Guerra de información y ética militar: entre la tradición de guerra justa y la teoría de guerra irrestricta[1]

4

https://doi.org/10.21830/9789585377134.04

Carlos Enrique Álvarez Calderón[2]
Hans Jiménez Martínez[3]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen

En el siglo XXI, la tecnología se ha convertido en uno de los medios cruciales para la conquista de nuevos dominios de batalla, en los cuales la pérdida de vidas ya no es el principal objetivo estratégico. En guerras de quinta generación, el objetivo estratégico es inducir la implosión del adversario mediante el empleo de la fuerza no cinética de ataques cibernéticos, que pueden incluir operaciones de información y/o guerra de información. Por consiguiente, la guerra de información está redefiniendo la forma como se llevan a cabo los conflictos en la posmodernidad, y al hacerlo, está planteando nuevos problemas éticos y morales, especialmente a la luz de la tradición de guerra justa y la teoría de la guerra

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 los autores y no reflejan necesariamente los de las instituciones participantes.

2 Politólogo y magíster en Relaciones Internacionales de la Pontificia Universidad Javeriana y Coaching Ontológico Empresarial de la Universidad San Sebastián de Chile. Becario del Center for Hemispheric Defense Studies "William Perry", Washington. Profesor e investigador principal de la Maestría en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Orcid: https://orcid.org/0000-0003-2401-2789 - Contacto: carlos.alvarez@esdegue.edu.co

3 Magíster en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Abogado con especialización en Derecho Administrativo de la Universidad del Rosario y asesor de la Consejera Presidencial para los Derechos Humanos en la Política de Prevención de Reclutamiento de Niños y Niñas por parte de Grupos Armados Organizados y Grupos Delincuenciales Organizados. Orcid: https://orcid.org/0000-0001-7867-8610 - Contacto: hansjimenez@presidencia.gov.co

sin restricciones. El objetivo general de este capítulo es determinar, a partir de la tradición de guerra justa, cuáles son los principales desafíos que la guerra de información y la guerra sin restricciones le plantean al Derecho Internacional Humanitario y a la ética militar en Occidente.

Palabras clave: Derecho Internacional Humanitario; ética; guerra; guerra de información; guerra sin restricciones; tradición de guerra justa.

Introducción

La guerra ha sido un fenómeno recurrente en la historia de la humanidad. No obstante, desde el inicio de la historia registrada de los conflictos se ha intentado elaborar un enfoque ético de la guerra, condicionada a perspectivas culturales y filosóficas particulares, como aquellas emanadas desde Occidente y Oriente. En el contexto occidental, y "ante una aparente vocación de la naturaleza humana por hacer la guerra, se hizo necesario justificarla a través de la razón con bases teológicas, legales y filosóficas" (Álvarez & Duque, 2020, p. 89). Por consiguiente, con la aceptación de que la guerra es un mal necesario siempre y cuando busque el mantenimiento de la paz y el orden, la teoría de guerra justa estableció en Occidente las normas éticas aceptables en el ejercicio del combate militar por parte de los Estados. Como lo señala Frost (2006),

> hacer la guerra es una actividad desarrollada dentro de una práctica social a la que son intrínsecos componentes éticos muy sólidos. Sin esos componentes, hacer la guerra no sería una actividad significante para quienes la hacen, sino más bien un comportamiento "sin sentido". Hacer la guerra es hacer algo que, desde el punto de vista del actor, tiene una dimensión ética; una dimensión que no es algo que se agrega opcionalmente, sino central a la propia actividad de la guerra. (p. 1)

Empero, la guerra en el siglo XXI tiene variaciones significativas de aquellas guerras realizadas en siglos anteriores. Hasta principios del siglo XX, era evidente y necesario justificar las guerras, ya que los Estados luchaban generalmente por territorio o riqueza, y en su curso ocasionaban la destrucción masiva de personas y mercancías. Pero en el siglo XXI, la guerra ha asumido nuevas formas: la tecnología se ha convertido en uno de los medios cruciales

para la conquista de nuevos dominios de batalla, en el cual la pérdida de vidas ya no es el principal objetivo estratégico. En guerras de quinta generación, el objetivo estratégico es inducir la implosión del adversario, afectando su conectividad, su infraestructura productiva y su proceso de toma de decisiones (Álvarez *et al.*, 2017), mediante el empleo de la fuerza no cinética de ataques cibernéticos, que pueden incluir operaciones de información y/o guerra de información.

La naturaleza de estas nuevas amenazas es tan crítica, que ciberanalistas como Clarke y Kanke (2010) y Brenner (2011) predicen que en el futuro próximo podría suscitarse un "ciber Armagedón", de magnitud similar a los ataques terroristas del 11 de septiembre en los Estados Unidos. Y según los expertos en guerra de información, una guerra cibernética podría ser tan generalizada y destructiva como una guerra convencional o incluso nuclear; en consecuencia, y en el actual marco de las guerras de quinta generación (Álvarez *et al.*, 2017), la "guerra de información" está redefiniendo el concepto mismo de la guerra y cómo se llevan a cabo los conflictos en la posmodernidad. Al hacerlo, está planteando además nuevos problemas éticos y morales, que incluyen la posibilidad de imponer restricciones legales significativas al desarrollo de armas cibernéticas o al uso de la guerra de información, especialmente a la luz de estrategias militares como la guerra sin restricciones, promulgada oficialmente y perseguida aparentemente por China, Rusia y otros Estados nacionales. Por consiguiente, en la presente era de la información, se hace necesario volver a examinar los conceptos éticos en relación con la guerra, ya que están surgiendo nuevas formas de conflicto que ponen a prueba la comprensión existente de las "guerras justas", dado que las avanzadas tecnologías de la información "ya requieren un replanteamiento de una amplia gama de leyes comerciales y penales" (Arquilla, 1999, p. 379).

Generaciones evolutivas de la guerra moderna y posmoderna

Históricamente, los avances tecnológicos han determinado cambios significativos no solo en las estructuras sociales, políticas y económicas de la humanidad, sino también en las organizaciones militares de los Estados. En

el caso de las guerras modernas, que inician con el uso sistemático de armas de fuego a partir del siglo XVI, el uso de la pólvora allanaría el camino para la creación de los ejércitos profesionales al servicio de los recientemente creados Estados-nación, y en abandono del uso de fuerzas mercenarias que monopolizaron el ambiente militar del periodo de la Edad Media. En lo que Lind *et al.* (1989) caracterizaron como guerras de primera generación, el comienzo de la guerra moderna fue posible por el uso generalizado de mosquetes y cañones, que redujo el tiempo y el costo de entrenar a los soldados, y aumentó la capacidad de los Estados de constituir, ya para el siglo XVIII, ejércitos de decenas o cientos de miles de soldados. En esta primera generación de la guerra, el teatro de operaciones era unidimensional (tierra y mar de superficie), en el cual los ejércitos y las marinas buscaban, mediante la aplicación de la fuerza cinética contra el centro de gravedad del adversario, la "aniquilación" o destrucción directa del enemigo (Álvarez *et al.*, 2017). Un ejemplo de guerras de primera generación fueron las guerras napoleónicas entre 1803 a 1815, que, junto a las guerras revolucionarias francesas, ocasionaron la pérdida en vidas de tres millones de soldados y un millón de civiles (Ellis, 2003).

La segunda generación de la guerra marca el inicio de la guerra industrializada y la creciente mecanización de las fuerzas militares de los Estados, producto de las armas de retrocarga, artillería de mayor alcance, redes telegráficas y el uso de locomotoras y barcos a vapor para movilizar a millones de soldados a los campos de batalla. Por ende, esta segunda generación de la guerra fue posible gracias a la primera y segunda revolución industrial, así como a la incorporación de los avances de la tecnología civil en el desarrollo de las operaciones militares. El uso de las primeras ametralladoras conllevó que las antiguas tácticas de línea y columna, y la aproximación directa en busca del combate cuerpo a cuerpo quedaran en desuso, por lo cual la movilidad que había caracterizado las guerras en el pasado daba ahora paso a la lógica de la guerra de posiciones. Según Álvarez *et al.* (2017),

> la industrialización produjo un cambio profundo en la forma en la cual se combatían las guerras. Como resultado del desarrollo de un mayor poder de fuego por parte de los ejércitos, la mayoría de la cual era fuego de arti-

> llería indirecto, se generalizaría la utilización de las trincheras como medio de protección de los soldados. (p. 162)

En consecuencia, las guerras de segunda generación, como lo fue la Primera Guerra Mundial, requerían un mecanismo de derrota distinto: ya no sería la aniquilación directa del adversario, sino, por el contrario, el desgaste de los recursos del enemigo para sostener su posición. Y debido a la montaña de suministros, municiones y hombres que se requería para "aguantar" y mantener la posición, se hizo necesario incorporar en la economía de defensa los avances civiles en los procesos industriales, como la producción masiva de armas serializadas con partes intercambiables, cadenas de montaje, los motores eléctricos y la electrificación a escala industrial (Álvarez & Ramírez, 2020).

Las guerras de segunda generación también implicaron un alto número de fallecidos, no solo por la mayor letalidad de las armas cinéticas, sino además por el uso de otros instrumentos mortales como las armas químicas: por ejemplo, se estima que en la Primera Guerra Mundial lucharon 65 millones de soldados, de los cuales murieron 1 de cada 8, un promedio de 7.534 hombres fallecidos cada día entre 1914 a 1918 (Álvarez *et al.*, 2017). En total, se calcula que la Gran Guerra produjo quince millones de soldados muertos y seis millones de civiles fallecidos (White, 2012). Sin embargo, y al igual que en las guerras de primera generación, las bajas civiles fueron minoritarias cuando se las compara con el total de fallecidos por acciones directas de las hostilidades, dado que las batallas se concentraron en amplios territorios rurales en los cuales se podía desarrollar la guerra de trincheras, como las tácticas de formación de línea y columnas durante las guerras de primera generación.

Las guerras de tercera generación se producen con el advenimiento de la Segunda Guerra Mundial y el uso generalizado de los tanques, los submarinos y el poder aéreo, con el objetivo de volverle a dar movilidad a la guerra y así escapar de la lógica de desgaste de los recursos característico de las guerras de segunda generación. Ahora la guerra se libra con mayores capacidades de destrucción que buscan acortar los tiempos y recursos necesarios para doblegar la voluntad de lucha del adversario, a través del método de aproximación indirecta que permite, mediante la velocidad y la sorpresa, la dislocación mental y física del enemigo. Esta fue la esencia alemana de la "guerra relámpago" o

Blitzkrieg o de la estrategia japonesa de "fuerza móvil" o *Kido Butai* (Álvarez *et al.*, 2017). Ahora el escenario de guerra es tridimensional (tierra, aire y guerra submarina), en el cual el bombardeo aéreo se convierte en un factor disruptivo que busca doblegar la capacidad de lucha del oponente mediante la destrucción de sus ciudades y el ataque inmisericorde de su población civil. En efecto, durante la Segunda Guerra Mundial, tanto en Occidente como en Oriente, murieron sesenta y seis millones de personas, de los cuales veinte millones fueron soldados y cuarenta y seis millones fueron civiles (Keegan, 1990).

Las guerras de cuarta generación inician con la última fase de descolonización en todo el mundo, particularmente en Asia y África. Ante el advenimiento de fuerzas militares estatales de tercera generación, con gran capacidad destructiva, fuerzas aéreas y número de efectivos que podrían incluso superar el millón de soldados, se requirió que las fuerzas insurgentes y revolucionarias no estatales, con capacidades humanas y materiales limitadas, tuviesen que buscar un mecanismo de derrota del oponente que no implicara la aniquilación directa o el desgaste de los recursos del enemigo (lo cual sería imposible), como tampoco la dislocación física y mental mediante la velocidad y la sorpresa (al no contar con los medios tecnológicos para hacerlo). En consecuencia, se implementa la estrategia de guerra irregular o guerra de guerrillas, en la cual, si bien se sigue combatiendo en el plano físico de tierra, mar o aire, el escenario de combate decisivo es el político, ya que el mecanismo de derrota en guerras de cuarta generación es desgastar "la voluntad política de lucha del adversario, más que denegarle los medios (destrucción de sus capacidades militares) para hacerlo" (Álvarez *et al.*, 2017, p. 172).

