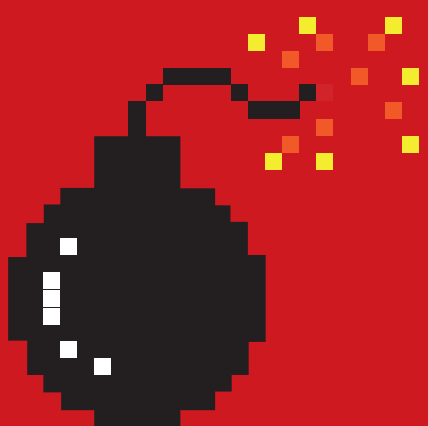
CIBERGUERRA

La consolidación de un nuevo poder en las relaciones internacionales contemporáneas

Andrés Gaitán Rodríguez



ediciones USTA

Ciberguerra

La consolidación de un nuevo poder en las relaciones internacionales contemporáneas

Ciberguerra

La consolidación de un nuevo poder en las relaciones internacionales contemporáneas

Andrés Gaitán Rodríguez

ediciones USTA

Gaitán Rodríguez, Andrés

Ciberguerra. La consolidación de un nuevo poder en las relaciones internacionales contemporáneas / Andrés Gaitán Rodríguez, Bogotá: Universidad Santo Tomás, 2018.

209 páginas; gráficos y tablas

Incluye referencias bibliográficas (páginas 187-208)

ISBN: 978-958-782-151-2
E-ISBN: 978-958-782-152-9

1. Relaciones internacionales 2.Tanques (ciencia militar) 3. Segunda Guerra Mundial 4. Internet - Control. 5. Grupos sociales 6. Tecnologías de la información 7. Internet - Medidas de seguridad 8. Realidad virtual 9. Ciberespacio 10. Aviones militares I. Universidad Santo Tomás (Colombia).

CDD 303.625 CRAI-USTA-Bogotá

Ediciones USTA
Bogotá, D.C., Colombia
Teléfono: (+571) 587 8797, ext. 2991
editorial@usantotomas.edu.co
http://ediciones.usta.edu.co

Corrección de estilo: Eduardo Franco
Diagramación y diseño de carátula: Juliana Pardo Torres
Imagen de carátula: © Rubyknight1 - Brik.co/blogs/pixel-art/

Hecho el depósito que establece la ley

ISBN: 978-958-782-151-2
E-ISBN: 978-958-782-152-9

Primera edición, 2018

Esta obra tiene una versión de acceso abierto disponible en el Repositorio Institucional de la Universidad Santo Tomás: https://doi.org/10.15332/li.lib.2018.00130

Contenido

Introducción

En este primer momento del libro, el encargado de la autoría de las siguientes páginas quisiera hacer algunas consideraciones sobre el porqué se llegó a la creación del mismo. Como estudiante de pregrado en el programa de Ciencia Política y Relaciones Internacionales, existió un interés por las capacidades de cambio y revolución de las tecnologías informáticas, como se conocen actualmente, y la influencia que podrían tener sobre la vida de los seres humanos, entendidos estos, por supuesto, dentro de un contexto social y político. Por eso, algunos de los experimentos propios en investigación académica, en especial el desarrollo de la monografía de grado, estuvieron dirigidos al análisis o al estudio de las tecnologías de la información y de la comunicación (TIC) y al alcance que podían tener sobre los procesos democráticos dentro de los Estados.

No en vano, para dicho momento, hubo un enfoque en algo que se denomina *gobierno electrónico*, el cual se comprende como una proyección de algunas de las capacidades institucionales de los Estados nación a través de internet o el ciberespacio para que los ciudadanos tengan acceso a estos mismos. Por consiguiente, en aquel entonces, el interés en los conceptos de *cambio* y *revolución* se debe a la capacidad que podía tener o presentar un gobierno electrónico para mejorar de esta manera los niveles de democracia dentro de una sociedad,

entendiendo que, siendo estas unas herramientas propias de la información y la comunicación, cosas como la rendición de cuentas, la prestación de servicios y una comunicación entre los gobernantes y el ciudadano podrían ser mejoradas de manera sustancial.

Años más tarde, al tomar la decisión de continuar los estudios de posgrado, se enmarcó el análisis, como politólogo e internacionalista, en la seguridad y defensa nacional. En este nuevo contexto académico, se consiguió la oportunidad de ver y constatar que los dos mundos sobre los cuales se había despertado un interés desde la academia ya estaban coincidiendo desde años atrás. La oportunidad de conocer esta revelación llegó a partir de la lectura de un artículo que *The Economist* publicó en 2010, titulado "Cyberwar", y fue entonces cuando surge la comprensión de que, así como las tecnologías informáticas tenían mucho que ofrecer en diversos campos y procesos de los seres humanos, también esta relación se había configurado a partir del ejercicio de la guerra.

Al analizar lo ya descrito, para entonces el tema de la ciberguerra se convirtió en un gusto académico. Cada nuevo documento, entrevista, noticia, documental sobre la ciberguerra, despertaba más el interés por entender dónde se encontraban los límites de esta nueva práctica bélica que el ser humano había alcanzado. Y hay que reconocer que cada uno de estos elementos llevaba consigo una gran carga sorpresiva y de admiración, no solo porque el tema que estuviera tratando emanaba de un mundo netamente tecnológico y que pareciera más futurista que realista, sino porque daba cuenta de que precisamente aquellas cosas que sonaban tan futuristas ya se encontraban ocurriendo desde hace tiempo.

Han transcurrido ya varios años desde la adopción de la ciberguerra como uno de los temas de investigación predilectos y esto pudo ser así gracias a que en la vida profesional han existido oportunidades de trabajar con importantes instituciones educativas que han abierto espacios de formación y de investigación relacionados con la seguridad y defensa nacional. Asimismo, influyó el hecho de haber tenido el honor de trabajar por muchos años en diversas instituciones de las fuerzas militares de Colombia; sin duda, esto se convirtió en una oportunidad para mí de no separar espacios que otorgaran la libertad de

seguir estudiando un fenómeno que, como cualquier otro que hace parte de las ciencias sociales, demanda gran tiempo para su comprensión.

Por esto, el libro que el lector tienen en sus manos se presenta como producto de la Línea de Investigación en Seguridad en Escenarios Transformados, que pertenece al Centro de Investigación de la Facultad de Gobierno y Relaciones Internacionales de la Universidad Santo Tomás. Por tanto, debe reconocerse el interés de la Facultad por apoyar iniciativas de investigación que estén encaminadas a abordar temas que en la academia colombiana no se han tratado de manera exhaustiva y que de una manera u otra permiten comprender los nuevos límites de la seguridad y defensa nacional, como en este caso el fenómeno de la ciberguerra.

Aunque esta como proceso social sigue siendo una cuestión novedosa, sería absurdo afirmar que se continúa en un limbo interpretativo y analítico sobre el tema. Actualmente, hay libros, análisis y estudios que permiten construir una idea bastante clara de lo que representa este fenómeno bélico. Pero, asimismo, como fenómeno social y humano, la ciberguerra plantea una infinidad de retos exploratorios en sí misma, y por esto en la academia todavía quedan múltiples aristas para poder desarrollar investigación sobre esta cuestión.

Aceptando de antemano que la guerra como tal ha sido una de las formas más claras de constitución y lucha por el poder político, se entiende la ciberguerra como una derivación de esta práctica humana, pero diferenciando sus métodos y el lugar donde se lleva a cabo: las batallas cibernéticas representan en la actualidad también una forma de poder o son, en otras palabras, una continuidad del poder militar que pueden poseer los actores armados.

Entendiendo de la misma manera que con la evolución de la guerra se han aceptado varias formas de esta, principalmente dos, en la cual se debe comprender que el ejercicio bélico en algún momento fue exclusivo de los Estados nación y su ejército, hoy la guerra también puede ser una práctica llevada a cabo por grupos no estatales o armados de manera ilegal. Por ende, y ya que la ciberguerra se fundamenta en tecnologías consideradas como informáticas y de la comunicación, es mucho más previsible entender que otros tipos de actores diferentes de los Estados pueden estar utilizando estas estrategias para alcanzar fines, bien sea

políticos o de otro orden. Cabe recordar que, a diferencia del armamento convencional, las computadoras y los servicios de conexión a internet pueden ser adquiridos por los civiles en todos los mercados del mundo.

Así es como, partiendo del hecho de que los actores armados regulares o constitucionales que representan a los Estados nación, denominados también Fuerzas Armadas o ejércitos, tienen la capacidad gracias a los recursos que sus Estados les dan para hacer la ciberguerra, hay que aceptar, al tratarse de elementos de fácil acceso y bajo costo en términos económicos, la existencia de otros actores, en especial de aquellos actores irregulares que han penetrado este mundo de la ciberguerra, por supuesto, con algunas diferencias frente a las fuerzas militares.

Comprendiendo un poco el nuevo contexto, surge la pregunta que permite el desarrollo del libro: ¿puede considerarse al ciberespacio como una nueva dimensión de acción humana para reproducir la práctica de la guerra interestatal propia de las relaciones internacionales? A partir de esta, nace a su vez la hipótesis que la responde: el ciberespacio sí se ha convertido en un escenario novedoso donde se puede reproducir el fenómeno de la guerra.

El objetivo general busca exponer los argumentos que sustentan la noción de que en la actualidad el ciberespacio se ha convertido en una dimensión de acción humana para reproducir la práctica de la guerra interestatal propia de las relaciones internacionales, del cual a su vez se desprenden tres objetivos específicos. El primero hace referencia a realizar un análisis de la práctica de la guerra, los elementos perennes que este fenómeno contiene y, finalmente, entender su relación con la tecnología. En un segundo momento, presentar las cualidades y los elementos que hacen del ciberespacio una nueva dimensión de acción humana óptima para reproducir la práctica de la guerra. El tercero es analizar la naturaleza de la ciberguerra y las formas en las que se ha materializado en la vida real como parte de la práctica de la guerra interestatal propia de las relaciones internacionales. Para finalizar, si bien el objetivo general identifica la ciberguerra como un fenómeno interestatal, un último interés es identificar la existencia, si hay, de nuevos actores que busquen aprovechar las características de los enfrentamientos bélicos en el ciberespacio.

Gracias a lo anterior, la estructura pensada para este libro contiene cinco capítulos, que, al parecer del autor, cubren el análisis de los elementos que son determinantes para entender o hacerse la mejor noción posible sobre lo que significa la ciberguerra, cuáles son sus alcances y qué tipo de actores podrían llegar a ejercer esta práctica que desde la concepción ciberespacial y contemporánea también se plantea como algo bélico.

Se presenta, en primera instancia, un capítulo que, si bien no expone inmediatamente el concepto de *ciberguerra*, y aunque no se concentra directamente en las temáticas circundantes de esta, cumple la función de ofrecer un contexto tanto desde el punto de vista de la naturaleza de la guerra como de la evolución desde el sentido tecnológico; además, este apartado expone el fenómeno de los enfrentamientos bélicos a partir de las características propias y los dominios en los cuales se ha llevado a cabo, con el fin de comprender por qué lo que hoy se vive con la ciberguerra y el escenario donde esta se lleva a cabo son producto de una tendencia evolutiva de la guerra como tal.

