Capítulo 5

El poder en la era digital: perspectivas sobre el ciberpoder*

DOI: https://doi.org/10.25062/9786287602700.05

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

Resumen: Este capítulo analiza las dinámicas que tienen lugar en el ciberespacio; expone cómo empieza a hablarse de ciberpoder en el ámbito general del poder; examina las acepciones del término de acuerdo con diferentes perspectivas regionales y en el entendido de que se define según como se comprenda y dónde se localice; describe el poder desde la perspectiva militar de EE. UU. y desde la óptica de la Unión Europea, y amplía la comprensión del ciberpoder, a partir de su localización, todo lo cual apunta a establecer estimaciones adecuadas de este objeto de estudio.

Palabras clave: ciberconflicto; ciberespacio; ciberpoder; ciberseguridad; poder.

* Capítulo de libro resultado del proyecto de investigación "*Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio*", del grupo de investigación *"Ciberespacio Tecnología e Innovación"*, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no necesariamente reflejan los de las instituciones participantes.

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

Citación APA: Realpe Díaz, M. E. (2024).El poder en la era digital: perspectivas sobre el ciberpoder. En M. E. Realpe Díaz, & A. M. González González (Eds.), *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio* (pp. 143-166). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602700.05

TECNOLOGÍAS DISRUPTIVAS, LOGÍSTICA Y SEGURIDAD Y DEFENSA NACIONAL EN EL CIBERESPACIO
ISBN impreso: 978-628-7602-69-4
ISBN digital: 978-628-7602-70-0
DOI: https://doi.org/10.25062/9786287602700

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2024

Introducción

La revolución tecnológica de los últimos años del siglo XX tuvo un impacto profundo en la forma en que las personas se relacionan entre sí y perciben el mundo que les rodea. La llegada de la internet y la digitalización de la información revolucionaron la forma en que la información se transmitía y se procesaba. Por su parte, la revolución de las tecnologías de la información actuó remodelando las bases materiales de una nueva sociedad. Las tecnologías de la información se tornaron en herramientas indispensables para la generación de riqueza, el ejercicio del poder y la creación de códigos culturales (López, 2002). De acuerdo con Castells, este tiempo donde ocurrió la revolución tecnológica correspondió a un intervalo histórico, durante el cual el desarrollo alcanzado por las tecnologías de la información ocasionó un cambio en la cultura material de la sociedad, pues influyó de manera considerable en las distintas actividades realizadas por el hombre, no como una fuente exógena de afectación sino directa (Castells, 2001, p. 112).

Adicionalmente, el desarrollo e implementación de las tecnologías provocó una transformación acelerada de la base material de la sociedad, que afectó profundamente la forma en que las personas se relacionan entre sí y perciben el mundo que les rodea, dando lugar a la *sociedad de la información,* lo que significa que estas tecnologías están presentes en la vida diaria de las personas y son utilizadas en una variedad de actividades, desde el trabajo y la educación hasta el entretenimiento y la comunicación interpersonal. Como lo afirma Estudillo, se trata de una sociedad en la que las nuevas tecnologías y la información afectan la estructura social en diferentes ámbitos de la vida de los seres humanos como la economía y el bienestar social (2002, pp. 83-84). Asimismo, Castells (1996) sostiene que las tecnologías de la información y la comunicación (TIC) son la fuerza impulsora

detrás de la transformación de la sociedad, y que han permitido la creación de una economía global y la conexión en tiempo real de personas de todo el mundo.

Como lo establece Perlroth (2022), la internet como muchas otras cosas que ahora nos damos cuenta, nos ha dejado conectados de forma inextricable. Las vulnerabilidades digitales que afectan a uno afectan a todos. La barrera entre lo físico y lo digital es cada vez más insignificante. Es verdad que todo "se puede interceptar", y la mayoría de lo que nos importa ya se ha interceptado: nuestros datos personales, propiedad intelectual, empresas químicas, centrales nucleares e incluso las propias ciberarmas del país (p. 475). Con esta percepción, el progreso tecnológico y la internet son considerados factores del cambio social y, en este contexto, como lo afirman De Vergara y Trama, (2017), la internet y los desarrollos tecnológicos también han tenido un impacto significativo en el carácter de las guerras y los conflictos, así coinciden varios autores del siglo XXI, lo que reitera los postulados de Clausewitz en cuanto a que "estos son como un camaleón que cambian de carácter según sea su naturaleza, propósito, la manera en que se los conduce, la tecnología y el ambiente operacional donde tienen lugar" (p. 58).

Surge así, el ciberespacio que es el escenario común donde tienen lugar todas aquellas interacciones de orden social, comercial, industrial, tecnológico y militar entre personas, organizaciones, instituciones, bancos y ejércitos; allí, actúan también las amenazas, tanto criminales como aquellas que orientan sus esfuerzos contra la estabilidad de los Estados, vinculadas por lo general a otro país rival o enemigo. Estas acciones materializan los ciberconflictos, "un tipo de conflicto que se lleva a cabo en el ciberespacio y que puede involucrar operaciones militares, de inteligencia, de propaganda y de sabotaje, en el que los actores utilizan herramientas y técnicas cibernéticas para alcanzar sus objetivos" (Singer & Friedman, 2021, p. 2), una escalada mayor de tales hostilidades en el ciberespacio deriva en una ciberguerra, "…una forma grave de ciberataque disruptivo por parte de una nación al ciberespacio de otra nación, cruzando la línea para ser considerado un uso de la fuerza, en ese momento entran en juego cuestiones del derecho de la guerra" (Hunker, 2010, p.4). De esta manera, surge un nuevo concepto: *ciberpoder,* definido como "la capacidad de utilizar el ciberespacio para crear ventajas e influenciar eventos en todos los entornos operativos y en todos los instrumentos del poder" (Kuehl, 2009, p. 25).

Como lo define Mitchell (1995), el ciberespacio es una nueva dimensión, digital, sin fronteras, un espacio de comunicación e intercambio de información que se ha convertido en una parte integral de la vida cotidiana de muchas personas. Es una realidad en que

> las nuevas tecnologías traen oportunidades y vulnerabilidades para los países más desarrollados y al mismo tiempo contribuyen a aumentar la brecha tecnológica hacia los países en vías de desarrollo, especialmente en lo que se refiere a los campos de la seguridad y la defensa nacional. (Ferreira, 2018, p. 36)

Si bien la tecnología trajo consigo muchos beneficios, también planteó nuevos desafíos éticos, políticos y legales que aún se están tratando de abordar. Si se analizan las múltiples fuentes de información, la tecnología es cada día más accesible y permite que surjan nuevas amenazas procedentes de regímenes ilegítimos, grupos terroristas, grupos al margen de la ley y delincuencia organizada, quienes pueden tener acceso al ciberterrorismo, ciberdelincuencia, armas de destrucción masiva, mercado negro armamentístico, etc. Esto implica un cambio en la idea de la amenaza tradicional procedente de enemigos identificados (CESEDEN, 2012, p. 126).