Entonces, la estratagema que adopta una guerrilla es el uso selectivo del terrorismo en contra de la población civil y la infraestructura del Estado, así como la prolongación indefinidamente del conflicto armado, buscando erosionar el apoyo de la sociedad civil a los esfuerzos de la guerra por parte de los Estados. Esto permite en teoría que fuerzas irregulares cuantitativa y cualitativamente inferiores puedan triunfar sobre fuerzas militares estatales superiores en tamaño o armamento; no porque la guerra se decida en los dominios tradicionales de la guerra, sino en el escenario político de la guerra, relacionado con el apoyo de la población y su legitimidad ante esta. Como el

primer practicante moderno de la guerra de cuarta generación, Mao Tse-tung comprendió que la guerra revolucionaria era una cruzada política en la que se debía prestar especial atención el mantenimiento de la buena voluntad del pueblo (Tse-tung, 1954). Con ello, y junto a una disposición a sufrir bajas y a que el conflicto se prolongase en el tiempo, una guerrilla podría llegar a tomarse el poder del Estado a través de las armas; no en vano los chinos comunistas lucharon durante 27 años; los vietnamitas lucharon contra los franceses y norteamericanos durante 30 años; los afganos combatieron a los soviéticos durante 10 años, y las Fuerzas Armadas Revolucionarias de Colombia (Farc) y otras insurgencias contra el Estado colombiano durante más de 60 años (Álvarez *et al.*, 2017). En resumen, entre la guerra civil en China, la guerra de Vietnam, la guerra civil de Camboya, la revolución en Cuba, la guerra de Nicaragua y la guerra insurgente en Colombia, el total aproximado ha sido de once millones de muertos, la mayoría de ellos civiles (White, 2012).

Al menos hasta las guerras de tercera generación, se entendía que la guerra era tradicionalmente el uso de la violencia por parte de un Estado, a través del despliegue de sus fuerzas militares, con el fin de determinar las condiciones de gobernanza sobre un territorio determinado (Gelven, 1994); en otras palabras, que la guerra era la contienda entre dos o más Estados a través de sus fuerzas armadas, con el propósito de imponer sobre el otro su voluntad. Pero con las guerras de cuarta generación, y la proliferación de grupos armados no estatales, el Estado pierde el monopolio sobre la guerra; si las guerras de primera generación se basaron en la movilización de la mano de obra, las guerras de segunda generación en el incremento del poder de fuego y las guerras de tercera generación en una mayor libertad de maniobra, las guerras de cuarta generación se caracterizaron por la combinación de todas las formas de lucha por parte de un actor no estatal (van Creveld, 1991).

Si la guerra de cuarta generación señala el final de las guerras modernas, la guerra de quinta generación marcaría el inicio de las guerras posmodernas, caracterizadas por la incorporación de los avances de la tercera revolución industrial a las operaciones militares. Si bien la tercera revolución industrial se daría a partir de la década de los sesenta con el desarrollo de los primeros semiconductores, y en la década de los setenta y ochenta con el avance en la infor-

mática personal (Álvarez & Ramírez, 2020), el pináculo de la revolución de las tecnologías de la información y las comunicaciones se dio con la irrupción del internet en la última década del siglo XX. Por consiguiente, y a partir de la revolución de la información y el ciberespacio, la expansión de los escenarios de la guerra más allá del dominio físico ha permitido que el espacio de batalla se torne omnipresente (Álvarez *et al.*, 2017).

Guerra de información y teoría de la guerra irrestricta

En las guerras de quinta generación, aparte de los dominios tradicionales de tierra, mar y aire, en donde una fuerza militar se mueve a través del tiempo y el espacio, se vuelven críticos los escenarios informativo, social y cognitivo. Según Reed (2008), el escenario de información es aquel donde se construye, se manipula y se comparte la información; el escenario social es donde los seres humanos interactúan, intercambian información, forman conocimientos compartidos y emprenden acciones colaborativas; y el escenario cognitivo es donde surgen los conceptos decisivos y se toman las decisiones estratégicas. Estos tres escenarios se caracterizan en la actualidad por tener asiento mayoritariamente en el ciberespacio, por lo que la guerra de información se convierte, entonces, en la forma preferida de llevar a cabo la guerra en el siglo XXI.

Kuehl (2002) define la guerra de la información como el conflicto o lucha entre dos o más grupos en el entorno de la información, mientras que Nichiporuk (1999) considera que la guerra de información es el "proceso de proteger las propias fuentes de información del campo de batalla y, al mismo tiempo, buscar negar, degradar, corromper o destruir las fuentes de información del campo de batalla del enemigo" (p. 188). No obstante, para efectos de este capítulo, y en el marco de la guerra de quinta generación, la guerra de información se entiende como una estrategia no cinética orientada a moldear y cambiar el comportamiento, y manejar las expectativas de audiencias amistosas o adversarias, usando lenguaje, imágenes o símbolos para lograr un efecto deseado o un estado final.

En el marco de las guerras de quinta generación, existen ciertas diferencias entre la moderna "guerra de información" y el concepto clásico de "operaciones de información". Formas tradicionales de operaciones de información, como

contramedidas de radar, contramedidas de C3[4], intrusión de computadoras y operaciones psicológicas, consisten generalmente en técnicas que poseen objetivos, alcances y orquestaciones limitados (es decir, están restringidos a una operación de combate específica), y desempeñan un papel de apoyo o soporte en las actividades de combate[5]. También referido como guerra de Comando y Control (Gc2), las operaciones de información convencionales abarcan todas las tácticas militares que utilizan la tecnología de las comunicaciones, entre las cuales se contemplan el engaño militar, las operaciones psicológicas (Opsic), la guerra electrónica (Ge), la guerra psicológica, las operaciones cibernéticas y la destrucción física de las instalaciones de comunicaciones enemigas (Johnson, 1997). El objetivo en la Gc2 es negar información al enemigo y así interrumpir sus capacidades militares de comando y control[6], mientras que de manera simultánea se toman precauciones para proteger las propias capacidades de C2[7].

En contraste, la guerra de información en el contexto de guerras de quinta generación no compromete simplemente un conjunto de técnicas y tácticas militares. Se rige por una estrategia o plan integral para el uso de procedimientos y armas cinéticas y no cinéticas, en el cual el objetivo puede ser militar, político, económico o cognitivo (figura 1). Por ende, una campaña de guerra de información unificada puede llevarse a cabo junto con múltiples operaciones de combate simultáneas o consecutivas, e incluso puede extenderse más allá del

4 En términos generales, el Comando y Control (C2) es un conjunto de atributos y procesos organizativos y técnicos que emplea recursos humanos, físicos y de información para resolver problemas y lograr los objetivos de una organización o una misión; el (C3) incluye Comando, Control y Comunicaciones, y el (C3I) o (C4) abarca el Comando, Control, Comunicaciones e Inteligencia.

5 Estas formas de ataque tienden a usarse a nivel táctico y en actividades que no son de combate, estas formas de ataque suelen ser independientes y aisladas.

6 Además de apuntar al C2 del enemigo, las operaciones de información pueden dirigirse a las comunicaciones políticas o civiles del adversario.

7 Desde el punto de vista estratégico, las operaciones de información pueden emplearse para alcanzar objetivos nacionales, influyendo en todos los elementos políticos, militares, económicos o aquellos relacionados con la información del poder nacional de un adversario, al tiempo que se protegen los propios. Desde lo operacional, las operaciones de información se proponen alterar las líneas de comunicación, de logística, de C2 del adversario, así como las capacidades y actividades relacionadas, al tiempo que se protegen las propias. Finalmente, desde el punto de vista táctico, el objetivo de una operación de información será alterar la información y los sistemas de información relacionados con la cadena de C2, los servicios de información y los procesos vinculados con la información directamente relacionados con la conducción de operaciones militares.

campo de batalla inmediato, cruzando los límites entre tiempos de paz, crisis y combate. El término *información* en la guerra de información sugiere que el objetivo de dicha campaña implica la generación de efectos sobre la información del adversario que evitarán o impulsarán ciertas acciones, con lo cual se crea una ventaja para el atacante[8]. Tal propósito implica, por lo tanto, que el verdadero objetivo de la guerra de información no sea un ataque a sistemas específicos, sino al proceso de decisión del adversario que reside en el dominio cognitivo. Por lo tanto, la planificación de ataques en la guerra de información debe basarse no solo en las características de esos sistemas, sino también en los efectos deseados de orden superior (Molander *et al*., 1996).

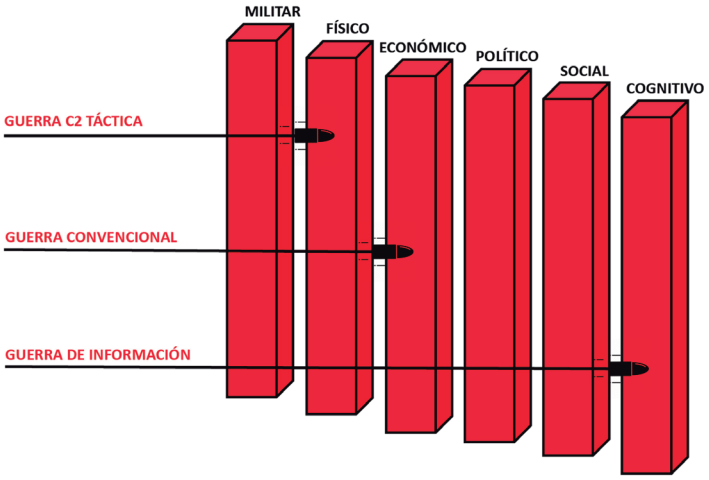

Figura 1. Guerra C2 *vs*. guerra de información.
Fuente: adaptado de Molander *et al.* (1996).

Por lo tanto, se puede considerar que el concepto general de la guerra de información está constituido de tres partes diferenciadas, pero complementarias (Johnson, 1997): un conjunto de técnicas y capacidades, una estrategia integral que los aplica y un objetivo. En consecuencia, un modelo útil de la guerra de información debe describir el objetivo final, identificar y enumerar los elementos aplicables de la guerra de información y mostrar cómo se

8 Por su parte, el objetivo de la guerra de información defensiva implica prevenir o contrarrestar esos efectos.

pueden combinar los elementos en la estrategia para atacar al objetivo. Cabe mencionar que un modelo genérico del objetivo de una campaña de guerra de información se basa en la diferencia antes mencionada entre guerra de información y operaciones de información individuales, caracterizado por tres capas (figura 2).

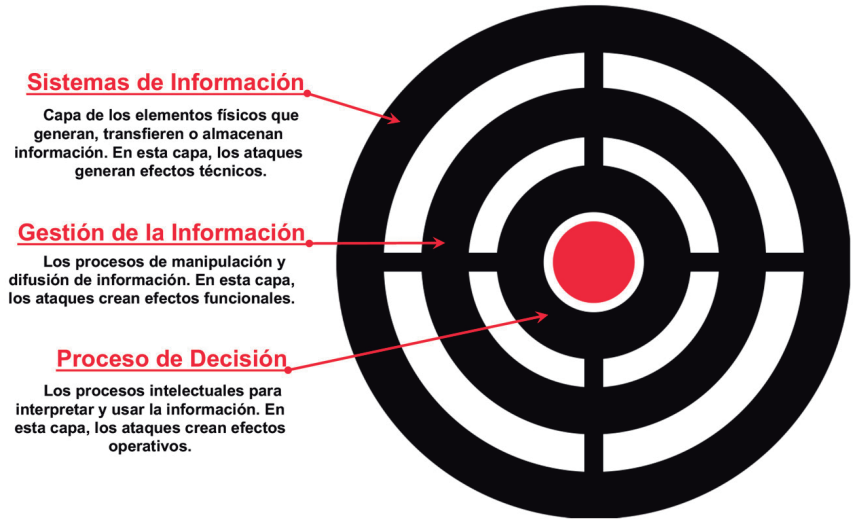

Figura 2. Modelo de tres capas.
Fuente: elaboración propia.