En segunda instancia, se explica qué significa el ciberespacio como dimensión para trasladar la práctica de la ciberguerra. Es importante tener en cuenta, desde el punto de vista clásico de la guerra, que, si esta se ha llevado a cabo en diferentes escenarios del planeta, es porque se han posicionado elementos sociales, políticos, económicos y culturales en dichos espacios para que sean vulnerables frente al ejercicio bélico. Por esto, y ahora desde el sentido de la ciberguerra, es importante preguntarse por qué una dimensión considerada virtual, de comunicación e información, como el ciberespacio, podría ser una dimensión sumamente pertinente para trasladar una práctica bélica. Cabe preguntarse, como Estados y como sociedades, qué es lo que se ha hecho para que los actores armados que utilizan la ciberguerra encuentren allí un capital militar para lograr o alcanzar sus intereses particulares. Y por qué no, asimismo, para defenderlos. Este segundo capítulo contiene la comprensión del ciberespacio como el lugar donde se lleva a cabo la acción de la guerra cibernética, los factores que lo vuelven atractivo para ella y las herramientas que se encuentran al alcance de aquellos en capacidad de manejarlas, para hacer daño a través del mundo ciberespacial.

En tercer lugar, se muestra que ciertos elementos históricos que han cambiado la realidad de la sociedad llevaron a un replanteamiento o a una actualización de lo que se puede considerar, a grandes rasgos, como doctrina militar; en un primer momento, frente al cambio que introdujeron las tecnologías informáticas en el quehacer castrense, y en uno segundo, ante cómo la concepción de una cultura cibernética termina por complementar el proceso revolucionario dentro del ejercicio de la guerra a partir de las capacidades que ofrecen elementos como las computadoras, las redes informáticas y los dispositivos informáticos a los actores armados. Por supuesto, al asumir este tema automáticamente, hay que tomar como punto de partida la historia de las fuerzas militares constitucionales o de los Estados, es decir, esta revolución primera empieza en los ámbitos militares y después se convierte en un fenómeno transformador de otro tipo de actores irregulares.

Después de haber comprendido algunos elementos que determinan el contexto para la ciberguerra, en el cuarto capítulo, no solo se analizan algunas definiciones para poder entender qué significa la ciberguerra, sino que, además, y desde una perspectiva original o propia, se expone que la ciberguerra no debe entenderse como un fenómeno plano o unidimensional, sino que se ha abierto camino para atacar o impactar diferentes elementos que son de vitalidad para el Estado nación. Lo anterior partiendo desde la misma concepción de la cibernética como teoría de control, y su transversalidad en la creación del ciberespacio y la ciberguerra, por tanto, de los fenómenos que actualmente rodean el comportamiento individual y social de los actores internacionales.

En otro sentido, este libro ofrecerá a sus lectores una perspectiva de la ciberguerra que no solo se queda en la concepción de atacar otros sistemas informáticos, sino que lleva su planteamiento a un punto mucho más estratégico: los elementos que dependen de los sistemas informáticos que están siendo atacados. Lo anterior permitirá encontrar que la ciberguerra es capaz de afectar en un primer escenario la psicología de las personas o soldados que hacen parte de una sociedad y también los sistemas de transporte de abastecimiento de servicios públicos, por ejemplo. A su vez, nos permite interpretar como otro

elemento de la ciberguerra el armamento robótico con el que cuentan los ejércitos debido a su estrecha integración con sistemas informáticos, y en última instancia, las capacidades de la guerra cibernética de afectar toda la tecnología cíborg que se está diseñando para integrar los cuerpos de los seres humanos y hacerlos más eficientes.

En una última instancia, se mostrará que los actores irregulares, de manera más precisa actores terroristas o que se conciben como subversivos o revolucionarios frente a los proyectos estatales, han llegado a utilizar el mecanismo de la ciberguerra para ampliar sus capacidades de lucha ilegal e irrestricta contra la constitucionalidad estatal o de la seguridad del sistema internacional.

La metodología empleada es de carácter cualitativo para la construcción temática de este libro, basada, fundamentalmente, en la revisión de fuentes primarias y secundarias, debido a que la realización de trabajo de campo para entender un fenómeno que connaturalmente se plantea como global por el escenario virtual e informático en el que se da y que tiene una cobertura planetaria e indiferente a las fronteras físicas de los Estados es imposible de abarcar por completo. En segunda medida, lo que se buscaba lograr era un proceso de concienciación dentro de la academia en Colombia y generar una motivación para que otros investigadores vean en la ciberguerra un gran potencial de estudio.

El libro tiene apartados en los cuales se puede hacer referencia a algunos elementos específicos sobre la tecnología en la cual se rige el ejercicio de una guerra cibernética. Es valioso aclarar al lector que la presentación y exposición que podrá observar se fundamentará o se llevará a cabo a partir de un enfoque teórico y contextual. Esto quiere decir, de manera más clara, que, así como los realistas basaron sus fundamentos en política internacional entre los Estados hablando constantemente de la guerra sin necesidad de entrar en la explicación de temas, como la operación del armamento, el modo de combate, la fabricación de las armas, o elementos más puntuales, se logró entender el significado del uso de la fuerza, su funcionamiento, sus causas y efectos. Así, este libro busca dar una perspectiva general de los aspectos que rodean la ciberguerra, y por supuesto, cómo a partir de esta se puede alcanzar una serie de intereses que las unidades políticas

quieren tener. Por esto, el lector podrá tener certeza de que hablar de ciberguerra no se convertirá en un proceso ilegible, sino que, por el contrario, podrá encontrar un lenguaje amigable que posiciona el fenómeno en cuestión en un escenario de análisis cotidiano.

Así, se da la bienvenida a todos los lectores que tuvieron confianza e interés tanto en la ciberguerra como en el trabajo del autor.

Capítulo I
Cómo comprender la guerra y por qué se requieren dimensiones para llevarla a cabo

Ya que la primera pregunta que compone este subtítulo se refiere a cuestionarse sobre qué es la guerra, es importante que el lector, más allá de esperar un sinnúmero de definiciones sobre lo que se puede entender sobre este fenómeno, sepa que encontrará elementos teóricos y conceptuales que contribuyan a dilucidar si la ciberguerra se conecta con los aspectos que normalmente se reconocen en un contexto bélico. También es importante afirmar que la guerra y otros fenómenos, como la religión, la movilización, las organizaciones sociales, han hecho parte de la evolución del ser humano, por tanto, ayudan a entender su comportamiento y su desarrollo hasta llegar a lo que es hoy.

Caracterización de la guerra

A continuación, la intención es entender las causas y las características principales de la guerra, en busca de comprenderla para lograr asociarla con el concepto de ciberguerra como acontecimiento político y social. En la actualidad, contando con tantas obras, estudios y análisis sobre la guerra, se ha podido determinar que esta ha presentado diversas causas a lo largo de la historia. A partir de la visión más primitiva del realismo político, se entiende que la causa fundamental

primaria de la guerra ha sido la supervivencia del ser humano. Por supuesto, esta noción de supervivencia no es entendida como una lucha o una empresa por que la humanidad sobreviva como especie, sino que, gracias a la racionalidad, característica particular del hombre, esta emerge de unidades políticas conformadas por grupos sociales específicos, que buscan alcanzar intereses particulares. A lo largo del tiempo, estas unidades han transformado o evolucionado sus características.

Se tiende a utilizar diferentes rótulos para referirse a estas unidades: inicialmente, pueblos, tribus, clanes, para ir evolucionando a otras formas que son conocidas y que actualmente se denominan ciudades, Estados, imperios; y, finalizando esa etapa, los Estados monárquicos absolutistas. Siguiendo a Molina (2010), las causas de las guerras entre estas unidades se pueden encontrar en elementos como la ambición de conquista, los propósitos de colonización, de ubicación de puertos comerciales, de disputas religiosas o de incremento de los medios de subsistencia y del espacio vital de los pueblos. Pasados los siglos, cuando los pueblos colonizados llegaron hasta el punto de inflexión moral frente a las injusticias de los imperios, el objeto de la guerra fue lograr la independencia nacional —lo anterior se menciona para interés de un acápite final de este libro—. También podría señalarse el mismo objeto dentro de las guerras civiles.

Molina (2010) permite comprender de manera práctica cuáles han sido las causas de la guerra a lo largo de la historia, presentando lo que Carl von Clausewitz explicaría como el *objetivo político* de la guerra. No obstante, a los ojos de este mismo filósofo prusiano de la guerra, es preciso entender que también, cuando se originan escenarios de combate entre dos actores políticos, se debe tener en cuenta que el objetivo político pasa a un segundo plano y lo importante durante la coyuntura es obtener o alcanzar el *objetivo militar*. Por esto, y de una manera más cercana al estilo de Clausewitz, se podría aceptar que la guerra es una combinación de muchos compromisos distintos. Tal combinación puede o no ser razonable, y el éxito depende mucho de esto. Sin embargo, el compromiso en sí es lo más importante, ya que solo una combinación de compromisos exitosos puede conducir a buenos resultados: "Lo más importante

en la guerra será siempre el arte de derrotar al oponente en combate"[1] (Clausewitz, 1942, p. 4).

Reconociendo que derrotar al oponente en combate nunca significó para Clausewitz la aniquilación de un ejército o un pueblo, se podría afirmar que la guerra, por más violenta que sea, nunca ha tenido como objetivo destruir al ser humano, sino que, a través de la ejecución de actos de violencia que terminan afectando o asesinando al contrincante, se logra que la maquinaria de guerra opuesta cese su acción bélica. Por esto, es una cualidad esencial de quienes están en comando durante la guerra determinar cuál es el objetivo y que, en el momento de atacarlo, el enemigo quede sin energía para seguir luchando en el campo de batalla. No es fortuito así que para Clausewitz (1942) las hostilidades deban ir dirigidas a conquistar y destruir el poder armado del enemigo y tomar posesión de sus recursos materiales y demás fuentes de fuerza.

Para el caso concreto de los Estados nación, y por ende se habla de características modernas y westfalianas de ordenamiento político, todos los tipos de guerra (aun cuando habían obedecido a modalidades bélicas diferentes, dadas sus diferencias en objetivos, los tipos de ejércitos que empleaban, la técnica militar y la economía de guerra) compartieron rasgos comunes, ya que son catalogadas como formas de violencia organizada por Estados que recurren a ellas como mecanismo para ejercer control y legitimidad en espacios territoriales, establecer una demarcación entre lo interno y lo externo, mantener el orden interno, o bien proporcionar a los tomadores de decisiones capacidades disuasivas o de respuesta frente a la amenaza de un actor violento del sistema internacional (Fazio, 2003).

Por supuesto, y siguiendo a Fazio (2003), se trató de un momento en el que cobró validez intentar reproducir una clara diferenciación entre la guerra y los otros tipos de conflictos y violencias. Este compromiso "demandó que el Estado actuara como un agente organizador de la guerra; los ejércitos, aun cuando fuesen guerras civiles, se ordenaban jerárquicamente y la economía de guerra se estructuraba desde un punto de vista estatal" (p. 43).

1 Traducción del autor.

Por esto, el elemento sobre el cual se concentró la guerra en la modernidad se conceptualizó gracias a Clausewitz como *centro de gravedad*. En primer lugar, el centro de gravedad de Clausewitz es un "punto focal", no es una fuerza, ni una fuente de una ni una debilidad *per se*. Por otra parte, se encuentra exclusivamente donde existe un nivel de conectividad tal entre las distintas partes del enemigo que se forma un sistema o estructura que actúa con un grado sustancial de unidad, como un cuerpo físico. En tercer lugar, un centro de gravedad ejerce cierta fuerza centrípeta que tiende a mantener un sistema o estructura entera juntos; así, un golpe en el centro de gravedad lanza a un enemigo fuera del punto de equilibrio, incluso, puede causar que el sistema entero se derrumbe. Cuarto, usar el concepto requiere ver al enemigo holísticamente (Echevarría, 2003).