Lo anterior divisa una gran preocupación no solo nacional sino internacional, pues si bien la relación entre la sociedad de la información y el ciberespacio ha traído grandes beneficios en términos de comunicación y globalización, también ha creado una serie de riesgos y desafíos para la sociedad y es importante que se tomen medidas para abordar estos problemas y garantizar que los beneficios de la tecnología se utilicen de manera responsable y equitativa.

Del poder al ciberpoder

Históricamente, se solía creer que la potencia de un país dependía de aspectos como su ubicación geográfica, sus recursos nacionales, el número de habitantes y su riqueza, ya que se consideraban elementos esenciales para el desarrollo del poderío militar (Tellis et al., 2009). Tradicionalmente, la capacidad de un país para salvaguardar sus fronteras de posibles ataques, a la par que exhibía la capacidad de amenazar a naciones vecinas, se percibía como el símbolo máximo de su fuerza nacional. No obstante, con la transición a la Cuarta Revolución Industrial, las concepciones sobre el poder nacional han evolucionado, incorporando el concepto de una revolución del conocimiento. Esta transformación anticipa un cambio significativo en la importancia, otorgada a la tecnología de la información y la innovación en la estructura y dinámica de la sociedad.

La evolución en la concepción del poder, desde las nociones tradicionales basadas en factores geográficos y económicos hacia un nuevo paradigma de

ciberpoder, refleja la adaptación necesaria a la Cuarta Revolución Industrial. En esta transición, la relevancia de la tecnología de la información y de la interconexión digital se convierte en un elemento crucial. La capacidad de aprovechar el ciberespacio para alcanzar objetivos estratégicos y tácticos redefine el panorama de la influencia y la seguridad en un contexto tanto nacional como internacional. A medida que las tecnologías digitales siguen evolucionando, se hace imperativo abordar esta emergente dimensión del poder en la era contemporánea, donde la tecnología y la información desempeñan un papel central en la configuración de las dinámicas de poder y las relaciones globales.

Migrar del poder al ciberpoder implica adoptar una serie de medidas y estrategias que permitan aprovechar las capacidades y recursos del ciberespacio para lograr objetivos estratégicos y tácticos. Adicionalmente, requiere una transformación significativa en la manera en que las naciones, organizaciones y actores individuales influyen en el escenario global. Esto debido a la creciente importancia de las tecnologías de información, comunicaciones y de operación, así como a la interconexión mediante internet (Kuelh, 2009). La transición de una estructura de poder convencional hacia un paradigma de ciberpoder implica la creciente preeminencia de las tecnologías digitales y el ciberespacio en la configuración de la influencia y la seguridad en un contexto tanto nacional como internacional. A medida que estas tecnologías continúan su evolución, se vuelve imperativo el análisis y la adaptación a esta emergente dimensión del poder en la era contemporánea.

En síntesis, el poder tradicional y el ciberpoder son dos conceptos que se entrelazan en la actualidad. Por una parte, todo poder puede caracterizarse como "la producción, en y por las relaciones sociales, de efectos sobre los actores que moldean su capacidad para controlar su destino" y solo se hace evidente por los efectos que tiene sobre los demás (Barnett & Duvall, 2005). Y por otra, el ciberpoder puede entenderse como la variedad de poderes que circulan en el ciberespacio y que dan forma a las experiencias de quienes actúan en el ciberespacio y por medio de él (Jordan, 1999, p. 3). El ciberpoder "no se crea simplemente para existir, sino más bien para apoyar el logro de objetivos más amplios... mediante los elementos del poder nacional: político, diplomático, informativo, militar y económico". (Kuehl, 2009, pp. 41-42). El ciberpoder es una de las últimas incorporaciones al árbol genealógico del poder, dado lo reciente que aún es la digitalización de nuestras sociedades y el surgimiento del ciberespacio.

Del ciberespacio al ciberpoder

Para trazar una evolución del ciberespacio, desde sus orígenes hasta la sociedad contemporánea es menester mencionar que este escenario es considerado un dominio estratégico debido a su capacidad para transformar la sociedad, influir en la economía y la política y afectar la seguridad y la defensa de los países. Sobre esta premisa, es preciso reconocer que *ciberespacio* es un término que viene siendo usado desde hace aproximadamente medio siglo y que, por lo tanto, es natural exponer su evolución; es así como fue presentado por primera vez en el libro *El shock del futuro,* de Alvin Toffler (1970); posteriormente, fue utilizado y recreado por William Gibson en sus obras *Burning Chrome* (1982) y *Neuromancer* (1984) y, en consecuencia, cuenta con múltiples definiciones como la establecida por Bauman: "el ciberespacio es un espacio de incertidumbre y ambigüedad, donde las identidades y las relaciones sociales pueden ser construidas y deconstruidas con facilidad" (Bauman, 2000). Para Castells,

> el ciberespacio es un espacio virtual que se extiende más allá del mundo físico, en el que los usuarios pueden interactuar, colaborar, crear y compartir información y conocimiento, y en el que la tecnología de la información y las comunicaciones juegan un papel central. (Castells, 2010, p. 69)

La historia de la humanidad es también la bitácora de las constantes confrontaciones entre civilizaciones y pueblos. La Modernidad, por su parte, trajo consigo dos guerras mundiales, posiblemente las más sangrientas hasta ahora conocidas; sin embargo, cabe conceder que estas dieron origen a diversas iniciativas formales institucionalizadas, como la ONU, y a un número importante de planteamientos teóricos que, por ejemplo, revitalizaron la romántica idea kantiana de la paz perpetua (Kant, 1795), o definieron o reforzaron las nociones y la necesidad de acatar los derechos humanos (DD. HH.), el Derecho Internacional Humanitario (DIH), las leyes de la guerra (LOW) en su expresión tradicional que divide el *Jus ad Bellum* (la decisión y causas de dar inicio a la guerra), del *Jus in Bello* (que regula la conducción durante la guerra).

La idea kantiana era romántica e incluso anacrónica; no obstante, materialmente acertada, pues la creación de una liga de naciones era una apuesta plausible, así se hubiera visto después su ineficacia operativa o el surgimiento de nuevas formas de conflicto y opresión a sus expensas, bajo la bandera de la intervención humanitaria o las operaciones de paz. Al respecto, Fisher (2011) señala: "Las

intervenciones humanitarias pueden adoptar una gran variedad de formas, desde la aportación de ayuda hasta el uso de la fuerza militar" (p. 221). Es inevitable citar a Kant, para poner en contraste las buenas ideas e intenciones con las realizaciones políticas pragmáticas y sus resultados e impactos.