Los ataques de guerra de información[9], independientemente de su objetivo final, usualmente comienzan afectando la capa del "sistema de información", que es a menudo, pero no siempre, un sistema electrónico. En muchos casos, pero no en todos, ese sistema es el objetivo inicial del ataque y se pretenden efectos técnicos: sobrecarga del receptor, corrupción de datos, apagado del sistema, borrado de datos, destrucción física, etc. La capa de gestión de información hace referencia a la transferencia, diseminación, almacenamiento, fusión y conversión de información; estas funciones las realizan los sistemas de información y representan una capa lógica superpuesta a la

9 Toda operación cuyo propósito sea perturbar, negar, deteriorar o destruir la información contenida en computadores o redes informáticas también son referidos como "ataques contra redes informáticas" (*Computer Network Attack*).

capa física de los sistemas de información. Según Johnson (1997), ejemplos de efectos funcionales derivados de un ataque a la capa de gestión de la información son un cambio en la capacidad de transferencia de información, retrasos en el rendimiento y enrutamiento incorrecto del tráfico[10].

Sin embargo, el objetivo final de la guerra de información es la forma en que se utiliza la información, es decir, la capa del proceso de decisión, ya que los efectos deseados de los ataques de guerra de información pueden ser no solamente cegar o confundir al enemigo, sino también moldear sus percepciones, decisiones, opiniones o comportamiento. En efecto, muchos comandantes y estrategas exitosos a lo largo de la historia tenían una comprensión intuitiva de sus adversarios en este nivel cognitivo, y a menudo lo aplicaban en tácticas y operaciones psicológicas con el propósito de confundir, demorar, manipular o paralizar al enemigo (Álvarez *et al.*, 2018).

Los efectos de una capa generan efectos consiguientes en las siguientes capas; por ejemplo, un ataque de interferencia de comunicaciones en un sistema de información crea un bloqueo o corrupción de la señal en un receptor (efecto técnico), lo que a su vez reduce la información disponible en este canal (efecto funcional), y un tipo de efecto operativo consecuente sería el retraso en la decisión (Johnson, 1997). Hay que reconocer, sin embargo, que esta propagación de efectos no es la única forma de atacar la capa de decisión, porque los ataques pueden realizarse contra cualquier nivel. Aunque un ataque finalmente se reduce a una operación física que involucra un sistema de información físico, ese sistema puede ser solo un vehículo, y no el objetivo del ataque. Por lo tanto, el ataque puede tener poco o ningún efecto técnico directo. De hecho, es posible que un ataque tampoco tenga un efecto funcional; puede crear

10 La gestión de la información se está convirtiendo en un asunto cada vez más importante y vulnerable, porque los sistemas de información modernos apenas siguen el ritmo de las tecnologías de la información en constante evolución. Otra vulnerabilidad es la incompatibilidad de información. Este problema se debe a la evolución de los requisitos para las operaciones conjuntas, junto con un gran aumento en la cantidad de sistemas de comunicaciones y datos que tienen estrictos requisitos de compatibilidad; un enemigo podría aprovechar este problema identificando y apuntando a los nodos críticos donde se realiza la conversión de datos, o aprovechando la confusión a través de engaños o ataques de intrusión. Si los administradores de información están acostumbrados a ver datos ilegibles, es posible que no reconozcan el hecho de que algunos datos se han distorsionado o corrompido, atribuyendo los problemas a las deficiencias conocidas de su sistema.

directamente un efecto operativo en quien toma las decisiones. Un ejemplo es una campaña de propaganda en la que el sistema de información que se utiliza es el periódico o cualquier otro medio de comunicación convencional, y en el cual el objetivo es influir la percepción de quien toma las decisiones; en este caso, por lo tanto, los efectos técnicos y funcionales son nulos. Por lo tanto, los ataques pueden tener diferentes objetivos y efectos inmediatos, y no todos se propagan necesariamente desde la capa básica del sistema de información (Molander *et al*., 1996).

En la tabla 1 se ilustran algunos ejemplos de diferentes procesos de ataque y cómo se pueden asignar al modelo de tres capas (Johnson, 1997), resaltando que en la guerra de información los efectos operativos son el objetivo más importante, ya que cualquier ataque tiene que crear o contribuir a los efectos operacionales deseados, ya sea por sí mismo o en combinación con otros ataques. Es preciso considerar que la propagación de efectos puede ser compleja y que no todos los ataques de la guerra de información crearán todos los tipos de efectos. Un efecto técnico dado puede generar efectos operativos muy diferentes, dependiendo de qué se ataca y en qué circunstancias; además, los efectos operativos pueden depender de combinaciones de efectos técnicos y funcionales, por lo cual una estrategia de guerra de información debería tener en cuenta estos factores.

Tabla 1. Modelo de tres capas

Tipo de ataque	Capa objetivo	Efecto técnico	Efecto funcional	Efecto operativo
Interferencia de comunicaciones	Sistema de información	Bloqueo de señal	Pérdida de información	Decisión retrasada o incorrecta
Intrusión de comunicaciones	Gestión de la información	Ninguna – El enlace continúa existiendo	Enrutamiento incorrecto de la información, sobrecarga autogenerada (diagnóstico, corrección, repetición de mensajes)	Retraso, confusión

Continúa tabla...

Tipo de ataque	Capa objetivo	Efecto técnico	Efecto funcional	Efecto operativo
Virus informático	Sistema de información	Parálisis del sistema	Pérdida de datos, pérdida de función en el nodo	Decisión retrasada o indirecta
Gusano de red	Gestión de la información	Ninguna – Los enlaces de red continúan existiendo y operando	Retraso o sobre-carga que equivale a pérdida de función	Decisiones retra-sadas; apagado deliberado de los nodos no afectados
Opsic (Operaciones Psicológicas)/ Propaganda	Proceso de decisión	Ninguna	Ninguna	Influencia en la decisión
Operación militar como maniobra Opsic	Proceso de decisión	Ninguna	Ninguna	Manipulación de la percepción

Fuente: Adaptado de Johnson (1997).

En las guerras de quinta generación los dominios de batalla son multi-dimensionales, con la posibilidad de que la guerra se lleve a cabo en el plano físico (tierra, mar, aire, espacio), y en el virtual (informativo, social y cogni-tivo). De acuerdo con Álvarez *et al*. (2017), "esta expansión de los escenarios de la guerra hace posible la extensión exponencial del concepto de campo de batalla más allá del dominio físico, eliminando sus limitaciones geográficas y políticas, permitiendo que el escenario de guerra se torne omnipresente" (p. 192). En la actualidad, los dominios informativo, social y cognitivo dependen en gran medida del ciberespacio[11], por lo que su importancia como escenario de conflicto de las guerras de quinta generación estaría directamente relacio-nada con la revolución de la información y las comunicaciones.

Históricamente, los avances tecnológicos han determinado cambios que afectan la estructura tanto de la sociedad civil como de las organizaciones mili-

11 El término "ciber" se deriva del sustantivo griego *kybernaein*, que se refiere a un "espacio" o un dominio.

tares. Como lo señalan Toffler y Toffler (1993), este fue el caso de la revolución neolítica, cuando los seres humanos fabricaron armas por primera vez con madera y rocas, y posteriormente con la revolución industrial, que proporcionó los medios para la guerra industrializada y para la diseminación de armas de destrucción masiva. Pues bien, la revolución de la información sería el ejemplo actual de cómo un avance tecnológico significativo ha cambiado las actividades humanas de varias formas y en varios niveles, incluyendo la guerra. En consecuencia, y como producto de esta última revolución tecnológica, surge la "ciberguerra"[12], que puede asumir una de las siguientes tres formas (Orend, 2014): (1) *espionaje*, es decir, utilizar el ciberespacio para recopilar información que un Estado protege como una cuestión de seguridad nacional; (2) *difusión de desinformación*, por los mismos medios, de una manera que perjudique los intereses de seguridad del Estado antagonista, y/o (3) *sabotaje*, o en otras palabras, utilizar el ciberespacio para provocar la disrupción o destrucción de varios sistemas que son parte integral de los intereses básicos de una comunidad política (como la electricidad, la distribución de agua y combustible, los sistemas de transporte, el sistema bancario y bursátil, e incluso internet)[13].

En épocas pasadas, la decisión de emprender una guerra convencional implicaba generalmente un compromiso político sustancial, debido al elevado costo humano, moral y económico al que se podía incurrir por la movilización de grandes contingentes de soldados y armas de gran poder destructivo, tal como lo evidenciaron las guerras de primera, segunda o tercera generación. En este orden de ideas, la guerra se entendía tradicionalmente como el uso de la violencia por parte de un Estado a través del despliegue de sus fuerzas militares, con el fin de determinar las condiciones de gobernanza sobre un territorio determinado (Gelven, 1994); es decir, la guerra era una contienda entre dos o más Estados a través de sus fuerzas armadas, con el propósito de dominarse mutuamente e imponer las condiciones de paz que le pareciera al

12 El término "ciberguerra" fue acuñado en un informe de Rand Corporation escrito por Arquilla y Ronfeldt (1993), para predecir una nueva forma de guerra consistente en la interrupción del flujo de datos en los sistemas de información.

13 En consecuencia, un "ataque cibernético" se refiere entonces a cualquier uso específico de cualquiera de las tres formas de ciberguerra descritas.

vencedor. Empero, la guerra de información ha cambiado radicalmente estos aspectos, y proporciona tanto a actores estatales como no estatales los medios para llevar a cabo la guerra posmoderna de una manera completamente diferente, afectando no solo la forma como los militares y los políticos consideran y/o libran la guerra, sino también la forma en que la guerra es percibida por la sociedad civil.

Pero si bien la preferencia por el uso de fuerza no cinética se convierte en una de las características principales de la guerra de quinta generación, la guerra de la información también puede ser muy poderosa y potencialmente muy disruptiva, ya que, a diferencia de las generaciones anteriores de la guerra, la guerra de quinta generación es potencialmente incruenta, rentable y no requiere experiencia militar. Además, si la guerra convencional comprometía solo a seres humanos y objetos físicos, la guerra de información involucra entidades artificiales que no son físicas, junto con seres humanos y objetos físicos. En resumen, las tecnologías de la información y las comunicaciones han modificado los costos de las guerras posmodernas y, por lo tanto, su comprensión y evaluación. En consecuencia, y ante una tendencia a librar la guerra en múltiples escenarios que requieren el uso de medios cinéticos y no cinéticos, y en el cual todos (Estados, organizaciones no estatales e individuos) son potencialmente actores de la guerra de la información, puede llegar a ser más adecuado definir la guerra en el siglo XXI como "un estado de conflicto colectivo y organizado, que puede desarrollarse a través de hostilidades violentas y no violentas" (Álvarez *et al.*, 2017, p. 152).

Con referencia a esta concepción posmoderna de la guerra, Liang y Xiangsui (1999) demuestran que la guerra no es solo el uso de la fuerza armada que obliga al enemigo a ceder a los propios deseos, sino más bien el uso de todas las formas en que la fuerza cinética y no cinética, militar o no militar, se utiliza para obligar al enemigo a someterse a los propios intereses. Esta es la esencia de la teoría de guerra "irrestricta" o guerra "sin restricciones", que adapta la lógica de guerra asimétrica a la actual era de la información, con el empleo de armas que ya no se limitan a balas, bombas o misiles. Liang y Xiangsui (1999) abogan por una estrategia consistente en impedir la capacidad del enemigo para librar la guerra y defenderse contra un aluvión de ataques

contra su economía, sus instituciones civiles, sus estructuras gubernamentales e incluso su sistema de creencias[14].