> Diferentes tipos de equipos e instrumentos se han introducido y utilizado en las guerras y han conformado diferentes tipos de guerra. La guerra convencional expresa la reducción de la capacidad militar de un oponente a través de la batalla abierta, la guerra no convencional es lograr la victoria militar a través de la aceptación, la capitulación o el apoyo secreto a un lado de un conflicto existente[2]. (Bazyan, 2012, p. 2)

Para interés de un acápite final del presente libro, podría señalarse que, dentro de las guerras civiles que han enfrentado a naciones a partir de antagonismo en las concepciones políticas, económicas, religiosas y étnicas de los componentes de la sociedad, estas también deberían considerarse como causa de las conflagraciones bélicas (Molina, 2010).

Conforme a lo que establece Fabricio, se pueden enumerar tres cualidades que deben estar presentes para hablar de guerra: un ambiente donde se pueda llevar a cabo, tecnologías militares para su desarrollo y la doctrina, entendida como "un conjunto de técnicas, estrategias, tácticas y prácticas que constituyen un enfrentamiento bélico y propone los pasos por seguir para ganar una guerra" (s. f.).

2 Traducción del autor.

El entorno

La guerra y el territorio han presentado una estrecha relación a lo largo de la historia. Con el surgimiento de la organización política, en el momento donde se evolucionó de jefaturas y pequeñas poblaciones a la figura del Estado nación, la principal razón de los enfrentamientos y la guerra como fenómeno era la clara necesidad de imposición como autoridad soberana por parte de quien aspiraba a convertirse en gobernante. Con el levantamiento de las primeras ciudades-Estado, la causa de la guerra fue la conquista del territorio de los pueblos vecinos (Molina, 2010, p. 113).

Respecto del primer componente, el ambiente, Sun Tzu planteaba siglos atrás que el terreno implica las distancias y hace referencia a dónde es fácil o difícil desplazarse, y si es campo abierto o lugares estrechos, puesto que influye en las posibilidades de supervivencia (Maggio, 2013, p. 82; Tzu, 1999, p. 3; Tzu, Von Clausewitz y Musashi, 2016, p. 13).

Por su parte, Droznes (2005) describe el ambiente por aquello que deben emplearlo como escenario de combate a partir de los tipos de superficie. Se pueden distinguir seis tipos de superficie, a saber: terreno accesible, terreno difícil, terreno neutro, de pasos estrechos, alturas abruptas y posiciones que se encuentran a gran distancia del enemigo. Para el autor, la formación natural del suelo es el mejor aliado del soldado.

La guerra puede ser clasificada por el ambiente o el área en la cual está ocurriendo. Esto significa que dos tipos de guerra, convencionales y no convencionales, afectan un área de acuerdo con las estrategias y la región donde necesitan actuar, y también puede ocurrir lo contrario: que los tipos de ambiente cambien el tipo de guerra. Muchos teóricos han intentado catalogar la forma de hacer la guerra conforme a los entornos donde se iba a llevar a cabo. Bazyan (2012) las cataloga entre guerra de la selva, guerra ártica, guerra de la montaña y guerra urbana. Ejemplos de guerra no convencional incluyen la guerra psicológica, la guerra biológica, la guerra electrónica y la guerra nuclear (p. 3).

La tecnología

Hablando en términos complementarios de tecnología, Martí (2006) describe la tecnología militar como aquella parte del desarrollo tecnológico que está enfocado en la aplicación a cualquier aspecto relacionado con la seguridad, la defensa y la eficacia en el enfrentamiento. Desde esta línea de pensamiento, las invenciones que allí se producen se enfocan en resolver los problemas fundamentales que se le presenten, entre ellos: la capacidad de destrucción, la protección propia, la movilidad eficiente, el mando, el control, las comunicaciones y el apoyo logístico.

En otro sentido, la relación de la guerra con la tecnología también se ha derivado de la capacidad de evolución de la industria bélica y lo que esta, al final del camino, le pueda ofrecer al soldado para desempeñar mejor su labor en el campo de batalla. Black, por ejemplo, permite comprender este aspecto cuando estudia, desde la perspectiva europea, lo que significó para los ejércitos propios de los siglos xv al xvii dejar atrás las ballestas para emplear armas de fuego como los arcabuces, las pistolas de la época, o bien armas largas como el mosquete o los pedreñales (2009, p. 98). Esta idea es reforzada con superioridad cuando se hace referencia a la gran obra de Martin van Creveld, *Technology and war.*

La evolución de las armas en la guerra, así como ha determinado la consecución de más poder para los Estados, también ha demandado responsabilidades en sus instituciones castrenses. Se trata de comprender que la transformación de la guerra no simplemente implica concebir o desarrollar nuevas tecnologías y arquetipos, sino también establecer las instrucciones que los militares deben seguir para poder aprovechar las capacidades de los armamentos en el momento de emplearlos. En palabras de Cooper (1997), las nuevas capacidades no solo deben desarrollarse físicamente y demostrar su superioridad, sino que la implementación exitosa de las innovaciones requiere un proceso complejo de integración en la estructura de las fuerzas militares y en los condicionamientos operacionales. La adopción de la innovación exige más que solo la capacidad de equipar una fuerza o un servicio militar con armas innovadoras; las organizaciones, los patrones

operativos y los procesos de toma de decisión también deben ser modificados para implementar la innovación como un elemento integral del carácter distintivo del servicio (p. 119).

La era de la máquina, como denomina Davis (1997) al momento de industrialización de las guerras desde finales del siglo XIX y hasta las guerras mundiales, fue una época dirigida a la concatenación de habilidades que promovieron el aprovechamiento del potencial militar de una manera cada vez más orquestada, jerarquizada e institucionalizada, pero, a su vez, descentralizada, como lo demostró la Wehrmacht (Fuerzas Armadas de la Alemania nazi) en la Segunda Guerra Mundial. Fue un momento de aprovechamiento de los vastos recursos de los Estados para dar vida a los ejércitos y a la guerra en masas (p. 82).

> Otra realidad alcanzada entre la tecnología y la guerra fue la cultura de la integración de artefactos preexistentes con nuevos adelantos en armamentos. Por ejemplo, hacer de los trenes de pasajeros máquinas de combate al emplazarlos como cañones y blindajes, instalar radios de comunicación en los diferentes medios de transporte, dotar de ametralladoras de alto calibre a los aviones de caza. Esta era culminó en la Segunda Guerra Mundial con la innovadora aplicación de la mecanización, la aviación y la tecnología de las comunicaciones al uso militar, lo que permitió al ejército alemán reintroducir la movilidad estratégica y operativa[3]. (Davis, 1997, p. 82)

Esto recuerda el panorama descrito por William S. Lind en *Fifth generation warfare*. A partir de los adelantos científicos que emergieron de la Guerra Fría, se dio un incremento exponencial frente a la cultura de la integración tecnológica señalada. En este momento, el desarrollo tecnológico no se trata específicamente de armas y vehículos, por ejemplo, sino de la información y de cualquier cosa que la industria militar quisiera integrar con esta. Gran parte de la maquinaria, los dispositivos, las armas, los vehículos e, incluso, los mismos soldados que fabricaron y alimentaron las dos superpotencias durante

3 Traducción del autor.

la Guerra Fría demandaron grandes cantidades de información para ejecutar sus funciones, tomar decisiones, emprender misiones y realizar operaciones, campañas o guerras. El aumento de la cantidad de información que debe ser digerida para que los propósitos bélicos se lleven a cabo se convirtió en una tarea tan compleja que obligó a la adaptación casi inmediata de la informatización y automatización de los procesos de recopilación, análisis y distribución de información, lo que permitió a comandantes y soldados responder a las velocidades adquiridas por el ejercicio de la guerra (Davis, 1997, p. 82).

Para comprender la evolución de la variable tecnológica, solo hay que imaginar lo que hubiera sido lanzar un misil nuclear balístico desde los Estados Unidos sin la capacidad científica y tecnológica para integrar estos procesadores de información que guiaran su trayectoria de vuelo hasta la antigua Unión Soviética, así como la altura a la cual activar el mecanismo de detonación al llegar a su objetivo; todo esto debía estar informatizado y automatizado. Como se expondrá a lo largo de este libro, la informatización de la guerra, y muchos asuntos importantes para los Estados y sus sociedades, abrieron la puerta a la ciberguerra, la cual contiene las mismas características de la guerra y, por tanto, afecta todos los escenarios en los que se desarrolla la vida humana.

Al recapitular, es posible decir que existen dos variables que han ayudado a determinar o dar ciertas connotaciones especiales a la guerra. Un primer elemento determinado como terreno y, de este, la descripción frente al hecho del lugar en que se va a combatir. Y un segundo, el elemento tecnológico, el cual, más allá de ofrecer categorías, termina siendo uno de los fenómenos más decisivos en el momento de abordar las grandes transformaciones de la guerra. Ahora bien, aunque ambos elementos puedan encontrarse en vías diferentes, tanto la definición de las condiciones en las que se va a pelear, así como el equipo diseñado y empleado para el enfrentamiento, demandan al unísono otra forma más de transformación: el cambio en la doctrina.

La doctrina

Como ya se había anunciado, los cambios que llevaron a la ciberguerra no solo se concentraron en las preguntas sobre *en dónde* se lucha la

guerra y *con qué* se puede luchar en la guerra, sino que también debe incluirse el *cómo* se debe luchar. La estrategia significa la combinación de compromisos individuales para alcanzar el objetivo de la campaña o la guerra. Retomando a Clausewitz, "es cierto que, si sabemos cómo luchar y cómo ganar, muy poco conocimiento extra es necesario en la guerra para combinar resultados afortunados. Es solo una cuestión de juicio y experiencia"[4] (Clausewitz, 1942, p. 17).

Es importante reconocer que este cambio en las técnicas para llevar a cabo la guerra se puede entender como una revolución, pero no simplemente siendo una condición existencial; por tanto, no es creada simplemente por la aparición de nuevas capacidades tecnológicas. Sin el reconocimiento y la explotación, donde ambos requieren una acción positiva, no puede haber revolución. "Crear una revolución es, por tanto, más que empujar los límites de la tecnología militar; es un proceso activo que requiere una adaptación efectiva por parte de los individuos y las organizaciones para que exista una explotación exitosa"[5] (Davis, 1997, p. 80).

> Este conocimiento ha tenido que ser transmitido a la estructura militar para que cada miembro o unidad que la compone tenga los parámetros de comportamiento que deba asumir a fin de dar respuesta a las diferentes situaciones que se pueden presentar en el ámbito castrense, o bien para la guerra, o bien para actividades de contención o rutina. Por esto, se requieren planes para preparar todos los instrumentos nacionales de poder para la guerra o conflicto, una guía práctica para preparar las Fuerzas Armadas y el liderazgo de estas para alcanzar objetivos estratégicos. El nivel doctrinal se refiere al empleo de fuerzas militares en un teatro de guerra o un teatro de operaciones para obtener una ventaja sobre el enemigo y así lograr objetivos estratégicos a través del diseño, la organización y la conducción de campañas y operaciones importantes. En la guerra, una campaña implica el empleo de las fuerzas

4 Traducción del autor.

5 Traducción del autor.

> militares en una serie de operaciones militares relacionadas a fin de lograr un objetivo común en un tiempo y un espacio dados. Los comandantes deben diseñar, orquestar y coordinar operaciones y explotar eventos tácticos con el propósito de apoyar los objetivos generales de la campaña[6]. (USAF College of Aerospace Doctrine, Research and Education, 1997, pp. 1-2)

De este nivel estratégico mencionado, se desprenden los niveles operacionales y tácticos (USAF College of Aerospace Doctrine, Research and Education, 1997, p. 2). El nivel táctico traduce el poder potencial real de combate que puede presentar un determinado Estado a través de sus fuerzas en las batallas y compromisos a través de decisiones y acciones que crean ventajas cuando están en contacto o en las proximidades del enemigo. Las tácticas se ocupan de los detalles de los juicios y son extremadamente sensibles al entorno cambiante del campo de batalla.