> Artículos preliminares de una paz perpetua entre los Estados. 1) Ningún Estado independiente (pequeño o grande, lo mismo da) podrá ser adquirido por otro Estado mediante herencia, cambio, compra o donación. 2) Los ejércitos permanentes (*miles perpetuus*) deben desaparecer por completo con el tiempo. 3) Ningún Estado debe inmiscuirse por la fuerza en la constitución y el Gobierno de otro Estado. (Kant, 1795, pp. 247-249)

Hasta aquí dejaremos esta reflexión solo para hacer notar que las regulaciones de la guerra y los conflictos humanos evidentemente se quedan cortas y resultan inapropiadas para atender las exigencias de los ciberconflictos, tanto más complejos, difusos y condicionados.

El *orden global postmoderno,* como es adecuado llamarlo, habitualmente se estudia desde las relaciones internacionales, la ciencia y la filosofía política. Según Gómez (2017):

> es decir, en cuanto a la estructura, los actores, los procesos y sus relaciones, el poder y fenómenos como la violencia. La estructura está determinada por la inclinación hacia el modelo ordenado o anárquico del sistema internacional, la posición de los actores por el rol que desempeñan, y los procesos operan en función de las interacciones de conflicto o cooperación. (p. 59)

Según Hardt y Negri (2004):

> en el orden global contemporáneo se libra una guerra global permanente donde los actores, aun sin perseguir objetivos comunes y a pesar de sus desigualdades se ven forzados a cooperar […] El imperio gobierna un orden global fracturado por divisiones y jerarquías internas, y abatido por la guerra perpetua. El estado de guerra es inevitable en el imperio […] la guerra se está convirtiendo en un fenómeno general, global e interminable que erosiona la distinción entre la guerra y la paz, de manera que no podemos imaginar una paz verdadera, ni albergar una esperanza de paz, entre otras cosas porque también la distinción tradicional entre la guerra y la política se desvanece, hasta tal punto de que la guerra se está convirtiendo en el principio organizador básico de la sociedad, no la política. (p.8)

Lo que destaca del planteamiento de Hardt y Negri acerca del orden global contemporáneo es que la noción misma de *potencia mundial* se ha erosionado; si bien es cierto, existen actores clave que luchan incansablemente por la hegemonía económica, como China, o geoestratégica, como Rusia, las interdependencias complejas, esa suerte de necesidad de recursos vitales e intereses dispersos, hacen que la cooperación, la disuasión o incluso el engaño sean lógicas válidas para prosperar y obtener ventaja, máxime que muchos de esos activos son intangibles, productos del conocimiento, *software,* ciberarmas disponibles al mejor postor, libres del control de los Estados; así lo refleja la investigación de Nicole Perlroth registrada en su libro, *Así es como me dicen que acabará el mundo:*

> Durante décadas, bajo la protección de niveles clasificatorios y acuerdos de confidencialidad, el gobierno de EE. UU. se convirtió en el principal acaparador de días cero del mundo. Los agentes del gobierno de EE. UU. pagaron un alto precio (primero, miles; después, millones de dólares) a los *hackers* dispuestos a vender sus códigos para forzar cerraduras y su silencio. Pero luego, EE. UU. perdió el control de su provisión y del mercado. Ahora esos días cero están en manos de naciones hostiles y mercenarios a los que no les importa si tu voto se pierde, se contamina tu agua o si nuestras centrales nucleares colapsan. (Pelroth, 2022, p.1)

Estudiar el poder ciberespacial permite comprender las amenazas actuales. En un mundo cada vez más digitalizado, las operaciones militares y la seguridad nacional dependen en gran medida de los sistemas ciberespaciales. Comprenderlos permitirá tener claro el camino para proteger los intereses nacionales, mantener la estabilidad internacional y fomentar el avance científico y tecnológico en el campo de la seguridad cibernética.

Foucault (1966) afirma que el conocimiento científico está ligado a relaciones de poder y cómo el discurso científico puede ser utilizado para justificar formas de dominación social. Estudiar el poder ciberespacial constituye un factor esencial, porque el ciberespacio se ha convertido en un componente fundamental de las actividades militares modernas. En este contexto, los conflictos militares actuales a menudo implican operaciones cibernéticas, que pueden tener un impacto significativo en la capacidad de un país para protegerse o llevar a cabo operaciones militares.

En los contextos de guerra, pero también en escenarios donde esta no ha sido declarada —como afirmarían Hardt y Negri, en el contexto de guerra global

permanente—, han venido suscitándose diferentes tipos de incidentes en el ciberespacio, ataques o conflictos que reflejan la competencia por el poder entre los diferentes Estados, empresas u organismos nacionales e internacionales. Valeriano y Maness sostienen que, en el ciberespacio, la competencia por el poder y la influencia son elementos centrales en la ciberseguridad y el ciberconflicto. Este enfoque tiene importantes implicaciones para la política y la seguridad internacional, ya que el ciberespacio se convierte en un nuevo ámbito de competencia estratégica en el sistema internacional (Valeriano & Maness, 2015).

Es momento de decir que, sobre la premisa de guerra global permanente, han surgido formas de librarla que han dado origen a definiciones, tales como guerras de quinta generación, guerras híbridas, ciberguerras o ciberconflictos, incluso la guerra especial —desarrollada doctrinariamente por el US Army— en el Manual de operaciones especiales del Ejército de los EE. UU., ADP 3-05 (2012, p. 9) y, por supuesto, las MDO (operaciones multidominio). Todas ellas tienen en común que son libradas, se sirven o involucran en mayor o menor medida acciones en el ciberespacio; en consecuencia, su comprensión es necesaria al momento de valorar el poder ciberespacial en cada una de ellas.

Un alto número de acciones tiene lugar en el ciberespacio; además, se puede afirmar sin prevenciones que estas son ejecutadas por actores estatales, por fuerzas de inteligencia y agencias; se conducen operaciones mediáticas y en el ciberespacio, no declaradas generalmente, de las que solo alcanzamos a ver sus efectos. Para nuestro objeto de estudio, esto resulta *a priori* inabordable o incluso inútil, pero en verdad se trata justamente de la fuente de nuestra indagación. ¿Qué tipo de ciberarmas se emplean? ¿Cómo operan? ¿Qué tanto tiene que ver la inteligencia artificial en todo esto? Y lo que resulta de mayor interés: ¿Cómo, siendo clandestinas estas capacidades, pueden valorarse como parte del arsenal o ciberpoder de un Estado?