Por consiguiente, la clave es traspasar las fronteras no solo físicas, sino también cognitivas para superar al enemigo. La aplicación de esta nueva aproximación estratégica a la forma como se lleva a cabo la guerra asimétrica se puede constatar en las manifestaciones y protestas sociales en América Latina en 2019 y 2020, ya que uno de los principales objetivos de esos movimientos sociales ha sido transcribir el discurso político a la realidad, mediante la movilización de manifestantes a las calles a través de las redes sociales, y en el cual la protesta pacífica eclosiona con el vandalismo y otras acciones disruptivas. En conformidad, se produce una politización creciente de estas acciones, y a medida que el ciberactivismo se extienda a nuevos dominios, termina perdiendo un concepto exclusivamente militar.

> El ciberactivismo se constituye en una nueva forma de expresión revolucionaria o forma de alentar la revolución, en medio de un universo en el que los intereses geopolíticos de las grandes potencias y actores pueden hacer uso de ellas para promover e incitar las revueltas revolucionarias sin ofrecer rastro alguno, o por movimientos antisistémicos que ven en el ciberactivismo la mejor forma de desestabilizar las formas de poder desde el descontento social y su accionar colectivo. (Cortés & Garzón, 2017)

En consecuencia, el ciberespacio se convierte en el principal dominio de combate en guerras de quinta generación, en el cual un actor buscará mediante la guerra de información esconderse, conocer, engañar y persuadir al adversario, con el objetivo de interrumpir o modificar lo que una audiencia objetivo "sabe" o "piensa que sabe" sobre sí misma y sobre el mundo que la rodea (Arquilla & Ronfeldt, 2001). Y dicha guerra de información guarda

14 Liang y Xiangsui (1999) reconocían que ningún actor detentaba las capacidades (al menos hasta inicios del siglo XXI) para enfrentar en una guerra convencional a las fuerzas armadas estadounidenses; por lo tanto, recomendaban que la única forma en la que China podía enfrentarse a Estados Unidos era mediante el desarrollo de capacidades ofensivas y defensivas en otras áreas, incluido el ciberespacio, en el que los Estados Unidos no son dominantes y, por el contrario, son muy vulnerables. De esta proposición nacieron las campañas de ciberespionaje y acciones encubiertas (bombas lógicas en infraestructura civil vital, robo masivo de tecnologías industriales y militares clasificadas, entre otras), que ha llevado a cabo el Estado chino a través de un rama ultrasecreta del Ejército de Liberación Popular conocida como la "Unidad 61398".

relación con la proliferación del uso de redes sociales y foros en línea por parte de algunos movimientos políticos en América Latina, así como el empleo de tácticas de desinformación, imitando en cierto sentido la metodología de la revolución cultural de Antonio Gramsci, la cual se podría sintetizar de la siguiente manera:

> Primero, desacreditar todo lo tradicional; Segundo, inventar una nueva doctrina para suplantar a la anterior; Tercero, infiltrarse en la superestructura (Educación, Iglesia, Fuerzas Militares, Medios de Comunicación, Economía, etc.) para seguir desacreditando lo "antiguo", y fortalecer el nuevo pensamiento desde el interior; Cuarto, legalizar todo lo anterior (convertirlo en ley); y Quinto, tomar el poder político, es decir, el gobierno. (Álvarez *et al.*, 2017, p. 222)

Asimismo, la era de la información del siglo XXI ha dado paso a la ciberguerra, en la cual los nuevos protagonistas son los piratas informáticos, cuyo principal objetivo es amenazar gravemente la seguridad de un Estado, atacando mediante virus informáticos la infraestructura crítica y los procesos de información del enemigo. Si bien no ejercen necesariamente una profesión militar, algunos *hackers* trabajan para unidades de guerra cibernética existentes en países como China, Rusia, Estados Unidos e Israel, entre otros. Para los Estados y los actores no estatales, participar de la guerra cibernética ofrece una serie de ventajas asimétricas, ya que el ciberespacio es un dominio en el que resulta relativamente fácil asegurar el anonimato, los ataques se pueden lanzar desde casi cualquier parte del mundo, y los efectos de los ataques cibernéticos son desproporcionados en relación con su bajo costo (Rosenzweig, 2013).

Con base en lo anterior, la ciberguerra y una de sus subsidiarias, la guerra de información, desborda el tradicional papel de las instituciones militares del Estado, por lo cual la seguridad nacional ya no puede depender únicamente de la fuerza militar (Liang & Xiangsui, 1999). Entonces, la guerra sin restricciones se convierte en una fórmula para el lento pero inexorable asalto contra las instituciones sociales, económicas, políticas y militares de un enemigo, a menudo sin que el enemigo sepa que incluso está siendo atacado[15]. Es buscar librar la

15 Como escribió una vez Sun Tzu (2012): "Si una parte está en guerra con otra y la otra parte no se da cuenta de que está en guerra, la parte que sabe que está en guerra casi siempre tiene la ventaja y generalmente gana"(p. 67).

guerra contra un adversario con métodos tan encubiertos, al menos al principio, y aparentemente tan benignos (no cinéticos), que la parte atacada no se da cuenta de que está siendo víctima de ataque. En resumen, Liang y Xiangsui (1999) advierten que en un entorno globalizado en donde todo es interdependiente, "el significado de límites y fronteras es algo simplemente relativo, y que, por tanto, es preciso combinar en un gran método de guerra todas las dimensiones y procedimientos (tanto militares como no militares) para llevar a cabo la guerra" (Álvarez *et al.*, 2017, pp. 217-218). En consecuencia, el principal argumento de Liang y Xiangsui (1999) se basa en la premisa de que en la guerra sin restricciones no existen reglas, y que las partes en contienda llevarán a cabo la guerra comercial, la guerra financiera, la nueva guerra del terror, la guerra ecológica, la guerra psicológica, la guerra de contrabando, la guerra mediática, la guerra contra las drogas, la guerra de redes, la guerra tecnológica, la guerra de recursos, la guerra cultural y la guerra de derecho internacional, con el propósito de satisfacer sus objetivos estratégicos (Bunker, 2000).

La teoría de la guerra sin restricciones plantea varios interrogantes sobre cómo los Estados se involucrarían en este tipo de guerra, particularmente en relación con el derecho internacional. Como lo señala Bunker (2000), ninguna guerra es buena, pero al menos durante el último siglo, principalmente en Occidente, se ha hecho un intento real de limitar sus horrores y distinguir entre combatientes y no combatientes. Pero la guerra irrestricta ni siquiera será una guerra, al menos en su concepción tradicional occidental, ya que el planteamiento de Liang y Xiangsui (1999) vuelve borrosa, por ejemplo, la cuestión de qué es y qué no es un acto de guerra, y/o quién es y quién no es un combatiente. Estas preguntas se han formulado muchas veces en el pasado con respecto a la guerra de información, máxime cuando por reivindicación de la libertad de información en democracias liberales, el derecho al libre flujo de información es también una política de puertas abiertas para que un actor inserte su propaganda en los sistemas de pensamiento y creencias de su enemigo, por lo que la dificultad de localizar al oponente o de comprender las reglas del juego también daría cuenta de la dificultad de abordar este tipo de guerra desde los principios éticos de la tradición occidental de la guerra justa.

La tradición de guerra justa en el marco de las guerras de quinta generación

Con el primer Convenio de Ginebra en 1864 se dio nacimiento al Derecho Internacional Humanitario, si bien ya existían ciertas normas para la protección de las víctimas desde el año 1000 a. C. Por ejemplo, los hindúes, egipcios y hebreos formularon reglas que regían el tratamiento humano de prisioneros y no combatientes en tiempos de guerra, y Sun Tzu (2012) insistía en que los ejércitos tratasen con respeto tanto a prisioneros como a los no combatientes. En la Grecia clásica, el uso del combate singular o *monomaquia*, y en el Imperio Romano, la implementación de la doctrina de Cicerón, fueron intentos de "humanizar" la guerra primitiva. Sin embargo, estas costumbres de guerra solían aplicarse solamente a las guerras iniciadas en el seno de una misma civilización y aun así, podían llegar a ser ignoradas (Bellamy, 2009). Estas convenciones se ocupaban de asegurar que las políticas individuales dentro de una determinada civilización pudieran resolver sus diferencias de manera violenta con un mínimo de perjuicio para la civilización en su totalidad, y más aún, estas reglas y tradiciones eran parte constitutiva de la vocación de un guerrero, ya que servían para distinguir a los soldados profesionales de los asesinos.

Sin embargo, el Derecho Humanitario, como parte del Derecho Internacional de la Guerra, adquirió características más específicas con el Convenio de Ginebra de 1864, que además de establecer una serie de disposiciones activas que los Estados debían llevar a cabo para con las víctimas del conflicto armado, también limitaba la soberanía del Estado en la conducción de las hostilidades con respecto a los individuos que estuviesen implicados en ellas. A la par del desarrollo de la protección de las víctimas de conflictos armados, los Estados consideraron también necesario establecer limitaciones de derecho a los medios y métodos de combate. Esta necesidad nacería de la tradición occidental de guerra justa, que, si bien consideraba la guerra como un mal necesario, también contemplaba que la guerra no debía ocasionar más dolor ni destrucción que lo inevitable para el desempeño de su cometido[16].

16 Por consiguiente, y a partir del Convenio de Ginebra de 1864, de la Declaración de San Petersburgo de 1868 y de los Convenios de La Haya de 1899 y 1907, el derecho de la guerra se ha

Por lo tanto, la teoría de la guerra justa se ha considerado tradicionalmente como un camino intermedio entre el pacifismo, por un lado, y el realismo, por el otro (Reichberg, 2002). En efecto, como lo señala Patterson (2007), "en un mundo imperfecto, la doctrina de la guerra justa equilibra el ideal de paz con la realidad que supone la violencia y el derramamiento de sangre" (p. 35). Y desde Aristóteles (2004), Platón (2014), San Agustín (1946), Santo Tomás de Aquino (2002), Rousseau (1927), Grocio (1925), entre otros, los exponentes de la teoría de guerra justa han estructurado sus argumentaciones en torno a una lista de criterios destinados a ayudar a organizar el pensamiento moral sobre la participación en la guerra. Según Brough *et al*. (2007), la tradición de la guerra justa se basa en dos ideas fundamentales: "Existen normas a partir de las cuales se puede concluir que en algunas situaciones el recurso a la guerra es justo, y que existen normas que permiten que la guerra se lleve a cabo de manera justa" (p. 243). Es decir, si el recurso a la fuerza militar tiene un fundamento moral, este debería proceder de una "causa justa", ser autorizado por una autoridad legítima y llevarse a cabo de manera proporcional a los fines que pretende alcanzar, discriminando entre aquellos que son objeto de ataque (combatientes) y aquellos que no lo son (no combatientes-civiles). Por consiguiente, las normas de la tradición de guerra justa se dividen usualmente en dos niveles: las que guían la decisión de iniciar la guerra (*jus ad bellum*), y las que rigen su conducta (*jus in bello*). El primer nivel o *jus ad bellum* determina las razones legítimas con las que un Estado decidirá ir a la guerra, enfocándose en seis principios sustanciales (Brough *et al.*, 2007):

1. *Justa causa*: una guerra está justificada solo si se libra por una o más causas justas, como la propia defensa o el socorro a un aliado contra un ataque injusto, la protección a los civiles de violaciones generalizadas y recurrentes de los Derechos Humanos cometidas por su propio gobierno o por otras partes en una guerra civil (intervención humanitaria), así como la amenaza inminente de agresión y/o las amenazas futuras por el posible uso de armas de destrucción masiva

orientado hacia la protección de las víctimas en las guerras y la limitación de los medios y los métodos de combate.

por parte de terroristas o Estados "rebeldes" (guerra preventiva); es decir, la causa justa de la guerra suele limitarse a la autodefensa, la defensa de otros, la restauración de la paz, la defensa de los derechos y el castigo de los infractores.

