pero requiere un camino que se enfoque en capacidades de investigación, articulación transdisciplinar y entendimiento de la complejidad geopolítica y ética por la que atravesamos en el actual contexto de pandemia global. Los retos de cara a las tres próximas décadas están ya en marcha y exigen la articulación de diferentes instancias.

La guerra cibernética ofensiva plantea serios problemas éticos para las sociedades, problemas que deben abordarse con políticas. Dado que las armas cibernéticas son tan diferentes de las armas convencionales, el público está mal informado sobre sus capacidades y pueden respaldar posiciones éticas extremas, en cualquier dirección. Las armas cibernéticas son difíciles de apuntar con precisión dada la interdependencia de la mayoría de los sistemas, por lo que el daño colateral a objetivos civiles es un peligro importante, como cuando un virus que apunta a sitios militares se propaga a sitios civiles. La evaluación de daños es difícil en los ataques de guerra cibernética, ya que la mayoría de los daños tiene lugar en datos internos ocultos; esto fomenta ataques masivos con la esperanza de garantizar algún daño, de manera que la reparación puede ser difícil, especialmente para los países víctimas que son tecnológicamente primitivos. Por estas razones, algunos ataques cibernéticos

pueden ser procesados como crímenes de guerra. Además, las armas de guerra cibernética son costosas y tienden a perder efectividad rápidamente después de su uso, ya que pierden su elemento sorpresa, por lo que resultan poco rentables (Rowe, 2007).

Campañas como la realizada en 2011, "Fe en la causa, comportamiento ético superior", ofrecen un precedente importante, al cual vale la pena hacerle un seguimiento para proyectar a futuro acciones de este tipo que fortalezcan los factores planteados en esta pesquisa: influencia moral, terreno y mando. Este análisis no solo se puede hacer desde la producción de los mensajes, sino también desde la recepción de sus audiencias, en la búsqueda de obtener cada vez mejores resultados en la comprensión y apropiación del público objetivo y de la sociedad en general.

La tecnología nos deslumbra como el amor y su impacto origina nuevas conductas, percepciones y sensibilidades (Manrique, 2019, p. 214). En la disolución del espacio-tiempo que trae implícito el internet se ha perdido la distancia y el respeto. Esta disolución conlleva, según el filósofo Byung Chul Han (2014), el cambio de lo que era la masa a lo que ahora él ha llamado el enjambre.

Finalmente, para cerrar, es crucial reflexionar sobre el alcance de las tecnologías disruptivas y emergentes para la seguridad y la defensa del país. Si bien hoy en día los países se preparan para su protección y defensa, cabe preguntarnos si podemos llevar ese ejercicio de guerra cibernética a un nivel en el que las consecuencias de las acciones entren en un conflicto ético de responsabilidad por cuanto pueden implicar la pérdida de vidas humanas.

Referencias

Agudelo, A. (2020). *Modelo para la recolección de información de personas en la dark web como insumo para la ciberinteligencia en la Armada Nacional de Colombia.* Escuela Superior de Guerra.

Alhadeff-Jones, M. (2008). Three generations of Complexity Theories: Nuances and ambiguities. *Propuesta Educativa*, 86-90.

Arquilla, J. (1999). *Ethics and information warefare.* En Z. Khalilzad, *Strategic appraisal: The changing role of information in warefare* (pp. 379-401). Rand Corporation.

Banco Interamericano de Desarrollo [BID]. (2020). *Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe*. BID.

Clausewitz, C. (1984). *De la guerra*. Editorial Labor.

Constaín, S. (2019, mayo 5). MinTIC.