Las guerras híbridas, según el Instituto LISA "son aquellas que combinan el uso de la fuerza militar con otros elementos como pueden ser los ciberataques, la manipulación de la información mediante internet y redes sociales, o vectores de presión económica" (Instituto LISA). En ellas, el ciberespacio tiene dos funciones: como herramienta para realizar operaciones de información y acciones afines, o como campo de batalla, donde se persiguen objetivos específicos del adversario. En este escenario, el uso de armas cibernéticas es masivo y suele ser más evidente y regulado incluso doctrinariamente su uso, concebidas como operaciones en el ciberespacio; los estudios de caso serán sumamente útiles para determinar en qué medida.

Antes de abordar los ciberconflictos, se introduce la denominada *guerra especial,* diseñada por la RAND corporation (2016) y definida como:

> una forma peculiar de guerra y como una estrategia para proteger y alcanzar los intereses nacionales de EE. UU. , desde una perspectiva realista que presta poca atención a las implicaciones éticas de los procedimientos. Se considera justificado y permisible intervenir en otros países de forma indirecta o subrepticia, y sacar provecho en beneficio de intereses unilaterales, evitando comprometer tropas y recursos en confrontaciones decisivas. (p. III)

En muchos casos, la guerra especial puede concebirse como una guerra no evidente, en la cual, según Libicki (2012) "Las innovaciones, tanto tecnológicas como organizativas, en las últimas décadas han creado un potencial de una guerra no evidente, en la que la identidad del lado combatiente e incluso el mero hecho de la guerra resultan completamente ambiguos" (p. 19). Libicki (2012) señala:

> […] además que el ataque tecnológico —ciberguerra, guerra espacial, guerra electrónica, guerra de drones— y otras estrategias de largos antecedentes históricos como el sabotaje, el asesinato y el uso de minas forman parte del espectro de acciones que se pueden llevar a cabo de forma no evidente; en todas ellas, la ambigüedad es la base de la falta de evidencia: se desconoce el actor mas no el acto. Algunos incidentes bélicos no evidentes serían claramente actos de guerra si fueran evidentes. (p. 19)

Resulta indiscutible, pero lo afirmamos una vez más. Para el estudio del ciberpoder, este tipo de guerra suma complejidades al momento de ponderar y estimar los activos y recursos que en verdad un Estado dispone o por aquellos que paga por poner al servicio de estos fines cuestionables.

En este tipo de conflictos bélicos, las diferencias políticas y las marcas de poder global, se manifiestan en acciones económicas, militares, de información y afectaciones de la población civil, y establecen un caldo de cultivo que es aprovechado por los diferentes actores globales para potenciar el poder del ciberespacio como un campo de operaciones, no solamente con objetivos estratégicos en las infraestructuras críticas cibernéticas y de información, sino como un lago de información donde las operaciones cibernéticas y cognitivas se consolidan como la fuente fundamental de un conflicto híbrido (Cano, 2021). Lo anteriormente expuesto permite concebir la importancia que tiene el ciberespacio en la actualidad y cómo su evolución puede afectar la seguridad, la estabilidad y el desarrollo de las naciones.

El presidente y fundador del Foro Económico Mundial Klaus Schwab y autor del libro *La Cuarta Revolución Industrial* (Schwab, 2017) afirma:

> La Cuarta Revolución Industrial promete grandes cambios sociales, esta revolución tecnológica alterará por completo los productos que elaboramos, cómo los elaboramos, cómo interactuamos y, sobre todo, quiénes somos. Como era de esperarse, aquel potencial caracterizado por la promesa de la automatización y la interconexión de los ecosistemas físicos con los digitales (Internet de las cosas, implantes neurales, prótesis inteligentes, etc.) no solo ofrecerían beneficios, sino que, consecuentemente, también supondrían peligros. La guerra también experimentará cambios. (p. 2)

Las citadas palabras de Schwab nos presentan una forma de conflictos tanto más complejos, donde las amenazas pueden no provenir ni estar vinculadas con actores de otro país y sin embargo ser capaces de poner en riesgo activos estratégicos de los Estados; se trata de una situación de amenazas desbordadas ante las cuales, sin duda, las respuestas tradicionales resultarán inoperantes y, virtualmente, se requerirá de un poder militar ciberespacial redefinido y posiblemente hoy inexistente en la mayoría de fuerzas de defensa del globo.

Desde el componente estratégico, el ciberespacio ha sido reconocido como un ámbito de importancia estratégica para el poder militar por muchos autores y organizaciones. En este contexto, Castells señala que el ciberespacio es un espacio de poder global que tiene el potencial de transformar el funcionamiento de la sociedad y el Estado. Según el autor, las redes digitales permiten la creación de nuevas formas de organización política, económica y social que pueden desafiar el poder de las instituciones tradicionales (Castells, 2001). Aunado a esto, Kramer (2009) argumenta que el ciberespacio es una dimensión fundamental del ciberpoder y la seguridad nacional, porque los conflictos en el ciberespacio pueden tener consecuencias devastadoras para la infraestructura crítica de los países y para la seguridad de los ciudadanos. En la sociedad moderna, el ciberespacio se ha convertido en un espacio fundamental para la actividad política, económica y militar y el papel que juega la inteligencia artificial y la ciberdefensa en la gestión de los conflictos cibernéticos (Arellano, 2019). En este sentido, Psychogiou (2022) establece que el ciberespacio se ha convertido en el quinto espacio de batalla en un panorama de seguridad cada vez más complejo, y las amenazas cibernéticas han sido parte del ámbito de la seguridad internacional (p. 1).

Lo anteriormente expuesto da cuenta de que el ciberespacio se ha convertido en una herramienta fundamental para el funcionamiento de las sociedades modernas, y los países que tienen la capacidad de controlar y dominar el ciberespacio tienen una ventaja significativa en el ámbito militar, económico y político. El ciberespacio se ha convertido en un campo de batalla en el que los países pueden llevar a cabo operaciones encubiertas sin necesidad de una intervención militar directa, lo que les permite alcanzar objetivos estratégicos sin sufrir las consecuencias de un conflicto armado. Nace entonces una forma relativamente nueva de conflicto: el *ciberconflicto,* que toma más relevancia a medida que se incrementan la dependencia de la tecnología y la interconexión global de los sistemas de información.