2. *Autoridad legítima*: el uso de la fuerza militar está permitido solo si está autorizado por un organismo político que sea ampliamente reconocido por todos los actores del sistema internacional; este principio también se conoce como el principio de autoridad apropiada o competente[17].
3. *Intención correcta*: una guerra debe librarse con la única motivación de alcanzar una justa causa; por ejemplo, si la causa justa es detener el genocidio, entonces el único motivo que guía la intervención humanitaria armada debe ser detener el genocidio[18] (Álvarez & Duque, 2020).
4. *Último recurso*: antes de recurrir a la fuerza militar se deben perseguir, dentro de límites razonables[19], otras alternativas no militares, incluidas la diplomacia, las negociaciones o las sanciones económicas y legales; por lo tanto, la decisión de retrasar el uso o la amenaza de la fuerza militar debe estar guiada por el interrogante de si el uso de la fuerza militar es la única manera o la más proporcionada de reparar el daño sufrido.
5. *Posibilidad razonable de éxito*: una guerra debe librarse solo si existe una esperanza razonable de que se cumplan los objetivos enraizados en su justa causa, ya que es objetable exigir grandes sacrificios a los combatientes, o infligir daños graves a los no combatientes, si la

17 Por supuesto, ha sido objeto de cierta controversia si los Estados-nación, independientemente de su estatus moral o credibilidad, tienen autoridad legítima para realizar la guerra; también hay desacuerdo sobre si los actores no estatales, como las guerrillas o los grupos terroristas, pueden tener autoridad legítima. E incluso si un organismo internacional como las Naciones Unidas puede tener una autoridad legítima frente a los Estados.

18 También es controversial, por ejemplo, si una intervención armada por razones humanitarias también puede estar originada por motivos secundarios, como el interés nacional, el acceso a recursos, ganancias económicas, el aumento de la influencia y el poder internacionales, lo que podría debilitar o socavar la legitimidad moral de una guerra.

19 Para una explicación correcta de este principio es crucial determinar qué se entiende por "dentro de límites razonables".

victoria militar parece una posibilidad muy remota; entonces, desde un punto de vista más amplio, una guerra justa implica la posibilidad de crear una paz duradera.

6. *Proporcionalidad*: este principio[20] establece que los bienes anticipados de librar una guerra deben ser proporcionales o acordes con sus males esperados; según la interpretación común, esto significa que los beneficios anticipados de la guerra deben pesar más que sus daños, o que al menos los daños esperados no excedan en gran medida los beneficios; en otras palabras, la guerra se considera justa si el daño global que puede causar la guerra es menor que el causado por el mal que se intenta corregir (Álvarez & Duque, 2020).

El segundo nivel de la tradición de guerra justa, o *jus in bello*, establece las prácticas aceptables de las fuerzas militares de un Estado mientras este se encuentre en guerra; contiene dos principios básicos (Brough *et al.*, 2007):

1. *Discriminación*: las partes en contienda deben discriminar entre combatientes y no combatientes, y aplicar solo a los primeros la fuerza militar[21]; es decir, los no combatientes nunca deberán ser atacados deliberadamente. Es importante resaltar que diferentes teóricos de la guerra justa (Coppieters & Fotion, 2002; Rodin, 2003; Walzer, 2000) ofrecen diferentes versiones de quiénes deben ser contados como no combatientes y por qué, ya que el daño a los no combatientes generalmente se considera un resultado aceptable de una acción militar si no se inflige intencionalmente y es proporcionado a la importancia de los objetivos de la acción militar. Sin embargo, un enfoque más estricto de cuánto "daño colateral" es moralmente aceptable, exige a los soldados minimizar las bajas de no combatientes incluso a riesgo de mayores costos para ellos mismos[22].

---

20 El principio de proporcionalidad en el *jus ad bello* se denomina principio de "macroproporcionalidad", a fin de distinguirlo del principio de "microproporcionalidad" del *jus in bello*.

21 Este principio también se denomina principio de "inmunidad de no combatientes".

22 Es moralmente inadmisible destruir objetivos que tengan propósitos esencialmente civiles, y el empleo de algunas armas como las nucleares y biológicas, o las minas terrestres, son moralmente objetables debido a su impacto indiscriminado.

2. *Proporcionalidad*: los medios de la fuerza deben usarse en proporción al fin que se pretende alcanzar, y la destrucción más allá de lo necesario para alcanzar un objetivo militar es moralmente objetable[23]. En este orden de ideas, las armas que causan lesiones a las personas mucho después de que han dejado de ser combatientes, como las armas nucleares y biológicas, son desproporcionadas; por consiguiente, los combatientes no deben usar armamento prohibido y su conducta, además, no debe violar las leyes de la guerra.

En los últimos años ha cobrado relevancia un tercer nivel de la tradición de guerra justa (Patterson, 2007), que se aplica en el proceso de transición desde un conflicto armado hacia una paz justa y sostenible (*jus post bellum*). El tercer nivel introduce una guía ética para una finalización justa de la guerra y la construcción de una paz duradera[24]. Por lo tanto, bajo el *jus post bellum* se exige al victorioso colaborar con la población huésped en la reconstrucción de su país, y ayudar a sentar las condiciones suficientes para la no repetición del conflicto al finalizar la guerra (Clifford, 2012). De acuerdo con Evans (2008), las cuatro tareas que un actor victorioso en la guerra debe acometer, una vez se alcance el final del conflicto, son: (1) establecer términos de paz que estén proporcionalmente determinados para hacer que esa paz sea justa y estable, así como para reparar la injusticia que provocó el conflicto; (2) asumir la plena responsabilidad de su justa parte de las cargas materiales de las secuelas del conflicto en la construcción de una paz justa y estable; (3) proseguir esas iniciativas políticas nacionales e internacionales para la prevención de conflictos, y (4) participar de forma plena y proactiva en los procesos socioculturales de perdón y reconciliación que son fundamentales para la construcción de una paz justa y estable.

Según Patterson (2007), para que el *jus post bellum* tenga utilidad en el mundo real, debe abordar los problemas pasados, presentes y futuros que

23 Podría afirmarse que las leyes de la guerra permiten la matanza sin límites de soldados enemigos, pero tal afirmación es objetable en términos del principio de proporcionalidad.

24 Aunque la tradición de la guerra justa había contemplado desde hacía tiempo preocupaciones sobre el *jus post bellum*, el primero en proponer la adición específica de un marco de *jus post bellum* a la teoría de la guerra justa fue Michael Schuck (1994).

rodean el conflicto. En este orden de ideas, un final justo del conflicto es aquel en el cual se resuelvan las causas que originaron el conflicto y eviten futuros enfrentamientos que perpetúan las condiciones de inseguridad, tomando en consideración tres principios rectores (Patterson, 2007):

1. *Orden*: el primer y fundamental principio del *jus post bellum* es el orden, ya que poner fin a la guerra suele ser más importante y urgente que continuar el derramamiento de sangre en la búsqueda de mejores términos. Por ende, las guerras deben terminar de manera que rehabiliten o creen un orden político duradero, y tal orden, como mínimo, es una seguridad entre los Estados y, por lo tanto, una seguridad contra los ataques externos a sus poblaciones.
2. *Justicia*: esta suele adoptar una de dos formas: compensación o castigo. La justicia puede tomar la forma de una compensación, es decir, un pago de algún tipo al agraviado o la(s) víctima(s), o puede tomar la forma de castigo, por emplear la violencia en primer lugar o por cómo se perpetró la violencia. Por lo tanto, además de crear una situación de seguridad, los agresores deben rendir cuentas de alguna manera por sus acciones, ya que la rendición de cuentas es un principio ético basado en la noción de responsabilidad de los líderes políticos y militares.
3. *Conciliación/reconciliación*: si los objetivos fundamentales de la teoría de la guerra justa son promover la seguridad y proteger la vida humana, entonces la conciliación lo hace mejorando las condiciones que pueden conducir a una nueva violencia. A diferencia del orden y la justicia, la conciliación se centra en el futuro porque ve a los antiguos enemigos como socios en un futuro compartido. En los conflictos internacionales es más probable que el objetivo sea el esfuerzo mutuo de ambas partes para superar la hostilidad pasada y reformular la relación como una de asociación, mientras que en conflictos intraestatales se habla de "reconciliación", o la acción de tender puentes entre partes que tienen un pasado compartido.

Ética militar y guerras de información

El interés del análisis ético aplicado a la guerra de información y el dominio cibernético ha venido ganando importancia en el debate de la ética militar. Sus inicios pueden rastrearse a finales del siglo XX en trabajos académicos realizados por pioneros como Denning (1998; 2007), Arquilla (1999), Arquilla y Ronfeldt (2001), Floridi (1999; 2005; 2007; 2010) y Rowe (2007; 2008; 2010; 2011). Empero, las primeras discusiones morales sobre las normas y las restricciones sobre el comportamiento aceptable durante la ciberguerra fueron llevadas a cabo por personas no especializadas en este campo de estudio, que consideraban la teoría de guerra justa como el marco conceptual adecuado que debía ser aplicado directamente a los conflictos cibernéticos (Lucas, 2015). Sin embargo, el primer análisis en ética militar en relación con la "ciberguerra" fue realizado por Arquilla (1999), y posteriormente por Dipert (2010; 2013), Carr (2011), Lucas (2013; 2014; 2015), Floridi y Taddeus (2014), y Singer y Friedman (2014), quienes ampliaron investigaciones sistemáticas en la materia. Cabe anotar que estas primeras discusiones éticas también deben diferenciarse de aquellas desarrolladas por Schmitt (1999; 2002; 2011; 2013) y Dunlap (2011), conforme a la aplicación del derecho internacional a los conflictos cibernéticos.

En cuanto a los principios éticos que rigen el *jus ad bellum*, y su aplicabilidad en relación con la guerra de información, la "justa causa" para ir a la guerra, expresada en la teoría clásica de la guerra justa en las nociones de la autodefensa y la prevención (es decir, atacar para evitar el surgimiento de una amenaza), la justa causa puede asumir diferentes interpretaciones en el contexto de una guerra de información o en el contexto del desarrollo de operaciones de información. En efecto, la guerra de información puede describirse como "operaciones de información que se efectúan en tiempo de crisis o conflicto para alcanzar o promover objetivos específicos contra uno o varios adversarios concretos" (Schmitt, 2002, p. 365), mientras que las operaciones de información (las cuales son un subconjunto de las guerras de información) "abarcan prácticamente toda medida no consensual cuyo objetivo sea descubrir, alterar, destruir, interrumpir o transferir datos almacenados en un ordenador, o procesados o transmitidos por él" (Schmitt, 2002, p. 365). Por consiguiente, si las

operaciones de información pueden efectuarse tanto en tiempos de paz como en las etapas estratégicas, operativas o tácticas de un conflicto armado, se establece que la diferencia entre la guerra de la información y otras operaciones que se distinguen por alterar o proteger la información se determina por el contexto en el que se realizan, sea en paz, crisis o conflicto[25].

Con respecto al segundo principio de "autoridad legítima", la naturaleza misma del armamento de información puede introducir nuevos desafíos para este concepto ético, ya que, para desplegar una campaña de guerra de información en el ciberespacio no se requiere de los mismos niveles de fuerzas requeridos en guerras de primera, segunda, tercera e incluso guerras de cuarta generación. Por lo tanto, el monopolio estatal sobre la guerra reflejado en el principio de "autoridad legítima", ya de por sí desafiada en guerras de cuarta generación, termina por ser afectada en guerras de quinta generación, en la medida en que actores no estatales e individuos adquieren capacidades para participar en una guerra de información.