Ejército Nacional de Colombia. (2010, diciembre 30). Video institucional Fe en la causa [video de YouTube]. https://www.youtube.com/watch?v=XAXA1EHh2eE

Ejército Nacional de Colombia. (2011, noviembre 11). https://www.ejercito.mil.co/index.php?idcategoria=27619

El ciberespacio es el quinto dominio de la guerra. (2020, enero 21). *El Espectador*. https://www.elespectador.com/judicial/el-ciberespacio-es-el-quinto-dominio-de-la-guerra-article-900856/

Fernández. (2018, agosto 8). [Comentario en Youtube]. https://www.youtube.com/watch?-v=XAXA1EHh2eE

Fuente, J. C. (2019). *La inteligencia militar aplicada a la defensa* [Documentos de Seguridad y Defensa, 79]. Instituto Español de Estudios Estratégicos. https://dialnet.unirioja.es/servlet/articulo?codigo=6896757

Han, B. C. (2014). *En el enjambre*. Herder.

Juliao, C. (2017). *Epistemología, pedagogía y praxeología: relaciones complejas*. Uniminuto. https://repository.uniminuto.edu/bitstream/handle/10656/4455/EpistemologiaRelacionesComplejas.pdf?sequence=1&isAllowed=y

Ley Estatutaria 1581. (2012). Por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial*, 48.587. Congreso de la República. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Louwerse, M. (2004). Un modelo conciso de cohesión en el texto y coherencia en la comprensión. *Revista Signos*, *37*(56), 41-58.

Manrique, L. (2019). *Ciberparamilitarismo en Colombia*. Universidad Nacional de Colombia.

Marín, E. (2019, agosto 8). Fe en la causa… Con todas nuestras Fuerzas. https://www.fac.mil.co/fe-en-la-causa%E2%80%A6con-todas-nuestras-fuerzas

Medina Ochoa, G. E., Sánchez Acevedo, M. E., Becerra, J., León, I., Bohórquez-Keeney, A., Páez Méndez, R. V., & Baldomero Contreras, R. (2019). *La seguridad en el ciberespacio: un desafío para Colombia*. Escuela Superior de Guerra.

Melucci, A. (1996). *Challenging codes. Collective action in the information age*. Cambridge University Press.

Melucci, A. (1998). La experiencia individual y los temas globales en una sociedad planetaria. En P. Ibarra, *Los movimientos sociales. Transformaciones políticas y cambio cultural* (pp. 380-381). Trotta.

Moliner, J. A. (2019). *La inteligencia artificial aplicada a la defensa*. Instituto Español de Estudios Estratégicos.

Morin, E. (1991). *Los siete saberes necesarios para la educación del futuro*. Universidad Pontificia Bolivariana.

Morin, E. (2011). *Introducción al pensamiento complejo*. Gedisa.

Organización del Tratado del Atlántico Norte [OTAN]. (2020). *Tendencias mundiales en ciencia y tecnología*. OTAN.

Pardo, N. (2007). *Cómo hacer análisis crítico del discurso*. Tipografía Editorial.

Pérez, R. (2001). *Estrategias de comunicación*. Ariel.

Pleyers, G. (2018). *Movimientos sociales en el siglo XXI*. CLACSO.

Presidencia de la República. (2019, mayo 5). Colombia en la cuarta revolución industrial. https://id.presidencia.gov.co/Paginas/prensa/2019/Colombia-en-la-Cuarta-Revolucion-Industrial.aspx

Rieffel, E. (2011). *Quatum computing: A gentle introduction*. MIT Press.

Rowe, N. (2007). Ethics of cyberwar attacks. En A. Colarik (ed.), *Cyber war and cyber terrorism* (pp. 1-6). The Idea Group.

Singer, P. (2009). *Especismo y estado moral*. Wiley Online Library.

Sullivan, G. (1995). *War in the information age.* Nueva York: Strategic Studies Institute.

Tara, A. (2020). *The Macy Conferences on cybernetics: Reinstantiating the mind*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190236557.013.541

Terrones, A. (2018). Inteligencia artificial y ética de la responsabilidad. *Cuestiones de Filosofía*, *4*(22), 141.

Tzu, S. (2007). *El arte de la guerra*. Taschen GmbH.