Los ciberconflictos deberían considerarse como una amenaza a la seguridad y defensa nacional, porque el ciberespacio se ha convertido en una dimensión crucial para la vida económica, política y social de las naciones; un entorno virtual donde las actividades de comunicación y el intercambio de información tienen lugar mediante redes interconectadas, tecnologías y humanos. A propósito, Thomas Rid ha definido los ciberconflictos como el uso de medios cibernéticos para desencadenar, intensificar o prolongar un conflicto armado en el mundo real (Rid, 2012). Carr y Tikk argumentan que "El ciberconflicto es un conflicto que involucra la utilización de herramientas y técnicas cibernéticas para causar daño o perturbar los sistemas informáticos de los adversarios, y que puede tener consecuencias significativas en términos de seguridad, política y economía" (Carr & Tikk, 2021, p. 6). En complemento, Singer y Friedman afirman que el ciberconflicto es "un conflicto que se lleva a cabo a través del ciberespacio y que puede involucrar operaciones militares, de inteligencia, de propaganda y de sabotaje, en el que los actores utilizan herramientas y técnicas cibernéticas para alcanzar sus objetivos" (Singer & Friedman, 2021, p. 2). Aunque las definiciones estudiadas muestran un amplio espectro de perspectivas sobre el tema, todas coinciden en que el ciberconflicto implica el uso de tecnologías de información y operación, para llevar a cabo acciones hostiles en el ciberespacio, ya sea para dañar o perturbar los sistemas tecnológicos de los adversarios, o para lograr objetivos políticos, militares, económicos o de otro tipo.

Entre tanto, Alberts y Hayes sostienen que los ciberconflictos se han convertido en una amenaza real para la seguridad nacional, ya que los sistemas informáticos y de comunicaciones son esenciales para el funcionamiento de la economía, el gobierno y la defensa. Los autores advierten que los ciberataques pueden tener consecuencias graves para la infraestructura crítica y la sociedad en general (Alberts & Hayes, 2003). En la actualidad, la naturaleza de la guerra y la seguridad

han cambiado con la evolución de la tecnología y la aparición del ciberespacio como nuevo campo de batalla, lo que presenta desafíos únicos y requiere un enfoque multidisciplinario. Diversos autores han abordado la importancia del estudio de los ciberconflictos. Por ejemplo, Kramer argumenta que la ciberseguridad es fundamental para la seguridad nacional y que los Estados deben tener en cuenta los aspectos tecnológicos, políticos y sociales de los ciberconflictos. Por su parte, Libicki, aborda el concepto de *ciberdisuasión* y la amenaza como parte de las represalias que pueden ayudar a disuadir a los agresores cibernéticos. Los ciberconflictos son una expresión del poder en la sociedad de la información, donde el control de la información y la tecnología es fundamental (Libicki, 2018).

Como se señaló, uno de los retos para estudiar el ciberpoder, que exhibe a la par una notable ventaja estratégica de los ciberconflictos, es que estos pueden ser llevados a cabo de manera encubierta, sin necesidad de una gran inversión de recursos materiales y financieros, y con la posibilidad de causar un gran impacto en la infraestructura crítica de un país o de una organización. Además, los ciberataques pueden ser lanzados desde cualquier parte del mundo, lo que hace que sea difícil atribuir la responsabilidad a un actor específico. Clarke argumenta que el ciberespacio ofrece una ventaja estratégica a los adversarios, porque les permite operar sin ser detectados y afectar sistemas críticos como infraestructuras, redes de comunicaciones y sistemas militares (Clarke, 2010). Esta nueva forma de conflicto permite a los actores estatales y no estatales nivelar el campo de juego contra adversarios más fuertes, considerando que el ciberespacio es un dominio en el que el tamaño y la capacidad económica no son necesariamente determinantes para el éxito de un ataque. Kramer sostiene que los ciberconflictos pueden proporcionar a los actores una ventaja táctica, ya que les permiten penetrar en sistemas de información y comunicación de los adversarios para obtener información clasificada o alterar los sistemas de comando y control (Kramer, 2009).

Otra de las ventajas estratégicas de los ciberconflictos es su capacidad para producir daños y afectar objetivos clave sin necesidad de una fuerza militar convencional. Mediante ciberataques, pueden causar daños significativos a los sistemas de infraestructura crítica, como los de energía, transporte, salud y finanzas, lo que puede tener consecuencias graves para la economía y la sociedad en su conjunto. Según Rid (2013), los ciberconflictos permiten a los actores poderosos "proyectar su poder en el ciberespacio sin el costo de las operaciones militares convencionales" (p. 4). Esto les permite infligir daños significativos a los sistemas de infraestructura crítica, sistemas financieros y de comunicaciones, entre otros,

sin necesidad de poner en riesgo a su propia fuerza militar. Los ciberataques pueden ser utilizados como una forma de coerción y disuasión en las relaciones internacionales; para enviar mensajes a otros actores internacionales y amenazar con mayores consecuencias si se cumplen ciertas condiciones (Libicki, 2009, pp. 11-12). Fernández (2022) afirma que:

> […] de 2021 a la actualidad los ciberataques están siendo usados como arma no convencional entre Estados, los principales implicados siguieron siendo los países que anteriormente tenían gran actividad en el ciberespacio, es decir, EE. UU. , China, Rusia y la Unión Europea, a los que se van sumando otras naciones hasta ahora poco beligerantes en la lucha cibernética, como India, así como otros actores que siempre estuvieron activos, casos Corea del Norte, Israel o Irán. (Fernández, 2022, pp. 313-314)

De estas afirmaciones, se puede inferir que la ventaja estratégica de los ciberconflictos radica en su capacidad para infligir daños significativos sin necesidad de poner en riesgo la propia fuerza militar y en su capacidad para ser utilizados como una forma de coerción y disuasión en las relaciones internacionales, por lo que el poder militar ciberespacial representa una necesidad latente en la agenda de los países; sin embargo, no se puede perder de vista que esta realidad complejiza la forma en que los Estados-nación definen, valoran y adquieren su poder militar ciberespacial.

El ciberpoder es una forma de proyección de poder en la era digital y su desarrollo es esencial para la seguridad y defensa de las naciones. Así lo argumenta Sánchez (2019), al señalar que el poder ciberespacial es una herramienta crítica para la seguridad y defensa nacional, ya que permite a los Estados proteger sus sistemas informáticos críticos y asegurar su soberanía en el ciberespacio. Los autores sostienen que el ciberpoder es un componente integral de la seguridad nacional y que su desarrollo debe ser una prioridad para los Gobiernos. Según Segal (2017), el poder ciberespacial se refiere a la capacidad de controlar y explotar el ciberespacio para lograr objetivos políticos, económicos o militares, ya sea mediante la protección de la propia infraestructura crítica o la interrupción de la de los adversarios.