De acuerdo con Arquilla (1999), ello puede reflejar un fenómeno general en el que "la revolución de la información está provocando una difusión del poder desde los Estados hacia actores no estatales, la sociedad civil y organizaciones criminales transnacionales" (p. 387). Esta facilidad para participar de la guerra de la información no solamente erosiona las restricciones basadas en el principio de "autoridad legítima", sino también evidencia que la convención sobre ir a la guerra como "último recurso" se torna confuso. A pesar de que la guerra de información puede desestabilizar la seguridad nacional de un Estado, produce poca destrucción física, y "probablemente resultará en una forma de guerra que resulte solo en la pérdida incidental de vidas" (Arquilla, 1999, p. 388). En este sentido, Arquilla (1999) señala que la guerra de la información puede guardar semejanza con las sanciones económicas como herramienta de coerción; sin embargo, al igual que con las sanciones económicas, ciertas acciones no letales de la guerra de información pueden no considerarse actos

25 Con este supuesto, las actividades de espionaje que se efectúan en tiempo de paz y que hoy dependen en gran medida del ciberespacio, por ejemplo, serían una operación de información que no forma parte de la guerra de la información, a no ser que se lleve a cabo durante una crisis o un conflicto armado.

de guerra y, por lo tanto, pueden estar exentas de consideraciones de la tradición de guerra justa.

Con respecto a la aplicación del *jus in bello* a la guerra de información, Schmitt (2002) advierte que el primer problema es determinar si un ataque cibernético está sujeto al derecho humanitario. Con base en lo anterior, Schmitt (2002) afirma que no existe disposición alguna en ningún instrumento de Derecho Internacional Humanitario que reglamente directamente las operaciones de información[26], debido a que: (1) los ataques cibernéticos se originaron con posterioridad a la creación del derecho convencional vigente, "por lo cual las Partes no los tuvieron en cuenta para incluirlos en esos instrumentos" (p. 368)[27], y (2) dado que el Derecho Internacional Humanitario está concebido para reglamentar los métodos y medios de guerra que son cinéticos por naturaleza, los ataques informáticos quedaron por fuera del ámbito del Derecho Internacional Humanitario, debido a que la acción ofensiva a través de una red informática no es "armada" o "cinética", al menos en la concepción tradicional del derecho internacional[28].

En relación con este último argumento, si el "conflicto armado" es la condición que activa el *jus in bello*, ¿cómo aplicar el Derecho Internacional Humanitario a las acciones ofensivas a través de redes informáticas, si estas no se desarrollan necesariamente mediante ataques cinéticos? En los Convenios de Ginebra de 1949 (Comité Internacional de la Cruz Roja [Cicr], 2012a) y en los Protocolos Adicionales de 1977 (Cicr, 2012b) se considera como

26 No obstante, Schmitt (2002) advierte asimismo que el hecho de que los convenios existentes no mencionen los ataques cibernéticos es poco significativo, ya que la cláusula de Martens del artículo 1.° del Protocolo Adicional I del 12 de diciembre de 1977 a los Convenios de Ginebra del 12 de agosto de 1949, relativo a la protección de las víctimas de los conflictos armados internacionales, estipula que, cuando una situación no esté prevista en un acuerdo internacional, "las poblaciones y los beligerantes quedan bajo la salvaguardia y el imperio de los principios del derecho de gentes, tales como resultan de los usos establecidos entre las naciones civilizadas, de las leyes de humanidad y de las exigencias de la conciencia pública" (Roberts & Guelff, 2000, p. 67). En otras palabras, que todo lo que ocurra durante un conflicto armado estaría sujeto a la aplicación de los principios del Derecho Internacional Humanitario.

27 Sin embargo, Schmitt (2002) también considera que este sería un argumento equivocado, ya que, en relación con las armas nucleares, desarrolladas también con posterioridad a la creación del Derecho Internacional Humanitario, la Corte Internacional de Justicia "rechazó de plano la afirmación de que, dado que los principios y normas humanitarios se han desarrollado antes que la invención de las armas nucleares, el Derecho Humanitario es inaplicable a estas" (p. 370).

28 Empero, nadie negaría, por ejemplo, que la guerra biológica o química (que no implica el empleo de armas cinéticas) está sujeta al Derecho Internacional Humanitario (Schmitt, 2002).

"conflicto armado" todo aquel conflicto en el que necesariamente intervienen unas "fuerzas armadas"; con base en lo anterior, los "conflictos armados internacionales" se presentan cuando se recurre a la fuerza armada entre dos o más Estados, y los "conflictos armados no internacionales" se caracterizarían por los enfrentamientos armados prolongados entre una fuerza armada gubernamental y las fuerzas de uno o más grupos armados, o entre estos grupos armados, en el interior del territorio jurisdiccional de un Estado (Cicr, 2008).

Empero, una disputa que da lugar a la intervención de las fuerzas armadas no puede ser el único criterio para calificar un conflicto como "armado". De acuerdo con Schmitt (2002), un conflicto armado ocurre cuando un "grupo toma medidas que causan muertos, heridos, daños o destrucción" (p. 373), aunque en la opinión jurídica predominante en la actualidad, acciones esporádicas o aisladas de ese tipo no serían suficientes para constituir un conflicto armado[29]. En el caso de los conflictos armados internacionales, las acciones deben ser atribuibles a un Estado, lo cual, como ya se ha advertido con anterioridad, es muy complejo en el ámbito del ciberespacio, así como en la naturaleza sutil y encubierta de la guerra de la información. En consecuencia, si los principios del Derecho Internacional Humanitario se aplican siempre y cuando los ataques cibernéticos puedan ser atribuidos a un Estado, no sean incidentes aislados y esporádicos, y tengan por objeto causar heridos, muertos, daños o destrucción, la guerra de información puede burlar las restricciones y normas consignadas en el derecho internacional.

En la guerra de la información también resulta complejo discernir quién es un "combatiente"[30] y qué se considera un "acto de guerra". Por el contrario, en guerras de primera, segunda y tercera generación está bastante claro que quien realiza los ataques son las fuerzas militares enemigas de un Estado-nación. Y si bien en las guerras de cuarta generación la distinción de quién se considera un combatiente es confusa debido a que los civiles a menudo terminan parti-

29 Además, el Derecho Internacional Humanitario no se aplicaría a acciones como la disrupción temporal del servicio de internet, el espionaje cibernético, la manipulación digital de datos financieros, una campaña de desinformación en redes sociales, porque, aunque podrían formar parte de una campaña sistemática de ciberguerra, las consecuencias previsibles no incluirían muertos, heridos, daños o destrucción.

30 Para el Derecho Internacional Humanitario, un "combatiente" es un miembro de las fuerzas armadas que participa directamente en las hostilidades y no forma parte del personal médico ni religioso.

cipando en la lucha, en las guerras de quinta generación casi cualquier persona puede participar activamente en la guerra, sobre todo si esta se libra en el escenario informativo, social y cognitivo. Además, en el contexto de las guerras de quinta generación, algunos Estados han optado por subcontratar con las compañías militares y de seguridad privadas (Álvarez, 2017) diversas funciones de guerra convencional y guerra de la información, por ejemplo la protección de infraestructura física o la conducción de operaciones informáticas, entre muchos otros.

Además, suele suceder que los ataques cibernéticos se encomienden a organismos de los gobiernos que no son necesariamente militares, de manera que los contratistas civiles que desempeñan un papel activo o de apoyo en la conducción de estas operaciones podrían ser objetivos directos de ataque militar (Schmitt, 2002). Por lo tanto, desde una perspectiva ética, resulta necesario hacer una distinción entre quienes tienen acceso a la tecnología de la información avanzada y quienes utilizan dicha tecnología para librar una guerra de información; asimismo, comprender que la naturaleza de los ataques cibernéticos son tan variados que a menudo puede ser difícil diferenciar entre acciones militares, terroristas y criminales.

> En consecuencia, el imperativo ético asociado a estas preocupaciones es la necesidad de determinar la identidad de los perpetradores de ataques de guerra de información y de hacer una distinción entre depredaciones esporádicas y acciones que forman parte de una campaña reconocible en pos de objetivos discernibles. (Arquilla, 1999, p. 386)

Sin embargo, Schmitt (2002) señala que a pesar de los avances en los medios de guerra, especialmente de la guerra de la información, "no basta con valerse de un umbral basado en los actores para poder aplicar el Derecho Internacional Humanitario, por lo cual sería más apropiado recurrir a un umbral basado en las consecuencias" (p. 375). A partir del razonamiento del umbral basado en las consecuencias, en el contexto de un conflicto armado, hacer padecer hambre o asfixia, bombardear o incluso lanzar ataques cibernéticos son actos sujetos al Derecho Internacional Humanitario porque tienen consecuencias particulares; por consiguiente, para Schmitt (2002), esto contradeciría cualquier afirmación de que los ataques cibernéticos no están sujetos

al Derecho Internacional Humanitario, así no los lleve a cabo una "fuerza armada"[31].

Es evidente que, en una campaña de ciberguerra, cualquier ataque cibernético que tenga como intención ocasionar muertos, heridos o daños está sujeto al Derecho Internacional Humanitario. En efecto, el artículo 48.º del Protocolo Adicional I de los Convenios de Ginebra de 1949 estipula que "las Partes en conflicto […], dirigirán sus operaciones únicamente contra objetivos militares" (Comité Internacional de la Cruz Roja, 2012b, art. 48.º); entonces, el artículo 48.º parecería excluir toda operación militar dirigida contra cualquier objetivo que no sea militar. No obstante, en los artículos 51.º y 52.º del mismo Protocolo se establecen proscripciones que están expresadas en términos de "ataques", y no explícitamente de "ataques militares". Y el término *ataque* está abiertamente definido en el artículo 49.º: "Se entiende por 'ataques' los actos de violencia contra el adversario, sean ofensivos o defensivos" (Cicr, 2012b, art. 49). Por ende, "la prohibición no se refiere tanto al hecho de elegir objetivos no militares, como al de atacarlos específicamente mediante el empleo de la violencia" (Schmitt, 2002, p. 377); empero, como el artículo 48.º lo que prohíbe es cualquier ataque contra objetivos no militares cuya finalidad sea causar muertos, heridos, daños o destrucción, a la luz del derecho internacional aquellos ataques cibernéticos que no generen las consecuencias indeseadas expresadas en el artículo 48.º están permitidos contra objetivos no militares, incluyendo la misma población.

Esta reflexión cobra interés por el suceso que se presentó entre el mes de marzo y diciembre de 2020, en el cual un número creciente de agencias gubernamentales de los Estados Unidos, como los departamentos de Estado, Tesoro, Comercio, Defensa, Seguridad Nacional y Energía, así como los institutos nacionales de salud de ese país fueron víctimas de lo que podría conside-

31 Un enfoque de la guerra de información es atacar las infraestructuras de transporte, energía, comunicaciones y financieras de un adversario a través del ciberespacio. Esto debería contemplarse como un "acto de guerra" que tiene como objetivo deliberado los "no combatientes", ya que será la población civil la que en últimas sufrirá las principales consecuencias de dichos ataques. El propósito de este tipo de guerra de información es socavar la voluntad del enemigo de resistir o persistir en la guerra; en este sentido, la guerra de información estratégica es muy similar a las primeras nociones del bombardeo estratégico de la teoría del poder aéreo en la Segunda Guerra Mundial, orientado principalmente a bombardear la infraestructura crítica y la población civil del adversario (Álvarez *et al.*, 2019).

rarse el mayor ataque cibernético realizado en contra de esa superpotencia en la historia. El ataque fue perpetrado mediante la corrupción del software de SolarWinds Orion (2020), la cual permite al personal de las tecnologías de la información acceder de forma remota a las computadoras en las redes corporativas. Los piratas informáticos manipularon las actualizaciones de software del sistema Orion de SolarWinds para introducir un malware que, una vez instalado, permitió a los *hackers* monitorear los sistemas de redes de sus clientes, entre los cuales está el gobierno y compañías estratégicas norteamericanas.