Por otra parte, y relacionados de forma directa con la doctrina o estrategia para llevar a cabo la guerra, los principios de esta son aquellos que expresan las reglas del pensamiento militar y las acciones militares que sirven como base permanente para la doctrina de combate. Su importancia relativa variará de un evento a otro. La lista de principios es una herramienta metodológica que difiere de ejército a ejército y de época en época. Mientas los principios se mantienen iguales, la lista se transforma según el tiempo y el lugar y la aplicación siempre depende del contexto (Mallick, 2009, p. 2). Los principios de la guerra han evolucionado durante un largo periodo. La evolución se puede clasificar en tres etapas: la primera, antes de la era de la guerra napoleónica; un segundo momento desde la era napoleónica hasta el final de la Segunda Guerra Mundial; y el último espacio temporal de la pos-Segunda Guerra Mundial (p. 3).

Modernizar los principios tradicionales de la guerra para los conflictos del siglo XXI no hace irrelevantes las versiones anteriores. Por el contrario, la intención de modernizar los principios de la guerra es capturar el espíritu de los existentes; por ejemplo, la información y la

6 Traducción del autor.

adaptabilidad. En resumen, el objetivo no es el reemplazo al por mayor de los principios tradicionales en sí, sino una renovación consciente del valor duradero de los antiguos. Los principios modernizados de la guerra podrían servir de guías para los líderes militares y civiles involucrados en los conflictos del siglo xxi (Dunlap, 2006, pp. 42-47). Tales principios podrían ayudar a la conducción de la guerra y ayudar a su organización, entrenamiento y equipamiento.

Dentro de este ámbito, también suele presentarse el proceso de absorción y adaptación a los nuevos instrumentos para hacer la guerra. Y este es un tema de suma vitalidad para la ciberguerra. El proceso de desarrollo tecnológico militar no ha tenido límites, pues siempre ha conllevado la introducción de nuevo armamento en las fuerzas militares, y se ha generado un constante conflicto entre el derecho en la guerra (*ius in bellum*) y las nuevas tecnologías. Muchas tecnologías, en especial las armas, se han percibido, al menos inicialmente, en desacuerdo con la ley existente.

La historia de la guerra ha sido puntuada repetidamente por las acusaciones de que ciertas armas nuevas son *ilegales*, por cuanto son *injustas* de acuerdo con los criterios prevalecientes de honor, equidad y demás, o porque su acción es más desagradable de lo que necesita ser. Cualquiera que sea la naturaleza y la fuerza de las objeciones al principio encontradas, las nuevas armas se deslizan en el uso común tan pronto como los objetores pueden adquirirlas por sí mismos, con lo cual la ley se adapta en consecuencia. Respecto de lo anterior, Liivoja (2015) explica que lo importante es que el cambio tecnológico no es un nuevo tipo de desafío para el derecho de la guerra. Lo que bien podría ser cierto, sin embargo, es que el cambio tecnológico está ocurriendo mucho más rápido ahora, con lo cual se exacerba el problema de que la ley tiende a quedarse atrás de la tecnología (p. 1173).

Los tres elementos que se han señalado como características de la guerra —entorno, tecnologías y doctrina— facilitan, hasta el momento, proseguir al elemento final de análisis. A continuación, un último paso sobre los escenarios en los que se lleva a cabo el enfrentamiento permitirá asumirlo como un tema central en la comprensión de la ciberguerra: dónde se lleva a cabo esta práctica y qué ocurrió para que existiera.

Las dimensiones de la guerra

A partir de la existencia y validez que han presentado los poderes en la historia militar, ha sido evidente que su aparición se debió a la tendencia del hombre a extender el empleo de la fuerza a nuevos escenarios de enfrentamiento con el fin de desarrollar nuevos tipos de estrategias para ganar la guerra. Consecuentemente, en una primera instancia, el conflicto se desenvolvió en los teatros terrestres. Luego, la conflagración se trasladó al mar y al océano. Y, finalmente, los conflictos alcanzaron la altura de la atmósfera y la estratosfera.

Ha sido cierto, de igual manera, que la extensión de los enfrentamientos armados a nuevos escenarios del planeta ha sido el producto directo de los procesos de desarrollo científico propio de las naciones y, por ende, de sus ejércitos. No hubiera sido posible, posteriormente a la constitución del poder terrestre, que surgiera el marítimo, el aéreo y espacial si la tecnología no lo forjara como posible; es decir, sin que los barcos y submarinos alcanzaran las grandes masas de agua, y las aeronaves y dispositivos espaciales ascendieran a las alturas y a la gravedad cero (Liang y Xiangsui, 1999).

Dimensión terrestre

El deseo de buscar escenarios donde dirimir los conflictos políticos se convirtió en una cuestión perenne a la guerra, debido, en primera instancia, a que el hombre, al ser un ser terrestre, se sintió más cómodo de ejecutar sus batallas en su medio natural. Como afirma Bellamy, la guerra es un fenómeno adscrito históricamente al escenario terrestre (1990, pp. 7-8). Pero la tecnología, por más primitiva que fuera, fue lo que permitió a los ejércitos empezar a ocupar otros espacios del planeta para extender la práctica bélica. Desde esta perspectiva, es importante tener en cuenta que la tecnología se presenta de dos formas: los desarrollos en materia de movilización y transporte y las armas e implementos para la batalla. A continuación, un breve recuento de algunos aspectos ilustrativos de este proceso de transición.

Es preciso reconocer que el primer propósito constructivo del hombre fue crear una industria armamentística que le permitiera protegerse

de los ataques de los animales (armas defensivas) o atacarlos (armas ofensivas) para conseguir comida y poderse vestir. Al fabricar sus primeras armas, el hombre no piensa en la guerra, sino en su supervivencia. "La guerra sería el producto paulatino cada vez que el hombre se convirtió en sujeto organizado en unidades políticas y vinieron los conflictos por intereses comunes" (Gutiérrez, 1995, p. 85)

Esquemáticamente, se puede dividir la evolución de las armas terrestres para enfrentar la guerra en cuatro etapas durante la modernidad. La primera, la de las armas de fuego durante la época napoleónica; la segunda, durante la Revolución Industrial hasta la Segunda Guerra Mundial; la tercera, los avances durante la Guerra Fría; y, por último, los adelantos del siglo xxi (Martí, 2006).

Introducir el arma de fuego en la guerra fue una innovación de gran magnitud en el ámbito militar. Su potencia explosiva creó la base para desarrollar artefactos con un poder de destrucción mucho mayor. Sin embargo, las primeras armas eran pesadas, lentas e imprecisas. Estas se podían clasificar en dos tipos: individuales, manejadas por una sola persona, y las grupales, específicamente los cañones (Martí, 2006). Este periodo también marcó el surgimiento de ejércitos profesionales, permanentes. "La introducción de las armas pequeñas, como el mosquete, cambió radicalmente el rostro de la guerra. Por primera vez, los militares tenían un arma portátil, relativamente precisa, fiable y mortal"[7] (Mehan, 2014, p. 43).

> Así, el arcabuz fue evolucionando hacia el mosquete y, a mediados del siglo xix apareció el fusil Mauser, que disparaba tiro a tiro. Posteriormente, ya en el siglo xx, aparecieron los fusiles con un tipo de cierre más avanzado que permitían tirar también a ráfagas. (Gutiérrez, 1995, p. 87)

> Los grandes avances en el conocimiento de la física, la química y las matemáticas que tuvieron lugar en el siglo xviii trajeron consigo en el siguiente siglo una Revolución Industrial gracias a la cual se produce un cambio tecnológico de gran magnitud

7 Traducción del autor.

> en los campos de los materiales, la propulsión, la munición y la electricidad que supondría una mejora sustancial del armamento, que a la postre se traduciría en una nueva forma de guerra. (Martí, 2006, p. 101)

> Hacia 1877 el fusil de repetición fabricado en acero se convirtió en el arma estándar de los ejércitos. La nueva munición aumentó su velocidad hasta superar el sonido, creciendo así su poder destructor debido a su mayor energía cinética […]. En este mismo periodo aparece la ametralladora moderna. (Martí, 2006, p. 116)

> Respecto del transporte, al principio de la Primera Guerra Mundial surgió la idea de que un vehículo blindado sobre orugas podía ser capaz de cruzar con impunidad las trincheras enemigas. Si se le equipaba con cañones apropiados, este vehículo podía destrozar las ametralladoras enemigas y abrir camino a un avance general. En el año 1920, las fuerzas terrestres tenían gran cantidad de fuerzas dotadas de fusiles de cerrojo, muchos morteros y artillería más pesada. En 1940, tenían más y mejores vehículos blindados y de un 5 a un 10 % de las tropas eran unidades mecanizadas. (Gutiérrez, 1995, p. 89)

Por otro lado, la Segunda Guerra Mundial vivió un desarrollo nunca visto de máquinas de guerra, en el marco de la Revolución Industrial. Antes de finalizar la contienda, aparecieron en el escenario vestigios de una nueva clase de tecnología destinada a dar un valor superlativo a la acción de los ejércitos en el campo de batalla: los carros de artillería (Lewis, 2002). A manera de contexto, los ejércitos avanzados todavía estaban estructurados, como lo habían sido desde la década de 1940, alrededor de fuerzas blindadas complementadas por tropas de infantería ligera que se mueven en vehículos y camiones.

El mundo vio el surgimiento del Abrams estadounidense, el Challenger II británico, el Leopard II alemán, el Merkava Mk. 4 israelí y, por supuesto, los tanques rusos T-80 y T-90. Todos los tanques modernos tienen torretas estabilizadas, capacidades de visión nocturna, localizadores de rayos láser y equipos de orientación que les permiten luchar en condiciones adversas, en movimiento o en

la oscuridad, que hubieran obstaculizado los modelos anteriores. Además, la armadura compuesta o reactiva ofrece mucha más protección que en años anteriores, y las armas principales que disparan rondas de uranio empobrecido tienen mucho más poder de penetración (Boot, 2006, p. 14).

Se podría señalar que la informatización y automatización de las cuales se habló en páginas precedentes también impactaron el desarrollo de las capacidades de actuar en tierra. En los Estados Unidos, a partir de 1980, se registró el inicio de proyectos en torno al desarrollo de carros militares sin tripulación (*unmanned ground vehicles* [UGV]), con las posibilidades de efectuar lanzamiento de armas, reconocimiento, vigilancia y adquisición de objetivos y eliminación de artefactos explosivos (Thong, Howe y Lee, 2012, p. 16).