El ciberpoder permite obtener la superioridad o supremacía en el ciberespacio. Su disputa puede proporcionar a un país una ventaja estratégica en términos de seguridad nacional, política, económica y militar. Al tener un dominio fuerte en el ciberespacio, un país puede proteger sus propios sistemas de información y

comunicación y, al mismo tiempo, espiar, sabotear o interrumpir los sistemas de otros países. Además, el ciberespacio es una plataforma vital para la economía digital y la innovación tecnológica, lo que significa que un país con una ventaja en el ciberespacio puede ganar una posición de liderazgo en el comercio mundial y la tecnología. Por lo tanto, la disputa por la superioridad o la supremacía en el ciberespacio se ha convertido en una parte importante de la competencia geopolítica actual. Los países compiten por la superioridad y supremacía en el ciberespacio porque consideran que el control de la información y las comunicaciones en este ámbito es fundamental para su seguridad, economía e influencia en el mundo. Los países están compitiendo por la superioridad en el ciberespacio y esto está afectando la seguridad nacional y las relaciones internacionales (Sanger, 2018).

Los países compiten por la superioridad en el ciberespacio para mantener la seguridad nacional, proteger los intereses económicos y garantizar la estabilidad política y social (Tikk & Kerttunen, 2020) Los países compiten por la superioridad en el ciberespacio porque la información y el conocimiento son los recursos más valiosos del mundo actual y porque el control de estos recursos es clave para el poder y la influencia (Stavridis & Farkas, 2012), lo que da cuenta de la importancia que representa para una nación u organización desarrollar el ciberpoder y disputar su superioridad o supremacía.

El poder cibernético se ha convertido en un elemento fundamental para la seguridad nacional y la defensa de los Estados, debido a que los ciberataques pueden causar graves daños a la infraestructura crítica y a la economía de los países (Cujabante et al., 2020; Libicki, 2018; Valeriano & Maness, 2020).

Perspectivas sobre el ciberpoder

De acuerdo con Nye (2011), no solo los tipos y las fuentes de poder de los países han cambiado; los cambios se presentan también en el contexto internacional, es decir, el escenario donde conviven los Estados; a propósito, destaca que los países tienen que convivir con otros actores no gubernamentales (s. p.). Las perspectivas del ciberpoder son amplias y variadas. En primer lugar, el ciberpoder se considera una herramienta esencial para la proyección de poder en el mundo moderno. A diferencia del poder tradicional, que se basa en la fuerza física y la coerción, el ciberpoder se basa en la capacidad de influir y controlar el comportamiento de los individuos por medio del ciberespacio. Aunque el ciberespacio aún no se ha utilizado como medio para demostrar el poder duro convencional de la coerción y las

amenazas respaldadas por la fuerza física, sí presenta un medio adecuado para la proyección del poder blando de atracción e imitación. A continuación, se presentan las perspectivas del ciberpoder analizadas desde las voces militares o estratégicas estadounidenses (Kuehl, 2009; Nye, 2010) en contraposición con las acepciones de Dunn respecto del ciberpoder en la Unión Europea (Dunn, 2018).

Para continuar este análisis se hace necesario comprender lo que he denominado *localización del ciberpoder*, que sigue dos tendencias: la primera puede vincularse con las definiciones de ciberpoder militar y corresponde a una perspectiva reduccionista que concibe el ciberespacio como medio de gestión que debe ser preservado para retener la iniciativa; de allí que los esfuerzos operacionales se orienten a generar protocolos para la defensa de activos estratégicos, en ocasiones no de la nación sino de las fuerzas, lo cual es aún más limitante. La otra perspectiva, que puede denominarse *comprehensiva*, se profiere con la definición de ciberestrategia o de ciberpoder integrado a otros dominios o al poder nacional; incorpora y expande el núcleo y capacidades asociadas al ciberpoder en función exclusiva del dominio ciberespacial y suma o se integra a otros componentes.

Ciberpoder en EE. UU.

Para comprender el ciberpoder desde la teoría del ciberpoder militar propuesta por el Gaines (2015), se hace necesario entender los términos y principios que forman la base de esta teoría y ayudan a comprender y aplicar las operaciones en el ciberespacio en el contexto de las operaciones conjuntas y la expansión del poder de combate:

- Ciberespacio: dominio global que abarca elementos físicos, lógicos y personales en el ámbito cibernético.
- Ciberpoder: aplicación de conceptos operativos, estrategias y funciones que emplean operaciones en el ciberespacio para expandir el poder de combate y lograr objetivos militares.
- Estrategia militar cibernética: desarrollo y empleo de capacidades operativas en el ciberespacio integradas con otras capacidades en diferentes dominios para expandir el poder de combate y lograr los objetivos militares.
- Terreno clave en el ciberespacio: cualquier elemento físico, lógico o personal del ciberespacio que, si es interrumpido, degradado o destruido, limita el poder de combate y otorga una ventaja marcada a uno de los combatientes.

- Espacios cibernéticos militares: diferentes ciberespacios que existen, teniendo en cuenta su diversidad y heterogeneidad.

Sobre estos preceptos, la teoría propuesta por Gaines plantea que la integración de las operaciones del ciberespacio con las operaciones conjuntas puede ampliar el poder de combate conjunto de varias maneras (Kern, 2015).

Las operaciones en el ciberespacio presentan una serie de ventajas estratégicas. En primer lugar, ofrecen una mayor capacidad de ataque, lo que permite a las fuerzas conjuntas perturbar la infraestructura de comunicación y comando del enemigo, debilitando significativamente su capacidad de respuesta. Además, estas operaciones brindan una mejor defensa al permitir a las fuerzas conjuntas proteger sus propias redes y sistemas contra ataques cibernéticos, asegurando la integridad de su poder de combate. Asimismo, las operaciones cibernéticas proporcionan una mayor conciencia situacional al recopilar información en tiempo real sobre las actividades y capacidades del enemigo, lo que facilita la toma de decisiones fundamentadas y la adaptación ágil a situaciones cambiantes (DoD, 2011).

Por último, estas operaciones tienen la capacidad de apoyar y potenciar otras capacidades militares, como las operaciones terrestres, marítimas y aéreas, lo que se traduce en un aumento de la eficacia y la coordinación en operaciones conjuntas, ya sea neutralizando defensas enemigas antes de un ataque convencional o proporcionando apoyo en términos de inteligencia y comunicaciones durante operaciones combinadas. En general, la integración de las operaciones del ciberespacio en operaciones conjuntas amplía el poder de combate conjunto al proporcionar nuevas formas de ataque y defensa, mejorar la conciencia situacional y potenciar otras capacidades militares (Gaines, 2015).