Según las primeras investigaciones, el ataque fue realizado probablemente por la Federación de Rusia, a través del empleo de un grupo privado de *hackers* rusos conocidos como Apt 29 (un subcontratista de las agencias de inteligencia rusas), con la intención de perpetrar un ataque estrecho, extremadamente dirigido y manualmente ejecutado ("SolarWinds Orion: More US government agencies hacked", 2020). Y al parecer, los piratas informáticos tuvieron acceso durante ocho meses a SolarWinds antes de que fuesen detectados, de manera que contaron con suficiente tiempo para espiar y robar material sensible de las agencias gubernamentales estadounidenses y empresas sensibles para la seguridad nacional de Estados Unidos, como Microsoft. Si bien es poco probable que se hayan violado las comunicaciones gubernamentales de alto nivel (ya que estas son altamente encriptadas y se envían en sistemas separados), los *hackers* de Apt 29 y la Fsb rusa seguramente tuvieron acceso a importantes documentos operativos, fragmentos de información o incluso claves digitales[32]. No obstante, y con base en el artículo 48.º del Protocolo Adicional I de los Convenios de Ginebra de 1949, este ataque no viola el derecho internacional, ya que, aunque fue dirigido también contra objetivos no militares, no causó muertos, heridos, daños o destrucción, pero es sin lugar a duda una acción militar que forma parte de la actual guerra de información entre Estados Unidos y Rusia[33].

32 La Agencia de Infraestructura y Ciberseguridad de los Estados Unidos afirma que tomará varios años comprender la total dimensión de la afectación de esta intrusión a la seguridad nacional.

33 No obstante, Rid (2011) ha objetado que ningún caso de conflicto cibernético, incluido el que acaba de mencionarse, puede clasificarse como un acto de guerra.

Otro tema complicado en la aplicabilidad de la tradición de guerra justa a las guerras de quinta generación (y particularmente a la guerra de información), lo plantea el principio de "proporcionalidad", cuya preocupación principal es conjurar el uso excesivo de la fuerza durante un conflicto armado. En apariencia, la guerra de información permitiría hacer la guerra de manera proporcional, ya que los ataques de esta índole son de cierto modo muy precisos y calculados; sin embargo, en la guerra de información se puede llegar a atacar civiles o bienes protegidos por el derecho internacional[34]. Según Schmitt (2002), el principio de "proporcionalidad" que rige las situaciones en las que dañar a personas o bienes protegidos es la consecuencia previsible de un ataque (pero no el fin buscado), es violado de manera recurrente, aunque en forma no intencional, por falta de entendimiento suficiente de aquello que se está atacando, por la incapacidad de medir quirúrgicamente la cantidad de "fuerza" que se va a aplicar contra un objetivo, y/o por la incapacidad de conseguir que el arma golpee con total precisión en el objetivo seleccionado; y estas situaciones pueden presentarse en los ataques cibernéticos.

Por efectos de todo lo anterior, Arquilla y Ronfeldt (2001) plantean la pregunta de cuándo se podrían utilizar medidas militares convencionales, incluida fuerza cinética, en respuesta a ataques de guerra de información, sin violar las nociones de proporcionalidad[35]. Pues bien, los pensadores estratégicos rusos consideran que amenazar a los atacantes de la guerra de información con variadas represalias, como el uso de armas de destrucción masiva, es un curso de acción aceptable[36]. Arquilla (1999) cita al analista de defensa ruso Vladimir Tsymbal, quien en un discurso denominado "Concepts of Information Warfare", y presentado en la conferencia sobre evolución de los

34 La prohibición de atacar a los civiles o bienes de carácter civil se estipula explícitamente en el Protocolo I a los Convenios de Ginebra de 1949. En efecto, se establece que "no serán objeto de ataque la población civil como tal ni las personas civiles. Quedan prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil" (Cicr, 2012b, art. 51.º), y "los bienes de carácter civil no serán objeto de ataque ni de represalias" (Cicr, 2012b, art. 52.º). Por ende, para el derecho internacional son civiles aquellos que no son considerados combatientes, y son bienes protegidos todo bien que no es un objetivo militar.

35 O si el objetivo que fuese víctima de un ataque de guerra de información tuviera pocos o ningún medio de responder con armamento de guerra de información.

36 Por ende, la sugerencia de Schelling (1966) de que respuestas variadas pueden resolver un dilema de proporcionalidad podría llegar a generar un nuevo dilema: que la respuesta asimétrica de represalia puede tender a la escalada.

problemas de seguridad nacional posteriores a la Guerra Fría, celebrada en Moscú en 1995, declaraba que

> desde un punto de vista militar, el uso de medios de guerra de información contra Rusia o sus fuerzas armadas no se considerará categóricamente como una fase no militar del conflicto, haya habido o no víctimas [...], considerando las posibles consecuencias catastróficas que tendrían en los sistemas económicos, en los sistemas de mando y control estatales, o en el potencial de combate de las fuerzas armadas. Por lo tanto, Rusia se reserva el derecho a utilizar armas nucleares primero contra los medios y fuerzas de la guerra de información, y luego contra el propio Estado agresor. (Tsymbal; citado por Arquilla, 1999, p. 390)

Otro tema de interés en relación con la aplicación del principio de "proporcionalidad" en guerras de información es el de las repercusiones ulteriores o efectos "secundarios", es decir, aquellos que no son directa e inmediatamente causados por un ataque, pero sí se derivan de dicho ataque. Un ejemplo fue el ataque contra el sistema eléctrico de Iraq durante la Guerra del Golfo (1990-1991), que si bien logró interrumpir el C2 de las fuerzas armadas de Sadam Hussein, también privó de electricidad al sistema hospitalario y a los servicios de emergencia en ese país ("primer efecto"). Asimismo, por falta de electricidad en los hogares de la población iraquí, se causó un mayor sufrimiento de la población civil ("segundo" efecto), en una situación que ya de por sí era bastante apremiante. Como lo afirma Schmitt (2002), el problema de los efectos en cadena es incluso mayor en un ataque cibernético, "habida cuenta de la conectividad entre los ordenadores, en particular entre los sistemas militares y civiles" (p. 393)[37].

Conclusiones

La guerra de quinta generación plantea algunos dilemas para la tradición de guerra justa, ya que, para aplicar las disposiciones existentes a la guerra de información, sería ineludible adherirse a varias premisas interpretativas.

37 Los efectos ulteriores, cuando son causados por un ataque cibernético, son difíciles de evaluar, si no se sabe cómo funcionan los sistemas informáticos implicados y con qué otros sistemas están vinculados.

Según Schmitt (2002), de la mayor importancia serían las interpretaciones de "conflicto armado" y de "ataque" basadas en las consecuencias, debido a que la falta de tales interpretaciones "cuestionaría la aplicabilidad y, por ende, la adecuación de los actuales principios del Derecho Internacional Humanitario" (p. 396). Efectivamente, como los ataques cibernéticos pueden no equivaler a un ataque militar, abren muchas posibilidades para atacar civiles y bienes protegidos, siempre y cuando no causen muertos, heridos, daños o destrucción; como los ataques cinéticos durante las operaciones militares clásicas suelen tener tales efectos, las personas civiles y los bienes de carácter civil gozan de amplia protección durante guerras del tipo de primera, segunda, tercera y cuarta generación.

Además, el sesgo del Derecho Internacional Humanitario a considerar un "ataque" como una ofensiva de naturaleza cinética, invita al empleo de ataques de información o desinformación carentes de efectos cinéticos, en contra de la población civil de un Estado antagonista, con el objetivo de incitarla a presionar a sus dirigentes a fin de que estos se comporten (o dejen de comportarse) de cierto modo[38]. Tales han sido los casos de las protestas sociales en noviembre de 2019, septiembre de 2020 y abril-mayo de 2021 en Colombia, que derivaron en violencia, saqueos y vandalización en varias ciudades del país; aparentemente, parte de las campañas de desinformación y polarización que eventualmente condujeron a tales actos violentos y destructivos fueron orquestadas por agencias de inteligencia en Rusia y Venezuela. La vicepresidenta de Colombia, Marta Lucía Ramírez, denunció este hecho:

> Sabemos que hay un proyecto internacional, sabemos que hay una red de apoyo internacional para estimular este malestar social. Tenemos certeza de que hay plataformas que desde Venezuela y desde Rusia han venido moviendo buena parte de todos estos mensajes en las redes sociales ("Vicepresidenta afirma que Rusia está detrás de los mensajes que motivan las marchas en Colombia", 2019).

38 Empero, "el mero hecho de que un objetivo pueda ser atacado por un medio no cinético no significa que las normas de Derecho Humanitario sean inaplicables" (Schmitt, 2002, p. 397), ya que los civiles y sus bienes siguen gozando de un estatuto de protección contra los aspectos de la ciberguerra que causen sufrimiento humano y daños físicos. Incluso, cuando se llevan a cabo ataques cibernéticos contra objetivos militares, el principio de proporcionalidad sigue protegiendo a las personas civiles y a los bienes de carácter civil de los perjuicios y los daños excesivos en relación con la ventaja militar, como interrumpir el suministro de electricidad a una ciudad para alterar la cadena de C3 del enemigo.

Como se ha evidenciado, y ante variados instrumentos y tácticas que comprometen la guerra de información, como cibervandalismo, hacktivismo, delitos cibernéticos, espionaje comercial e industrial, espionaje militar, actos de sabotaje y guerra cibernética propiamente dicha, no es sorpresa que exista una falta de consenso por parte de especialistas y académicos para distinguir y clasificar cuáles de estas acciones violan o no los principios de la tradición de guerra justa. Por lo tanto, y como lo señala Lucas (2015), "una característica muy crítica del advenimiento de la ciberguerra es que ha borrado las distinciones entre lo que alguna vez fueron niveles muy diferentes de actividad y conflicto, haciendo que el análisis moral apropiado sea mucho más difícil" (p. 251).

Además, como el empleo de armas y tácticas de las guerras de información han estado bajo el control de las agencias de inteligencia estatales, cuyas reglas de enfrentamiento son radicalmente diferentes de las de los combatientes militares convencionales, aplicar la tradición de guerra justa a estas actividades se torna engorroso (Taddeo, 2012). Asimismo, los agentes de inteligencia generalmente se dedican a actividades que, según el derecho internacional, no alcanzan el nivel de "acto de guerra", sino que, en cambio, y en el mejor de los casos, solo constituyen actos delictivos en la jurisdicción interna del sitio en donde se han llevado a cabo.

En resumen, la guerra de información parece ser una guerra sin restricciones llevada a cabo por agentes de inteligencia y espionaje que no se creen sujetos a restricciones legales, ni piensan en sus acciones como lo hacen los combatientes convencionales entrenados en el Derecho Internacional de los Conflictos Armados (Lucas, 2015). La guerra sin restricciones no es legalmente permisible ni moralmente justificable en el caso de la tradición de guerra justa, pero es una práctica rutinaria en las guerras de quinta generación, en la cual una plétora de armas y tácticas están diseñadas específicamente para operar contra civiles y objetivos civiles (no combatientes), una característica que sería ilegal, y decididamente inmoral, en las guerras de primera, segunda, tercera y cuarta generación.

Pero es innegable que la guerra de información puede facilitar la satisfacción de los intereses nacionales de un Estado o el cumplimiento de los objetivos militares deseados, con menos daños colaterales y perjuicios incidentales

que un ataque cinético tradicional. Asimismo, su relación costo-beneficio es más atractiva que el empleo de medios convencionales de guerra, los cuales no solo demandan mayores recursos económicos y humanos, sino también acarrean mayores riesgos políticos. En consecuencia, la guerra de información será cada vez más la regla general de la guerra posmoderna, y no su excepción, de manera que es absolutamente fundamental revisar continuamente los principios éticos de la tradición de guerra justa y las normas del Derecho Internacional Humanitario para actualizarlos a la dinámica de los conflictos del presente y a su prospectiva evolutiva en el futuro inmediato.

Referencias

Álvarez, C. (2017). Guerra Corp. ¿Prohibición o regularización de las compañías militares y de seguridad privada?: Un desafío para el Derecho Internacional Humanitario. En L. Vélez & D. Rodríguez (eds.), *Sociedad y fuerza pública ante los retos de la paz: Nuevas amenazas, Derechos Humanos y relaciones cívico-militares en el contexto colombiano* (pp. 55-86). Ibáñez.