Dimensión marítima

En la dimensión marítima, la evolución tecnológica también afectó el progreso del poder naval. Al igual que el combate en tierra, las luchas en los mares y océanos ya se habían institucionalizado a gran escala prácticamente desde las guerras entre el Imperio persa y los griegos. El desarrollo de acorazados y barcos desde el siglo XIX y la puesta en escena de submarinos y portaaviones en el siglo XX permitió el desarrollo de, como se podría expresar conforme a las ideas del almirante Thayer Mahan, una verdadera estrategia geopolítica de control de las vías de transporte comercial marítimo y un mecanismo de disuasión frente a un ataque a la nación (Mahan, 1911).

Una flota de buques podría controlar los mares y garantizar a una nación una posición como una potencia marítima. La fuerza naval se midió en el número de buques "líder" o de clase líder. Con esta magnitud de barcos y tipos de barcos, la dependencia tecnológica de la guerra en esta dimensión no se hizo esperar y, así mismo, se derivaron nuevas tácticas de la guerra naval (Fleming, 1993, p. 1). Con esa fuerza, surgió la capacidad de influir en el estatus económico y político de la nación. Además, si esa nación estaba involucrada en algún tipo de operación de tierra ofensiva o defensiva, las fuerzas navales se emplearían a menudo. Su empleo tendría una influencia decisiva en el resultado. Una vez que

ese compromiso fue activamente perseguido, la Marina se convirtió en un elemento clave en la estructura defensiva de la nación al mantener una postura en general ofensiva (pp. 3-4).

> El avance tecnológico trajo rápidamente a las flotas navales de los Estados buques más resistentes en combate. La propulsión de vapor permitió a los buques decidir sus destinos con libertad, ya que el viento no era un factor determinante en la batalla. El trabajo con el acero, propio de la industrialización, permitió generar blindajes a los barcos de guerra, así como armamento con capacidad explosiva. Esto dio origen al acorazado moderno a finales de 1800; recordemos los buques pre-Dreadnought y Dreadnought. (pp. 6-7)

Otro ejemplo de la expansión y el avance tecnológico de la guerra en la dimensión marítima fue la invención del torpedo autopropulsado en Gran Bretaña en 1866. Este primer modelo era un bote de hélice que portaba una carga explosiva, en el cual un mecanismo de relojería accionaba la hélice y uno de percusión hacía funcionar la carga. Alcanzaba un blanco a 1600 m a una velocidad de 40 nudos. En la Primera Guerra Mundial, los alemanes adaptaron el torpedo al submarino, lo que causó el 60 % de las pérdidas aliadas en navíos mercantes (Gutiérrez, 1995, p. 88).

Nada revolucionó tanto la guerra naval como los submarinos, los cuales se pusieron a prueba por primera vez durante la guerra civil norteamericana. En 1864, el submarino confederado CSS *H. L. Hunley* hundió el USS *Housatonic* en Carolina del Sur. Desde entonces, los submarinos han tomado muchas formas diferentes y se han utilizado en diferentes guerras (Khan, 2015). Durante la primera mitad del siglo XIX, se diseñaron varios tipos de submarinos, entre ellos, el Ictineo de Monturiol, movido por máquinas de vapor. En 1903, los periscopios proporcionaron a los submarinos el medio por el cual podían apuntar los torpedos hacia sus blancos mientras permanecían sumergidos (Gutiérrez, 1995, p. 89).

> Ya para la década de 1960, algunos submarinos estaban equipados con misiles balísticos intercontinentales, pero su orientación

> era tan imprecisa que no tenía sentido equiparlos con ojivas convencionales. Los misiles balísticos se convirtieron en un pilar de la disuasión nuclear. El desarrollo de misiles de crucero precisos que comenzaron en la década de 1970 permitió que los submarinos y los combatientes superficiales golpearan los blancos de la tierra a centenares de millas con la artillería convencional[8]. (Boot, 2006, p. 16)

> En la década de 1960, la marina de guerra de los Estados Unidos desarrolló un vehículo submarino controlado por cable para operaciones de rescate y recuperación de objetos desde el fondo del océano. En la década de 1970, los vehículos subacuáticos autónomos tempranos fueron desarrollados por los Estados Unidos y la antigua Unión Soviética. (Thong, Howe y Lee, 2012, p. 17)

Los misiles Tomahawk son otro ejemplo de cómo la guerra instó a las naciones a proponer nuevas tecnologías. Son misiles de crucero de largo alcance que tienen la capacidad de volar a baja altitud a una velocidad increíble. Pueden ser utilizados por los buques para golpear cualquier área de superficie. Las posibilidades de una falta son casi inexistentes, porque estos misiles vienen con un receptor GPS (*global positioning system* 'sistema de posicionamiento global') que se utiliza para localizar la ubicación del objetivo con mayor precisión (Khan, 2015).

Dimensión aérea

Se harán ahora algunas consideraciones acerca de la dimensión del aire. Hasta la Primera Guerra Mundial, los líderes militares habían concebido el avión principalmente como una herramienta de reconocimiento y de localización de artillería. A finales de 1918, sin embargo, el avión ya estaba realizando otras misiones, que incluyen la superioridad aérea, el bombardeo estratégico, la interdicción, el apoyo aéreo cercano y el transporte aéreo. La aviación siguió evolucionando después de la

8 Traducción del autor.

guerra, como lo demuestra el aumento de los rangos, las altitudes y las velocidades de los aviones. Estas capacidades crecientes permitieron vuelos transcontinentales y transoceánicos, así como el servicio de aerolíneas y el correo aéreo. El Servicio Aéreo del Ejército de los Estados Unidos (U.S. Army Air Service) realizó el primer vuelo alrededor del mundo en 1924 y demostró el alcance global de la potencia aérea. Los monoplanos de metal con cabinas cerradas y el tren de aterrizaje retráctil reemplazaron los biplanos de piel abierta y de cabina abierta con ruedas fijas. El Cuerpo Aéreo del Ejército, establecido en 1926, desarrolló grandes bombarderos de largo alcance y una doctrina para su uso (Haulman, 2003).

Es importante conocer la evolución de los avances tecnológicos que han permitido a los actores, principalmente políticos, comerciales y militares, gobernar el cielo. El primer Piper J-3 Cub salió a la venta en 1938. Con la guerra que amenazaba en Europa, el pequeño Cub se convirtió en un entrenador principal para el Programa de Capacitación de Pilotos Civiles. Para el final de la Segunda Guerra Mundial, el 80 % de todos los pilotos militares de los Estados Unidos recibieron su entrenamiento primario en un J-3. La construcción simple del Piper, su bajo costo y su manejo dócil lo convirtieron en uno de los aviones más populares de todos los tiempos (Clarke, 2015).

Poco antes de la Segunda Guerra Mundial, los científicos e ingenieros británicos descubrieron cómo utilizar la reflexión de las ondas electromagnéticas para localizar aviones a una distancia que permitiera a pilotos de caza interceptarlos. La serie de estaciones radar que montaron los ingleses, atentas a los vuelos procedentes del continente, se mostraron determinantes en la señalización de aviones de bombardeo alemanes durante la batalla de Inglaterra. El radar siguió desarrollándose muy rápidamente durante la guerra y encontró nuevos usos en la navegación de los aviones, el tiro y la técnica aeroespacial (Gutiérrez, 1995, p. 90).

El Supermarine Spitfire fue el único avión británico en producción continua durante toda la Segunda Guerra Mundial. Se convirtió en la espina dorsal del Royal Air Force Fighter Command y fue más conocido por derrotar a la Luftwaffe alemana durante la batalla de Inglaterra. Fue diseñado para llegar a velocidades más altas que muchos otros combatientes (Clarke, 2015).

Aunque los problemas del motor retrasaron su estado operacional con la Luftwaffe alemana, en 1942 el Schwalbe (Swallow) se convirtió en el primer avión de combate jet del mundo. Su efectividad se vio obstaculizada por problemas de fiabilidad del motor y ataques aliados a los suministros de combustible alemanes. El avión también tenía una vida útil limitada de producción, pero su velocidad y maniobrabilidad eran incomparables en ese momento y su diseño todavía se estudiaría y se aplicaría a futuros aviones de combate como el F-86 Sabre. El Bell X-1 es un avión de investigación supersónico famoso por ser el primer avión tripulado capaz de romper la barrera del sonido en 1947. Fue el primero en combinar tecnologías de aviones y cohetes. Estos aviones experimentales se usaron para probar sistemas avanzados y aerodinámicos, y las lecciones aprendidas impulsarían a los Estados Unidos en su carrera en el espacio. Además, los datos de vuelo supersónicos recogidos de pruebas X-1 resultaron invaluables para aquellos que diseñaron futuros aviones de combate estadounidenses (Clarke, 2015).

La llegada de cazabombarderos y de aviones espías de la Guerra Fría ha configurado el poder aéreo contemporáneo (Douhet, 2009). Pero también el ejemplo más reciente del avance en la tecnología tiene que ser los aviones furtivos. Los radares están ahora activos en casi todos los países, lo que significa que nada pasa desapercibido. Sin embargo, es una situación completamente diferente si existen aviones furtivos que se esconden de los radares en cierta medida. La tecnología Stealth hace que sea realmente difícil para los enemigos detectar el avión, lo que quiere decir que van a necesitar tiempo para encontrarlo, seguirlo y luego defenderse contra él. Los Estados Unidos tienen tres tipos de aviones sigilosos: F-35 Lightning, F-22 Raptor y B-2 Spirit (Khan, 2015).

El primer uso de la tecnología de aire no tripulada se remonta a la Primera Guerra Mundial, cuando los aviones no tripulados controlados por radio fueron utilizados como "bombas volantes" por los Estados Unidos. A partir de entonces, tales vehículos aéreos no tripulados fueron usados como señuelos. Luego, se utilizaron para fines de reconocimiento en la década de 1960 y, para la década de 1970, los Estados Unidos experimentaron con ellos para propósitos

de combate activo. Sin embargo, no fue hasta la década de 1990 cuando los vehículos aéreos de combate no tripulados fueron desarrollados y utilizados en operaciones, con el avance de enlaces de comunicación más confiables (Thong, Howe y Lee, 2012, p. 16).

El Predator fue el primer dron militar (aunque el término más preciso sería "vehículo aéreo no tripulado"). Se hizo famoso por su papel en la lucha contra los talibanes en Afganistán. El Predator puede ser pilotado remotamente para volar sobre un curso de 400 millas náuticas, rodear su objetivo por hasta 14 horas y volver a la base. El uso extensivo del Predator, no solo para recopilar información, sino también para disparar misiles dirigidos por láser Hellfire, marcó el comienzo de la era moderna de la guerra extensa de los aviones no tripulados por el Ejército estadounidense (Clarke, 2015).

Dimensión espacial

A manera de cierre, es un deber tener en cuenta el paso más grande que ha dado el ser humano para buscar nuevas dimensiones dónde realizar la guerra: la dimensión del poder espacial. Esta, al igual que su consideración como un poder estatal (militar), ha sido una cuestión de exclusividad. Aunque en la actualidad existen países que por sus PIB y su capacidad de deuda pública no pueden invertir demasiados recursos en sus presupuestos de defensa, de una manera u otra, han logrado desarrollar o adquirir capacidades para proteger o asumir una conducta bélica en la dimensión terrestre, marítima y aérea. No obstante, tanto alcanzar la dimensión espacial, la estratosfera del planeta y la Luna, como constituir un programa científico y tecnológico que permitiera desempeñar misiones y tácticas para cumplir a su vez estrategias, han sido un privilegio de pocos Estados nación. Es probable que en la actualidad en gran parte de los países del mundo se estén desarrollando artefactos que permitan a sus usuarios públicos o privados desarrollar nuevos procesos, pero, si se habla desde el punto de vista de la seguridad nacional, y de la guerra, todo se traduce en cuál es el número de países que en realidad tienen la capacidad de colocar dichos recursos en esta dimensión.