Ciberpoder en la Unión Europea

Impulsada por preocupaciones sostenidas sobre las amenazas del ciberespacio, la ciberseguridad se ha convertido en un tema prioritario en las agendas políticas de los Estados y organizaciones internacionales y supranacionales, entre ellas la Unión Europea (UE). El debate político asociado se centra en medidas políticas para dominar el comportamiento en el ciberespacio, a fin de convertirlo de un lugar rebelde e inseguro en uno más estable, confiable y ordenado. En el centro de esta discusión se encuentran cuestiones fundamentales de poder y control (Dunn, 2018).

La dificultad con el concepto de ciberpoder es que aún no existen análisis sistemáticos (empíricos) del tema; de hecho, el cuerpo de literatura sobre el ciberpoder es pequeño y fragmentado. Los textos existentes, incluidos aquellos que abordan específicamente el ciberpoder europeo (Klimburg & Tirmaa-Klaar, 2011; Sliwinski, 2014a, 2014b), son de naturaleza principalmente orientada a políticas que vienen acompañados de una comprensión contextualmente restringida del poder que no necesariamente es fácilmente aplicable a otras políticas y contextos (Dunn, 2018). Por lo general, abordar las cuestiones de poder mediante la investigación empírica, en lugar de hacerlo de manera conceptual, teórica o normativa, conlleva una serie de desafíos. Estos desafíos se evidencian en la extensa literatura escrita sobre diversos aspectos del poder en las relaciones internacionales y los esfuerzos realizados para cuantificarlo.

De acuerdo con Dunn (2018), la UE asume el ciberpoder de diversas maneras. En primer lugar, la UE reconoce la importancia de la ciberseguridad y ha desarrollado políticas y estrategias para abordar las amenazas cibernéticas (Manners, 2002). La UE utiliza diferentes instrumentos, instituciones y agencias para ejercer diferentes formas de ciberpoder, tanto interna como externamente. Internamente, la UE emplea arreglos voluntarios, incentivos, diálogo, cooperación y coordinación para fortalecer su ciberpoder.

Desde una perspectiva externa, la UE aboga por una política de cooperación que se fundamenta en la promoción del ciberespacio como un ámbito de libertades y derechos fundamentales. No obstante, se admite que la UE carece de un enfoque estratégico unificado para ejercer de manera deliberada su ciberpoder. A pesar de que la UE cuenta con la capacidad de utilizar elementos cibernéticos no estatales en apoyo de sus políticas, no existe una estrategia claramente definida para aprovechar plenamente su ciberpoder. A medida que la tecnología de la información se vuelve un componente cada vez más central en la convergencia de problemáticas de seguridad, se reconoce que cualquier actor político con ambiciones regionales o globales debe involucrarse en el ámbito cibernético. Por lo tanto, se sugiere que la UE debe desarrollar un tipo de ciberpoder que se sustente en la resiliencia y los valores fundamentales de la UE, tales como la prevención, la integridad y el multilateralismo (Dunn, 2018). En suma, la UE asume el ciberpoder con políticas y estrategias de ciberseguridad, utilizando diferentes instrumentos y agencias, tanto interna como externamente. Sin embargo, se reconoce la necesidad de desarrollar un enfoque estratégico integrado para ejercer plenamente su ciberpoder.

Conclusiones

La transformación del ciberespacio hacia el ciberpoder representa un cambio fundamental en la concepción del poder en la era contemporánea. Este cambio ha sido impulsado por avances tecnológicos que han convertido el ciberespacio, de simple medio de comunicación, a un campo estratégico donde se libran batallas por la influencia, la seguridad y la supremacía. El ciberpoder no solo implica la capacidad de controlar y manipular el ciberespacio, sino también la habilidad de ejercer influencia y lograr objetivos políticos, económicos y sociales por medios digitales.

Las diversas perspectivas sobre el ciberpoder reflejan la complejidad y las múltiples dimensiones de este fenómeno. Por un lado, algunas visiones resaltan las oportunidades que ofrece el ciberespacio para la innovación, la colaboración y el empoderamiento ciudadano. Desde esta perspectiva, el ciberpoder se considera una fuerza democratizadora que amplía el acceso a la información, facilita la participación ciudadana y estimula el desarrollo económico y social.

Por otro lado, existen enfoques más críticos que alertan sobre los riesgos y desafíos asociados al ciberpoder. Estas visiones advierten sobre la creciente vulnerabilidad de las infraestructuras críticas ante ciberataques, la pérdida de privacidad y seguridad de los datos personales, así como el potencial de manipulación y desinformación en línea para socavar la democracia y los derechos humanos.

En este contexto, comprender y abordar las diversas perspectivas sobre el ciberpoder es crucial para diseñar políticas y estrategias efectivas que fomenten un uso responsable y ético del ciberespacio. Esto implica fortalecer la ciberseguridad, salvaguardar los derechos digitales de los individuos y promover una gobernanza inclusiva y transparente del ciberespacio a nivel nacional e internacional. En última instancia, el desafío radica en aprovechar las oportunidades que brinda el ciberpoder para impulsar el progreso y el bienestar humano, al tiempo que se mitigan los riesgos y se enfrentan los desafíos planteados por esta nueva dimensión del poder en el siglo XXI.

Referencias

Alberts, D. S., & Hayes, R. E. (2003). *Power to the edge: Command... Control... in the information age*. CCRP Publication Series. http://www.dodccrp.org/files/Alberts_Power.pdf

Arellano, A. (2019). *Ciberconflicto: La nueva amenaza global.* Instituto de Ingeniería UNAM.

Barnett, M., & Duvall, R. (2005). Power in international politics. *International Organization, 59*(1), 39-75. https://doi.org/10.1017/S0020818305050010

Bauman, Z. (2000). *Modernidad líquida*. Fondo de Cultura Económica.

Cano, J. J. (2021). Los conflictos híbridos y el poder de los algoritmos. *Revista Sistemas,* (161), 62-72. https://doi.org/10.29236/sistemas.n161a6

Carr, M., & Tikk, E. (2021). *International law and cyber conflict: Responding to new challenges*. Cambridge University Press.

Castells, M. (1996). *La era de la información: Economía, sociedad y cultura* (Vol. 1, La sociedad red). Alianza Editorial.

Castells, M. (2001). *La galaxia internet.* Plaza & Janes.

Castells, M. (2010). *The information age: Economy, society, and culture* (Vol 1., The rise of the network society). John Wiley & Sons.

Centro Superior de Estudios de la Defensa Nacional [CESEDEN]. (2012). *El ciberespacio: Nuevo escenario de confrontación.* Ministerio de Defensa Nacional. https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it.* Harper Collins.