Álvarez, C., Barón, P., & Monroy, V. (2018). Poder astuto: Estrategia del empleo del poder en el siglo XXI. En C. Álvarez & A. Fernández (eds.), *Hacia una gran estrategia en Colombia: construcción de política pública en seguridad y defensa* (pp. 171-268). Sello Editorial ESMIC.

Álvarez, C., Benavides, E., & Ramírez, Y. (2019). Geopolítica del espacio exterior: Dominio estratégico del siglo XXI para la seguridad y defensa. En C. Álvarez & C. Corredor (eds.), *El espacio exterior: Una oportunidad infinita para Colombia* (vol. 1: *Mirando hacia las estrellas: una constante necesidad humana*; pp. 99-220). Fuerza Aérea Colombiana.

Álvarez, C., & Duque, F. (2020). Oportunidades para las Fuerzas Militares de Colombia en operaciones multidimensionales de mantenimiento de paz. *Revista Científica General José María Córdova*, *18*(29), 87-109. https://doi.org/10.21830/19006586.542

Álvarez, C., & Ramírez, Y. (2020). La cuarta revolución industrial y la era de la inteligencia artificial: Implicaciones para la seguridad y el trabajo. En Y. Rico, D. López & A. Cerón (comps.), *Enfoques y gestión en seguridad integral* (pp. 209-238). Escuela de Posgrados Fuerza Aérea Colombiana.

Álvarez, C., Santafé, J., & Urbano, O. (2017). Metamorphosis bellum: ¿mutando a guerras de quinta generación? En C. Álvarez (ed.), *Escenarios y desafíos de la seguridad multidimensional* (pp. 145-248). Escuela Superior de Guerra.

Aristóteles. (2004). *The Nicomachean ethics*. Penguin.

Arquilla, J. (1999). Ethics and information warfare. En Z. Khalilzad, J. White & A. Marshall (eds.), *Strategic appraisal: The changing role of information warfare* (pp. 379-401). RAND Corporation.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141-65.

Arquilla, J., & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. RAND Corporation.

Bellamy, A. (2009). *Just wars: From Cicero to Iraq*. Polity Press.

Brenner, J. (2011). *America the vulnerable: Inside the new threat matrix of digital espionage, crime, and warfare*. Penguin Press.

Brough, M., Lango, J., & Van der Linden, H. (2007). Appendix just war principles: An introduction. En M. Brough, J. Lango & H. van der Linden (eds.), *Rethinking the just war tradition* (pp. 243-250). State University of New York Press.

Bunker, R. (2000). Unrestricted warfare: Review essay I. *Small Wars & Insurgencies*, *11*(1), 114-121.

Carr, J. (2011). *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly Media, Inc.

Clarke, R., & Kanke, R. (2010). *Cyber war: The next threat to national security and what to do about it*. HarperCollins.

Clifford, G. (2012). Jus post bellum: Foundational principles and a proposed model. *Journal of Military Ethics*, *11*(1), 42-57.

Comité Internacional de la Cruz Roja [CICR]. (2008). ¿Cuál es la definición de "conflicto armado" según el Derecho Internacional Humanitario? https://www.icrc.org/es/doc/assets/files/other/opinion-paper-armed-conflict-es.pdf

Comité Internacional de la Cruz Roja [CICR]. (2012a). *Los Convenios de Ginebra del 12 de Agosto de 1949*. Comité Internacional de la Cruz Roja. https://www.icrc.org/es/doc/assets/files/publications/convenios-gva-esp-2012.pdf

Comité Internacional de la Cruz Roja [CICR]. (2012b). *Protocolos Adicionales a los Convenios de Ginebra de 1949*. Comité Internacional de la Cruz Roja. https://www.icrc.org/es/doc/assets/files/publications/icrc-003-0321.pdf

Coppieters, B., & Fotion, N. (2002). *Moral constraints on war: Principles and cases*. Lexington Books.

Cortés, D., & Garzón, T. (2017). El ciberactivismo en las revoluciones posmodernas. *Revista de Estudios en Seguridad Internacional*, *3*(1), 103-125.

Denning, D. (1998). *Information warfare and security*. Addison-Wesley.

Denning, D. (2007). The ethics of cyber conflict. En K. Himma & H. Tavani (eds.), *Information and computer ethics* (pp. 407-428). Wiley.

Dipert, R. (2010). The ethics of cyber warfare. *Journal of Military Ethics*, *9*(4), 384-410.

Dipert, R. (2013). The essential features for an ontology for cyberwarfare. En P. Yannakogeorgos & A. Lowther (eds.), *Conflict and cooperation in cyberspace* (pp. 35-48). Taylor & Francis.

Dunlap, C. (2011). Perspectives for cyber strategists on law for cyberwar. *Strategic Studies Quarterly*, *5*(1), 81-99.

Ellis, G. (2003). *The Napoleonic Empire*. Palgrave Macmillan.

Evans, M. (2008). Balancing peace, justice and sovereignty in jus post bellum: The case of just occupation. *Millennium Journal of International Studies*, (36), 533-554.

Floridi, L. (1999). Information ethics: On the philosophical foundations of computer ethics. *Ethics and Information Technology*, *1*(1), 37-56.

Floridi, L. (2005). Information ethics: Its nature and scope. *Computers and Society*, *36*(3), 21-36.

Floridi, L. (2007). Foundations of information ethics. En K. Himma & H. Tavani (eds.). En *Information and computer ethics* (pp. 3-24). Wiley.

Floridi, L. (2010). Ethics after the Information Revolution. En L. Floridi (ed.), The *Cambridge handbook of information and computer ethics* (pp. 3-19). Cambridge University Press.

Floridi, L., & Taddeus, M. (eds.). (2014). *The ethics of information warfare*. Springer Verlag.

Frost, M. (2006). Ética y guerra: Más allá de la teoría de la guerra justa. *Relaciones Internacionales*, (3), 1-27.

Gelven, M. (1994). *War and existence*. Pennsylvania State University Press.

Grocio, H. (1925). *De la guerra y de la paz*. Reus.

Johnson, L. (1997). Toward a functional model of information warfare: A major intelligence challenge. *Studies of Intelligence*, (1), 49-55.

Keegan, J. (1990). *The Second World War*. Penguin.

Kuehl, D. (2002). Information operations, information warfare, and computer network attack: Their relationship to national security in the information age. *International Law Studies*, (76), 35-58.

Liang, Q., & Xiangsui, W. (1999). *Unrestricted warfare*. PLA Literature and Arts Publishing House.

Lind, W., Nightengale, K., Schmitt, J., Sutton, J., & Wilson, G. (1989). The changing face of war: Into the Fourth Generation Warfare. *Marine Corps Gazette*, *73*(10), 22-26.

Lucas, G. (2013). Jus in silico: Moral restrictions on the use of cyber warfare. En F. Allhoff, N. Evans & A. Henschke (eds.), *The Routledge handbook of war and ethics* (pp. 367-80). Routledge.

Lucas, G. (2014). Permissible preventive cyber warfare. En T. Floridi & M. Taddeo (eds.), *The ethics of information warfare* (pp. 73-84). Springer Verlag.

Lucas, G. (2015). Cyber warfare. En J. Turner & E. Patterson (eds.), *The Ashgate Research Companion to Military Ethics* (pp. 245-258). Ashgate Publishing Limited.

Molander, R., Riddile, A., & Wilson, P. (1996). *Strategic information warfare: A new face of war*. RAND Corporation.

Nichiporuk, B. (1999). U. S. military opportunities: Information-warfare concepts of operation. En Z. Khalilzad, J. White & A. Marshall (eds.), *Strategic appraisal: The changing role of information warfare* (pp. 187-223). RAND Corporation.

Orend, B. (2014). Fog in the fifth dimension: The ethics of cyber-war. En T. Floridi & M. Taddeo (eds.), *The ethics of information warfare* (pp. 3-24). Springer Verlag.

Patterson, E. (2007). Jus post bellum and international conflict: Order, justice, and reconciliation. En M. Brough, J. Lango & H. van der Linden (eds.), *Rethinking the just war tradition* (pp. 35-52). State University of New York Press.

Platón. (2014). *Las leyes*. Alianza Editorial.

Reed, D. (2008). Beyond the war on terror: Into the fifth generation of war and conflict. *Studies in Conflict & Terrorism*, *31*(8), 684-722.

Reichberg, G. (2002). Just war or perpetual peace? *Journal of Military Ethics*, *1*(1), 16-35.

Rid, T. (2011). Cyber war will not take place. Journal of Strategic Studies, *35*(1). 5-32.

Roberts, A., & Guelff, R. (2000). *Documents on the laws of war*. Oxford University Press.

Rodin, D. (2003). *War and self-defense*. Oxford University Press.

Rosenzweig, P. (2013). *Cyber warfare: How conflicts in cyberspace are challenging America and changing the world*. Praeger.

Rousseau, J. J. (1927). *A proyect for perpetual peace*. Richard Cobden-Sanderson.

Rowe, N. (2007). War crimes from cyberweapons. *Journal of Information Warfare*, *6*(3), 15-25.

Rowe, N. (2008). Ethics of cyber war attacks. En L. Janczewski & A. Colarik (eds.), *Cyber warfare and cyber terrorism* (pp. 105-111). Information Science Reference.

Rowe, N. (2010). The ethics of cyberweapons in warfare. *Journal of Techoethics*, *1*(1), 20-31.

Rowe, N. (2011). Toward reversible cyber-attacks. En J. Ryan (ed.), *Leading Issues in Information Warfare and Security Research* (pp. 145-58). Academic Publishing.

San Agustín. (1946). *Sobre el libre arbitrio*. BAC.

Santo Tomás de Aquino. (2002). *Political writings*. Cambridge University Press.

Schelling, T. (1966). *Arms and influence*. Yale University Press.

Schmitt, M. (1999). Computer network attack and the use of force in international law: Thoughts on a normative framework. *Columbia Journal of Transnational Law*, *37*, 885-937.

Schmitt, M. (2002). Wired warfare: computer network attack and jus in bello. *International Review of the Red Cross*, *84*(846), 365-399.

Schmitt, M. (2011). Cyber operations and the jus in bello: Key issues. *U.S. Naval War College International Law Studies*, (87), 89-110.

Schmitt, M. (ed.). (2013). *The Tallinn Manual on the International Law applicable to cyber warfare*. Cambridge University Press.

Schuck, M. (1994). When the shooting stops: Missing elements in just war theory. *Christian Century*, (26), 982-984 .

Singer, P., & Friedman, A. (2014). *Cyber security and cyber war: what everyone needs to know*. Oxford University Press.

SolarWinds Orion: More US government agencies hacked. (2020, diciembre 15). *BBC*. https://www.bbc.com/news/technology-55318815

Sun Tzu. (2012). *El arte de la guerra*. Shambhala.

Taddeo, M. (2012). Information warfare: A philosophical perspective. *Philosophy & Technology*, (25), 105-120.

Tse-Tung, M. (1954). *On protracted war*. People's Publishing House.

Toffler, A., & Toffler, H. (1993). *War and anti-war: Survival at the dawn of the 21st Century*. Little, Brown & Company.

Van Creveld, M. (1991). *The transformation of war: The most radical reinterpretation of armed conflict since Clausewitz*. Free Press.

Vicepresidenta afirma que Rusia está detrás de los mensajes que motivan las marchas en Colombia. (2019, diciembre 12). *Semana*. https://www.semana.com/nacion/articulo/vicepresidenta-afirma-que-rusia-esta-detras-de-los-mensajes-que-motivan-las-marchas-en-colombia/644594/

Walzer, M. (2000). *Just and unjust wars: A moral argument with historical illustrations*. Basic Books.

White, M. (2012). *El libro negro de la humanidad*. Crítica.