En otras palabras, y según Fitzgerald (2001),

> el poder espacial se aplica en el caso específico de los actores del sistema internacional que lograron, y podrían hacerlo en el futuro, desarrollar la tecnología para rebasar la atmósfera terrestre mediante cohetes de propulsión o transbordadores, y poseer el control del espectro electromagnético del planeta mediante los satélites de carácter geopolítico, es decir, artefactos encaminados al aumento del poder político-militar, y no simplemente comercial[9]. (citado por Haulman, 2003, p. 11)

Debe reconocerse, como lo comenta Millán, que el reto más grande que se ha presentado para consolidar la conquista del espacio exterior ha sido garantizar en primera instancia un acceso seguro a este. Situar una astronave en órbita demanda un mecanismo —motor— de propulsión que genere una velocidad mínima de 28 440 km/h (2000, p. 209).

Se podría señalar entonces que el poder espacial presentó tres momentos de cercanía con la guerra. Primero, en lo que podría denominarse las raíces del poder espacial, momento que se caracteriza por el desarrollo de la bomba Aggregat 4 (A4), o más conocida como la bomba V2 en Alemania durante la Segunda Guerra Mundial (National Aeronautics and Space Administration [NASA], s. f.). Segundo, las décadas de 1950 a 1970, cuando alcanzar el espacio y poner el primer hombre en la Luna se convirtieron en una cuestión de orgullo nacional, la cuestión más representativa de la guerra político-cultural de aquel enfrentamiento capitalismo versus comunismo. Y tercero, entre las décadas de 1980 y 1990, momento en el que las capacidades espaciales se enfocan desde una perspectiva político-militar en garantizar aspectos de la seguridad nacional, como evitar ataques de misiles balísticos intercontinentales, o desde plataformas submarinas que lograran acercarse al rango de distancia requerido para lanzar artefactos nucleares (Grauer, 2013).

Wernher von Braun fue reconocido durante la Segunda Guerra Mundial por haber construido la bomba V2 (A4) para el Ejército alemán. Aunque técnicamente el arma no estuvo dispuesta en su capacidad máxima para ser empleada en la guerra, en especial por los

9 Traducción del autor.

bombardeos aliados sobre la fábrica, se reconoció el ingenio de Von Braun para construir un misil (cohete) con capacidad de alcanzar objetivos a 200 km de distancia, y se calculó que alcanzó altitudes que oscilaban entre los 50 y 55 km de altura; además de esto, tenía una capacidad destructiva de una tonelada de trinitrotolueno (TNT). Al finalizar la guerra en 1945, cargas de V2 y algunos de sus ingenieros fueron trasladados a los Estados Unidos. Uno de los mejores resultados de la Operación Paperclip fue el traslado de Von Braun a Norteamérica, pues su conocimiento fue determinante para todo el desarrollo de misiles, como el Redstone, en la División de Operaciones de Desarrollo de la Agencia de Misiles del Ejército de los Estados Unidos, así como para los primeros cohetes de la NASA (National Aeronautics and Space Administration 'Administración Nacional de la Aeronáutica y del Espacio'), como fue el Júpiter C (Haulman, 2003, p. 71).

Respecto de la segunda etapa que se planteó, se podría señalar que la antigua Unión Soviética inició ganando la carrera espacial de la Guerra Fría al poner en órbita el satélite Sputnik I y el Sputnik II, en el cual además viajó Laika, el primer ser vivo que el hombre puso en el espacio (NASA, s. f.).

Durante 1958, la Fuerza Aérea de los Estados Unidos (United States Air Force [USAF]) puso en órbita el primer satélite artificial de comunicaciones, artefacto que un día después de posicionado en órbita logró transmitir un mensaje de Navidad del presidente Dwight D. Eisenhower, el primer comunicado de una persona transmitido desde el espacio (Haulman, 2003, p. 84). En 1960, la NASA inició el programa Mercurio, el cual, a diferencia de la antigua Unión Soviética, no solo buscaba llevar dispositivos y animales al espacio, sino a los primeros seres humanos (p. 85). En respuesta a lo anterior, Yuri Gagarin, un cosmonauta soviético, fue el primero en orbitar la Tierra; aunque lo prosiguiera el astronauta Alan Shepard unos meses después gracias a las metas alcanzadas por Mercurio. Al final de 1950, los Estados Unidos y la antigua Unión Soviética transportaron satélites al espacio, con lo cual transformaron la comunicación, la navegación, la inteligencia y la exploración.

Es evidente que uno de los grandes paradigmas de la guerra en el espacio se dio en 1969 cuando, desde el Centro Espacial Kennedy en

Florida, se coordinó toda la operación para permitir que, de un módulo lunar de la NASA, la tripulación de Apolo 11, Neil Armstrong, Michael Collins y Edwin E. Aldrin fueran los primeros terrícolas en caminar sobre el satélite natural de la Tierra (Haulman, 2003, p. 107).

En una última etapa, el programa militar estadounidense lanzado por el presidente Ronald Reagan en 1983 con la denominación de Iniciativa de Defensa Estratégica fue rotulado por los medios de comunicación como "guerra de las galaxias" (Fitzgerlad, 2001). El objeto del programa consistió en disponer de capacidades balísticas, ubicadas desde baterías terrestres y plataformas espaciales, para destruir los misiles nucleares dirigidos a blancos estadounidenses. El procedimiento previsto para esto consistía en detectar cuanto antes el disparo de los misiles, seguir sus trayectorias y destruir las cabezas nucleares a suficiente altura para que sus efectos no afectasen a los blancos. Todo esto debería conseguirse en pocos minutos, los veinte más o menos que medían entre los momentos del disparo del misil y del impacto de la cabeza de guerra en el blanco (Millán, 2000, p. 219). El espacio es también objeto de una utilización muy importante en programas militares para muy diversas misiones. Su uso ha sido fundamental en la previsión y el control de crisis y en operaciones como la guerra del Golfo Pérsico de 1990 (p. 218).

Actualmente, una cantidad creciente de vigilancia, comunicaciones y trabajo de inteligencia está siendo realizada por aviones no tripulados y satélites. En 2001, los Estados Unidos tenían aproximadamente cien satélites militares en órbita. Este país gasta más de USD 15 000 millones al año en el espacio militar, por lo cual ha logrado que muchos de sus satélites de vigilancia puedan visualizar un objetivo de seis pulgadas de tamaño desde 150 millas de altura. Una nueva generación de satélites utiliza tecnología furtiva para que otros países no puedan rastrear sus movimientos y así saber cuándo esconder el equipo de los ojos estadounidenses (Boot, 2006, p. 21).

Durante la última década del siglo XX, la tripulación del transbordador espacial Endeavour completó la primera misión de montaje de la Estación Espacial Internacional, que incluyó la entrega y el acoplamiento de Unity, el primer módulo de los Estados Unidos, al módulo de Zarya, lanzado por Rusia. Los miembros de la tripulación también

lanzaron la USAF MightySat I para evaluar materiales compuestos, células solares avanzadas y otras tecnologías. Desde Cabo Cañaveral (Florida), un cohete Delta II lanzó Stardust, la primera nave espacial diseñada para interceptar un cometa y devolver muestras a la Tierra. La NASA programó que Stardust se reuniera con el Cometa Wild-2 el 2 de enero de 2004. China lanzó, supervisó, controló y desembarcó Shenzhou, su primera nave espacial no tripulada (Haulman, 2003).

Antes de concluir este capítulo, es valioso reconocer que a lo largo de estas páginas han faltado innumerables hechos, armas, operaciones, procesos de desarrollo científico, características y causas de la guerra que sin duda han sido determinantes en la historia de este fenómeno. No obstante, es importante recordarle al lector que la intención no era hacer un barrido específico de toda la evolución de la tecnología en la historia de la guerra o bien de todos los aspectos de la naturaleza que pueden definir esta práctica humana. La intención era ofrecer algunos datos para que el lector pudiera hacerse un contexto básico de unos elementos que son destacables en lo que, a juicio del autor, pueden dar explicación y lucidez frente al fenómeno de la ciberguerra, el cual para algunos es novedoso o confuso.

Se ha discutido sobre temas que han sido conceptualizados por muchos analistas para llegar a la noción o la idea de qué es lo que significa cuando dos actores políticos entran en un estado de guerra, y qué debe existir en este escenario para suponer que lo que está pasando allí puede recibir o amerita la categoría de guerra. De ahí la importancia de haber analizado los primeros elementos constitutivos de la guerra, que fueron planteados en este capítulo. Y, en un segundo punto, reconocer, como se verá de manera mucho más clara en el siguiente capítulo, la guerra y el desarrollo científico y tecnológico a lo largo de la historia en las dimensiones donde se llevó a cabo.

Para dar un enfoque mucho más claro en torno a estas capacidades tecnológicas, se mostró cómo influyeron en el fenómeno de la guerra, también dando a entender que la invención humana ha permitido en primera instancia que el hombre afiance las prácticas bélicas en su espacio connatural, que es la tierra. Además, se presentan nuevos escenarios, los cuales dominados por las capacidades humanas permitieron simultáneamente reconocer el desarrollo de artefactos que

pudieran gobernar dimensiones que parecían imposibles de alcanzar. Asimismo, cómo estos preconceptos fueron permeados por unas capacidades tecnológicas para permitir enfrentamientos en un entorno en el cual no existe un desempeño de manera connatural como sí lo pueden hacer otras especies.

Cuando se piensa en el mar, el aire y en el espacio como dimensiones que se alejan de la naturaleza y las características de hábitat propias del hombre, ha existido un aprendizaje sobre la generación de actividades como seres humanos en los espacios marítimos y oceánicos, aéreos y espaciales, si bien siempre se ha hallado la imposibilidad de vivir en dichos espacios de manera permanente. Así es que, en últimas, con mayor razón, el desarrollo científico y tecnológico permitió expandir las fronteras de la guerra para llevarla al mar, al aire y, aún más, al espacio. Y está, por supuesto, la otra idea que se quería aclarar a partir de este capítulo, pues, en últimas, y ya para concentrarse verdaderamente en competencia, esta evolución tecnológica que ha sobrepasado los límites permitió una perspectiva específica y diferente que se consolidará en una nueva dimensión para la guerra, que es de lo que trata el siguiente capítulo.

Capítulo II
Comprensión de la dimensión y las armas de la ciberguerra

Antes de iniciar este capítulo de manera formal en cuanto al tema que aquí se tratará, es relevante hacer una aclaración previa. Si bien el capítulo precedente se inició, desde un enfoque de la naturaleza de la guerra, estableciendo algunos aspectos tanto definitorios como característicos de esta práctica, cabe señalar que este no va a presentar la misma estructura en relación con lo mencionado. Es un capítulo que se constituirá más desde el enfoque que tiene el primero en su segunda parte, es decir, donde se intenta construir la idea de que la guerra frente a un concepto dimensional ha sido una cuestión tanto evolutiva como paralela. Y se quiere ver así, en últimas, que todas las dimensiones de la guerra y todos sus poderes siguen desarrollándose continuamente hoy, así que, si bien en algún momento de la historia primaron algunos escenarios, actualmente la cuestión sigue siendo transversal o se presenta como transversal.