Cujabante Villamil, X. A., Bahamón Jara, M. L. ., Prieto Venegas, J. C. ., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: Un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova, 18*(30), 357-377. https://doi.org/10.21830/19006586.588

DoD. (2011). *Department of Defense Dictionary of Military and Asociated Terms.* DoD. https://irp.fas.org/doddir/dod/jp1_02.pdf

Dunn, C. M. (2018). Europe's cyber-power. *European Politics and Society, 19*(3), 304-320. https://doi.org/10.1080/23745118.2018.1430718

Estudillo, J. G. (2002). *Visibilidad de la producción académica de feministas mexicanas a través de una base de datos* [Tesis de pregrado, Universidad Nacional Autónoma de México].

Ferreira da Silva, P. (2018). Oportunidades y desafíos de tecnologías emergentes: La importancia de la industria aeroespacial para Brasil. *Revista Fuerza Aérea-EUA,* (2), 36-48.

https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%201%20Issue%202/Spanish/05-peterson_s.pdf

Foucault, M. (1970). *El orden del discurso.* Fabula Tusquets Editores.

Gibson, W. (1982). *Burning Chrome.* Ace Books.

Gibson, W. (1984). *Neuromante.* Minotauro.

Gómez Rodríguez, G. A. (2017). *Riesgos de transgresión moral del militar en la post-modernidad* [Tesis, Universitat de Barcelona]. Repositorio UB. https://diposit.ub.edu/dspace/bitstream/2445/119533/1/GAGR_TESIS.pdf

Hardt, M., & Negri, A. (2004). *Multitud: guerra y democracia en la era del imperio.* Debate.

Hunker, J. (2010). *Cyber war and cyber power: Issues for NATO doctrine* [Research Paper, N.º 62]. https://ciaotest.cc.columbia.edu/wps/nat/0031912/f_0031912_25908.pdf

Jordan T., (1999). *Cyberpower: The culture and politics of cyberspace and the internet.* Routledge.

Kant, M. (1795/2010). *La paz perpetua*. Porrúa.

Kern, S. (2015). *Expanding combat power through military cyber power theory* [Tesis de maestría, Joint Advanced Warfighting School]. Repositorio institucional. https://apps.dtic.mil/sti/pdfs/ADA621664.pdf

Klimburg, A., & Tirmaa-Klaar, H. (2011). Cybersecurity and cyberpower: Concepts, conditions, and capabilities for cooperation for action within the EU. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf

Kramer, F. D., Starr, S. H., & Went, L. K. (2009). *Cyberpower and national security.* Potomac Books, Inc.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. En F. D. Kramer, S. H. Starr & L. K. Wentz, *Cyberpower and National Security* (pp. 1-17). https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/

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

Libicki, M. C. (2012). Cyberspace is not a warfighting domain. *Isjlp,* (8), 321. https://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc8&div=17&id=&page=

Libicki, M. C. (2018). Expectations of cyber deterrence. *Journal of Strategic Studies, 41*(1-2), 44-57. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-4/Libicki.pdf

Lisa Institute. (s. f.) ¿Qué es la guerras híbridas y cómo nos afectan las amenazas híbridas. https://www.lisainstitute.com/blogs/blog/guerra-hibrida-amenazas-hibridas#:~:text=En%20los%20%C3%BAltimos%20a%C3%B1os%20cobran,o%20vectores%20de%20presi%C3%B3n%20econ%C3%B3mica

MacDonald, D. B. (2009). *Thinking history, fighting evil: Neoconservatives and the perils of historical analogy in American politics.* Lexington Books.

Madden, D., Hoffmann, D., Johnson, M., Krawchuk, F., Nardulli, B. R., Peters, J. E., Robinson, L., & Doll, A. (2016, 23 de febrero). *Toward operational art in special warfare.* Rand Corporation. https://www.rand.org/pubs/research_reports/RR779.html

Manners, I. (2002). Normative power Europe: A contradiction in terms? *Journal of Common Market Studies, 40*(2), 235-258. https://doi.org/10.1111/1468-5965.003

Mitchell, W. J. (1995). *City of bits: Space, place, and the Infobahn.* MIT Press.

Nye, J. S. (2010). *Cyber power.* Harvard Kennedy School.

Nye, J. S., (2011). *The future of power.* Public Affairs.

Pelroth, N. (2022). *Así es como me dicen que acabará el mundo.* Tendencias.

Psychogiou, V. (2022) Cyberspace: Is NATO doing enough? https://finabel.org/wp-content/uploads/2022/02/cyberspace-is-nato-doing-enough-1.pdf

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5-32. https://doi.org/10.1080/01402390.2011.608939

Sánchez, M. E. (2019). La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan la seguridad y defensa del Estado. En G. Medina (Ed.), *La seguridad en el ciberespacio: un desafío para Colombia* (pp. 27-59). Escuela Superior de Guerra "General Rafael Reyes Prieto". https://doi.org/10.25062/9789585216549.01

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age.* Crown.

Schwab, K. (2017). *La cuarta revolución industrial.* Debate.

Segal, H. (2017). *Cyber-security at a frantic time: A rational plan.* Canadian Global Affairs Institute.

Singer, P. W., & Friedman, A. (2021). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

Sliwinski, K. F. (2014a). European union – Cyber power in the making. *Asia-Pacific Journal of EU Studies, 12*(1), 1-22. https://www.researchgate.net/publication/317717658_European_Union_-_cyber_power_in_the_making

Sliwinski, K. F. (2014b). Moving beyond the European union's weakness as a cyber-security agent. *Contemporary Security Policy, 35*(3), 468-486. https://10.1080/13523260.2014.959261

Stavridis, J., & Farkas, E. N. (2012). The 21st century force multiplier: Public–private collaboration. *The Washington Quarterly, 35*(2), 7-20. https://doi.org/10.1080/0163660X.2012.665336

Tikk, E., & Kerttunen, M. (Eds.). (2020). *Routledge handbook of international cybersecurity.* London: Routledge.

Toffler, A. (1970). *Future Shock.* Bantam House.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system.* Oxford University Press.

Valeriano, B., Jensen, B., & Maness, R. C. (2020). *Cyber strategy: The evolving character of power and coercion.* Oxford University Press.

Vergara, E., Trama, G., Uriona, M. N., Ortiz, J. U., & Destro, L. A. (2018). *Operaciones militares cibernéticas: Planeamiento y ejecución.* Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. https://cefadigital.edu.ar/bitstream/1847939/939/1/CAVI-II%20-%20OMC%20DE%20VERGARA.pdf