No obstante, asumiendo esta perspectiva, desde un concepto más consecutivo o evolutivo, el presente capítulo tiene su fundamento, en primera instancia, en recalcar la idea de que la consecución o construcción del ciberespacio, y su determinación como un espacio viable para generar nuevas actividades de violencia o fuerza enmarcada dentro del concepto de la *guerra*, fue el momento en el cual precisamente esta práctica encontró una nueva dimensión para extender sus límites.

Por esto, se asumirán algunas definiciones ya desde una perspectiva de la seguridad y de lo que significa el ciberespacio para la seguridad nacional de los Estados. Por supuesto, se seguirá manejando una lógica teórica y conceptual y el foco estará más en una explicación de fenómeno que de casos.

En una segunda instancia, se proporcionará una explicación desde la perspectiva del espacio de lo que significa el concepto de *centro de gravedad*, que fue explicado en el capítulo anterior y con el cual se llegó a la conclusión de que, a través del ejercicio de la guerra, más allá de querer aniquilar o destruir a un pueblo, aunque en ciertos casos de la historia sí haya sido ese el motivo, lo que esperan los estrategas militares es poder atacar a aquello que es de vitalidad para su enemigo y su continuidad en el campo de batalla. Al llegar al capítulo enfocado en los casos y las formas de ciberguerra, el lector observará que en muchos de ellos el ejercicio de lo que es denominado *ciberguerra* ya no se encuentra relacionado, como el término mismo lo indica, con un espacio de guerra o con una condición de guerra, sino que muchas veces lo que está de por medio es un conflicto de intereses que son vitales para los Estados nación.

En última instancia, se analizará qué es lo que se puede entender como armas dentro del ciberespacio, pues, a partir de lo planteado en el capítulo 1, poder hablar de guerra desde la perspectiva que interesa a este libro significa la sumatoria de varios elementos. Primero, y como es justo aclarar en este momento, implica la existencia de unas dimensiones que desde la característica clásica fueron dispuestas de manera natural por el planeta Tierra. Por ende, el primer elemento que se debe tener en cuenta es un espacio en el cual se puede desarrollar la práctica de la guerra —en este caso ya se hará hincapié en el ciberespacio como un nuevo campo de batalla—.

Segundo, y en un sentido lógico, al hablar de una práctica bélica que implica el uso de la fuerza y la violencia por parte de los Estados y sus ejércitos, y como se analizará al finalizar el libro, de otro tipo de actores no estatales que ya han sido reconocidos como ejecutores de guerra, se deberá analizar otro elemento: cuáles son las armas que se llevan al ciberespacio y cómo se configuran como armas al permitir ese objetivo militar de atacar aquello que es importante para un Estado enemigo o

un Estado que puede estar atentando contra los intereses o la seguridad de una nación.

Si aún existen cuestionamientos sobre por qué no se ha definido la ciberguerra, el presente libro, para seguir una línea lógica de lo expuesto en el capítulo anterior, considera preponderante entender, primero, el escenario en el cual se lleva a cabo toda la acción ciberespacial y cuáles son las herramientas que se pueden usar, es decir, *dónde* y *con qué* se lleva a cabo la guerra cibernética, para luego concebir el *qué*, esto es, como fenómeno y cuáles son sus características, sin necesidad de desviarse en conceptos clave para comprenderla. Por tanto, la intención es entender el contexto para luego poder sumergirse estrictamente en este y las clasificaciones que de él se derivan.

De igual forma, y con el propósito de lograr ubicar al lector, una definición general de ciberguerra es propuesta por Arquilla y David Ronfeldt (1997), en la cual se afirma que es

> conducir y prepararse para llevar a cabo operaciones militares de acuerdo con los principios relacionados con la información. Significa interrumpir, si no se logra destruir, los sistemas de información y comunicación, que ampliamente definidos incluyen la cultura militar, es decir, aquella información en la que un adversario confía para operar de forma correcta: quién es, dónde está, qué puede hacer en diferentes ocasiones, por qué iniciar un conflicto, qué contraatacar primero, etc. Significa tratar de saber todo acerca de un adversario mientras se evita que sepa mucho sobre el atacante. Significa poner el equilibrio de información y conocimiento a favor propio, en especial si el equilibrio de fuerzas no lo está. Significa usar el conocimiento para que haya que gastar menos capital y trabajo[10]. (p. 30)

En los siguientes capítulos, se hará un análisis mucho más detallado y completo de lo que representa la ciberguerra, y los cambios que esta ha generado.

10 Traducción del autor.

El ciberespacio como dominio

Con la globalización de las tecnologías informáticas y la consecuente configuración del ciberespacio, se estructuró un escenario para trasladar la lógica de la guerra. Como ya se formuló hace varios años, se podría entender el ciberespacio como la representación de la quinta dimensión de la guerra, o bien, como lo hizo *The Economist* (2010), el quinto dominio de batalla. Asumiendo este concepto inicial, se valida el trabajo contextual del capítulo anterior, pues los analistas no solo reconocen otros espacios previos para la guerra, sino que, además, asumen la existencia del ciberespacio como uno más, lo cual es fundamental para evidenciar si existe o no una forma de guerra en esta dimensión.

El Departamento de la Defensa de los Estados Unidos (United States Department of Defense [DoD]) fue uno de los primeros organismos gubernamentales en conceptualizar este nuevo territorio de la guerra. Sus concepciones se encuentran desde aceptarlo como un entorno en el que la información digitalizada se comunica a través de redes informáticas, hasta formas más complejas como definiciones que lo presentan como un dominio caracterizado por el uso de la electrónica y del espectro electromagnético. Para 2008, una "nueva" definición caracterizó el ciberespacio como el dominio global dentro del entorno de la información que consiste en la red interdependiente de infraestructuras de tecnologías de la información y de la comunicación (TIC), incluida internet, redes de telecomunicaciones, sistemas informáticos, y los procesadores y controladores incrustados (Singer y Friedman, 2014).

Para Ortega, el ciberespacio es el espacio artificial constituido por el conjunto de redes de ordenadores y de telecomunicaciones interconectados directa o indirectamente a nivel mundial, creado por el hombre para ser usado a su servicio. De manera más concreta, es

> un dominio global dentro del entorno de la información cuyo carácter distintivo y único está enmarcado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes

> e interconectadas utilizando tecnologías de la información y de la comunicación. (2012, p. 27)

Asimismo, el ciberespacio se ha configurado como el entramado de tecnologías informáticas que se constituye en el pilar sobre el que se erige y sustenta un medioambiente virtual de información y de continua interacción humana y artificial que transgrede el espacio geográfico y las barreras temporales de comunicación y forma parte de todas las actividades diarias del mundo (Trias y Bell, 2010). Las ideas de Trias y Bell suman elementos de análisis importantes, demuestran de manera implícita que, a diferencia de las otras dimensiones en las que se trasladó la guerra, esta ya posee la capacidad de no ser geográfica, no estar limitada por barreras físicas o políticas, y el tiempo de las actividades que allí se desarrollan en relación con el tiempo distan de cuando se hacen en el mundo real.

Si bien Singer y Friedman (2014) concuerdan con una definición técnica en la que se comprende el ciberespacio como un ámbito donde las redes que están compuestas por diversas computadoras, al igual que los usuarios que explotan sus capacidades, y a través de las cuales se almacena, comparte y comunica en línea la información, desde lo político, social y estratégico, es preferible acoger definiciones como la emitida por la Casa Blanca de los Estados Unidos en el año 2003, en la que el ciberespacio representa más el sistema de control del país, ya que está "compuesto por cantidades inmensurables de computadoras, servidores, *routers*, conmutadores y cables de fibra óptica, que, al encontrarse interconectados, permiten el correcto funcionamiento de las infraestructuras críticas"[11] (p. 1). Esto lleva a pensar que el ciberespacio, así como denota capacidades, simultáneamente significa riesgo (Stel, 2014).

Además de las posibles definiciones que se puedan exponer del ciberespacio, es posible afirmar que es una dimensión tanto para la guerra como para procesos no bélicos, que integra el conjunto de dimensiones precedentes —la terrestre, marítima, aérea y espacial— debido al número infinito de conexiones que en la actualidad se generan

11 Traducción del autor.

desde estos escenarios hacia el ciberespacio y como producto de que muchas de las herramientas, maquinarias, vehículos, etc., dependen de información para funcionar. Anteriormente, se abordó la capacidad de integración de las tecnologías, así que, si bien los carros, barcos y aviones se fusionaron con la artillería, muchas de las cosas que se usan en la vida cotidiana como en la guerra se fusionaron con la informática y la automatización.

Como consecuencia, el ciberespacio, en materia de los procesos humanos que permite realizar, evoluciona a una velocidad abismal debido al desarrollo tecnológico exponencial que constantemente lo alimenta, y el número de recursos que lo conforman, al igual que el de usuarios que lo explotan, aumenta sin desaceleración (López de Turizo y Sánchez, 2012).

Lo anterior, en paralelo a la referencia de Stel (2014) frente al riesgo, conduce a una realidad que será sustentada en los próximos capítulos. El ciberespacio logra trascender los límites geopolíticos y es bastante acertado en el momento de integrar las operaciones de la infraestructura crítica, de gobernabilidad, de comercio y, desde luego, de seguridad nacional (Gorman, 2005). Las cosas que están conectadas al ciberespacio, pero que hacen parte de las otras dimensiones de la guerra, también serán vulnerables frente a la ciberguerra.

No fue fortuito, entonces, que algunos ejércitos, los de los países militarmente desarrollados, al finalizar la década de 1990 comenzaran a discutir, teorizar y adoctrinar en lo que para el momento se llamó la *information war* e *information warfare* (IW). Asimismo, formaron una red de computadoras en un sistema integrado de comunicación (Dunn, 2001). En torno a estas prácticas, conformaron grupos especializados con capacidades informáticas para desarrollar una defensa y una ofensiva de carácter estratégico. Esto desencadena el análisis de algunos aspectos como la revolución de los asuntos militares en torno a esta evolución de la guerra gracias a la introducción de dispositivos que mejoraron la transmisión de información, así como la integración de equipo y armas preexistentes con dispositivos informáticos.

Aun así, en el contexto de la ciberguerra que invita este libro, la información como recurso y elemento se tratará como determinante en la guerra contemporánea. Pero se ha desarrollado otro escenario a

partir de las tecnologías informáticas y el ciberespacio, que en realidad da vida a lo que se denomina ciberguerra, y es donde las tecnologías informáticas se fundamentan a partir de los principios de la cibernética (Bieber, 2000).

Gracias a la ciberguerra, tanto la guerra interestatal como la guerra irregular se han traslapado al ciberespacio. El ciberespacio y las tecnologías que dan acceso a él han posibilitado que los ataques que se llevan a cabo en la virtualidad se pueden traducir en destrucción, caos suntuario, víctimas mortales y sociedades paralizadas, como si los Estados desplegaran sus ejércitos terrestres, fuerzas aéreas y armadas marítimas sobre su enemigo para ejercer fuerza y poder. Podría significar, de la misma manera, equilibrio al comprender que los terroristas, en vez de detonar sus artefactos explosivos o secuestrar aviones, emplearan el ciberespacio contra una nación.

La evolución del ciberespacio ha configurado nuevos escenarios para el desarrollo de los conflictos en el siglo xxi (Simonetti, 2008). Los países han explotado las posibilidades que ofrece el ciberespacio para realizar acciones como el ciberespionaje, que hace parte de un primer nivel en el cual se asume que la información es el fin, donde el objetivo de las operaciones es buscar información vital desde la perspectiva del perpetrador. Por dar solo un ejemplo, hay evidencias contundentes que demuestran que China ha realizado ciberespionaje a potencias occidentales desde 2002 dentro de lo que se denominó la operación Titan Rain (The U.S.-China Economic and Security Review Commission, 2009).

Las tecnologías informáticas se han vuelto estratégicas para acciones como el ciberespionaje, gracias a que presentan capacidades que inhabilitan los métodos y las tecnologías que las autoridades de muchos Estados han dispuesto para evitar este tipo de incidentes. Y, por ende, no hay forma de proponer herramientas eficientes de trazabilidad que permitan al actor agredido presentar pruebas contundentes frente a la violación de soberanía acaecida.

Es decir, el ciberespacio se ha descrito como una red interdependiente de sistemas de tecnologías informáticas, entre las que se denotan las computadoras o los procesadores, internet y los sistemas de control de la infraestructura crítica del Estado (U.K. Office of Cyber Security, 2009).

En general, una clara representación de lo anterior es que los gobiernos se preocupan constantemente por invertir en la construcción de *e-government* para generar una cercanía con la ciudadanía y alcanzar estándares óptimos de gestión, que los flujos de valores y capital circulen por el globo gracias a la interconexión de las bolsas y los mercados nacionales, que los sistemas informáticos de control de infraestructuras críticas del Estado y privadas se puedan controlar y monitorear a distancia, que los controladores de tráfico terrestre y aéreo funcionen en internet, que el sector privado y las personas apoyen sus actividades rutinarias en las capacidades de las TIC, entre otros casos que se pueden destacar (Gorman, 2005).

Extrapolación de los centros de gravedad de la guerra al ciberespacio

Sampaio (2001) propone que, tras su aparición, ha existido una dependencia entre el ser humano social y el ciberespacio, este expresado en sus recursos tangibles e intangibles, con la intención de facilitar los procesos cotidianos. Pero esta relación ha sido nociva por las potenciales vulnerabilidades que ha creado en la seguridad de los Estados y todos los actores que de él dependen, lo que abre fisuras que pueden ser penetradas por un enemigo para atacar las estructuras que el Estado haya asignado al control del ciberespacio, afectándolo física, moral y psicológicamente.

Esta capacidad tecnológica puede significar el dominio en un nuevo espectro, alejado de las armas tradicionales que poseen los Estados y las fuerzas militares y su superioridad convencional, atrae nuevas amenazas, pero no para las tropas que están en el frente de batalla, sino a cualquier sistema, de carácter gubernamental, militar, económico o social, que ahora haga parte del ciberespacio, así esté a kilómetros del campo de acción (Smith, 2004).

Si se tiene en cuenta a John Warden y su teoría sobre la existencia de cinco anillos, el panorama es más claro. Warden, en esencia, tiene la idea de que el Estado se encuentra compuesto por cinco anillos donde cada uno representa una parte vital de este, los cuales

se traducen en los mecanismos de combate, la población, la infraestructura crítica, los elementos orgánicos y sintéticos esenciales y los líderes gubernamentales (Fadok, 1995).

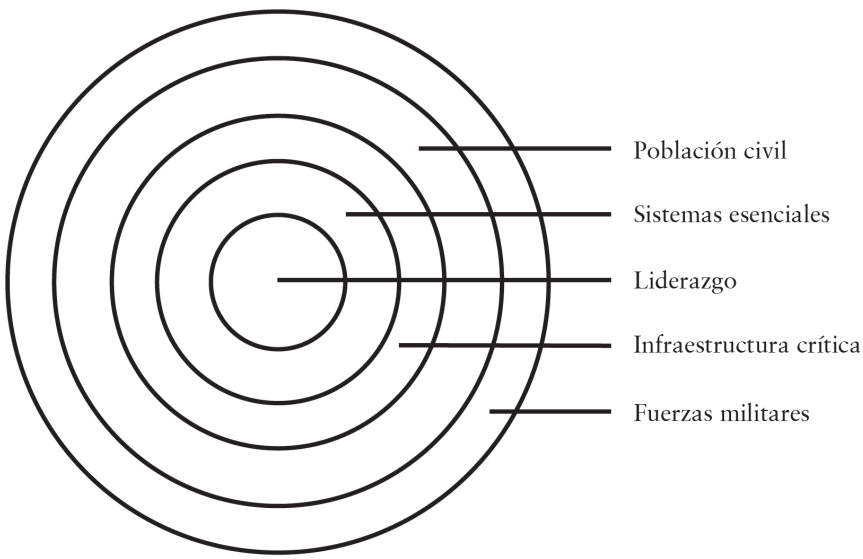
De esta manera, cuando se aterriza sobre el escenario descrito, donde los nódulos de subsistencia de una nación se encuentran integrados al ciberespacio, y sabiendo ya que se pueden desarrollar ciberataques con las tecnologías informáticas, se aclara cómo, desde la teoría de Warden, la estructura del Estado se encuentra en gran riesgo, ya no por las capacidades del poder aéreo como fue construido el postulado originalmente, sino por las capacidades que ofrecen las computadoras y el ciberespacio cuando los anillos se encuentran vinculados a estos.

Warden llevó el principio de centro de gravedad a una nueva instancia al observar al enemigo como un sistema organizado en anillos concéntricos. En conexión al concepto clásico, cada anillo de Warden representa un centro de gravedad diferente del enemigo (Jackson, 2000, p. 3). En un orden de importancia comprendido a partir del centro al exterior de los anillos, se identifica lo siguiente: un anillo de liderazgo que controla el sistema o Estado, es decir, los líderes del Estado; uno de sistemas esenciales que proporciona o representa la producción clave que es crítica para la supervivencia del Estado, esto es, el petróleo, la electricidad, la comida o el dinero; un tercer anillo de infraestructura crítica que une todo el sistema, como el transporte; luego el anillo de la población civil del Estado; y, por último, el anillo de las Fuerzas Armadas de los Estados. Warden cree que el objeto de la guerra es inducir al enemigo a hacer su voluntad; y se puede lograr de manera más eficaz y eficiente mediante ataques rápidos y simultáneos contra el anillo interior del enemigo (liderazgo). Solo si uno es incapaz de atacar el liderazgo de un enemigo, Warden recomienda atacar, en orden ascendente de importancia, los demás anillos (Jackson, 2000, p. 4) (véase figura 1).

Para que sea aún más fácil entender el alcance de estos potenciales riesgos, los Estados Unidos son un fiel ejemplo: casi la totalidad de las comunicaciones en el sector militar y de defensa son transmitidas por redes comerciales, que pueden ser interceptadas expeditamente. Además, en muchos casos, los insumos tecnológicos son comprados en Estados con intereses contrarios a los del país norteamericano y, por

supuesto, en múltiples casos, los archivos sobre temas delicados, secretos o los mismos avances tecnológicos ya se encuentran digitalizados y podrían ser manipulados o robados por actores que logren infiltrarse en los sistemas de seguridad cibernéticos (Bishop y Goldman, 2010).

Figura 1. Los cinco anillos de John Warden



Fuente: Elaboración propia a partir de Jackson (2000).

Esta realidad no es solo de los Estados Unidos o los países con mayores recursos o niveles altos de desarrollo. Debido a los bajos costos de las tecnologías informáticas y los servicios de redes, se convirtió en una realidad para millones de usuarios en el mundo, que la usan para conseguir sus intereses de una forma más inmediata. Al ser un proceso en constante crecimiento, que parece no detenerse en el futuro próximo, se podría hablar de un paradigma distinto de cualquier conocido, que transformó la vida de los Estados y de los ciudadanos en algo nunca antes visto (Estupiñán, 2001, p. 1). Pero ¿cómo ocurrió esto? Si bien es cierto que el ciberespacio es algo virtual, cabe preguntarse cómo se puede distinguir qué es lo que lo sustenta desde la realidad.

Como dato curioso e introductorio, Asaolu (2006) señala que, mientras que la radio tardó treinta años en llegar a más de sesenta millones de personas y la televisión tardó quince, internet, a partir de 1991, alcanzó esta meta tan solo en tres años (p. 338). Pero, asimismo, el número de usuarios de internet aumentó diez veces de 1999 a 2013. Los primeros mil millones se alcanzaron en 2005. Los dos mil millones en 2010 y los tres mil millones en 2014 (cf. Internet Live Stats).

El Pew Research Center encontró en 1995 que el 14 % de los adultos estadounidenses ya estaban conectados a internet para ese momento, la mayoría usando conexiones de módem de acceso telefónico. En 1996, el 77 % de los usuarios en línea envió o recibió correos electrónicos al menos una vez cada par de semanas, frente al 65 % de 1995. En 1998, el primer índice de Google hace referencia a veintiséis millones de páginas web; para 2000, Google rompió el récord de un billón de páginas (Press, 2015).

En 2003, se realiza la primera Cumbre Mundial sobre la Sociedad de la Información en Ginebra; en 2004, la banda ancha supera al *dial-up*; en 2005, se alcanzan los mil millones de usuarios de internet, el DSL es más veloz y se introducen los cables 3.0; en 2007, se hace el lanzamiento del primer iPhone; en 2008, los países en desarrollo tienen el 50 % de los usuarios de internet del mundo (InternetSociety, 2014).

Entre 2007 y 2008, el ciberespacio cobró una relevancia inesperada en otra época: por primera vez un país usó internet para realizar unas votaciones, Estonia. El 36 % de la población norteamericana hacía sus consultas en Wikipedia y el índice de Google alcanzó más de un trillón de direcciones únicas. En 2009, se realiza el primer lanzamiento de la red 4G; en 2010, la banda ancha móvil supera a la fija, Wikipedia alcanza los mil millones de ediciones y existen quinientos millones de abonados de banda ancha fija. Para 2011, el 50 % de los usuarios de internet tienen una conexión de banda ancha móvil; en 2012, los videos componen el 50 % del tráfico de internet y los países en desarrollo tienen más del 50 % de abonados a la banda ancha móvil del mundo; en 2014, los teléfonos inteligentes representan el 80 % de todos los teléfonos móviles (Internet Society, 2014). Para 2014, el número de usuarios de internet llegaba a los tres mil millones; actualmente alcanza casi los cuatro mil (Press, 2015).

En 2014, casi el 75 % (2,1 mil millones) de todos los usuarios de internet del mundo (2,8 mil millones) viven distribuidos en solo 20 países. El restante 2,5 % (700 millones) se distribuyen entre los otros 178 países, cada uno representando menos del 1 % del total de usuarios. China, el país con más usuarios (642 millones en 2014), representa casi el 22 % del total y tiene más usuarios que los tres países siguientes (los Estados Unidos, la India y Japón). Entre los 20 países con mayor penetración, la India es el de menor con el 19 %, pero en el que se aumenta con mayor velocidad anualmente. En el extremo, los Estados Unidos, Alemania, Francia y Canadá tienen la mayor penetración: más del 80 % de la población en estos países tiene conexión a internet (Unión Internacional de Telecomunicaciones, 2014). En lo respectivo al uso por regiones a nivel mundial, el mayor uso se da en Asia, con un 48,4 %; le sigue el continente americano, con un 21,8 %; Europa, con un 19 %; África, con el 9,8 %; y Oceanía culmina las estadísticas con un 1 % (cf. Internet Live Stats) (véase tabla 1).

Tabla 1. Uso de internet por regiones alrededor del mundo

	Total de usuarios		Crecimiento (%)
	2000	2017	
África	4 514 400	353 121 578	7722,1
Asia	114 304 000	1 874 136 654	1539,6
Medio Oriente	3 284 800	141 931 765	4220,9
América Latina y el Caribe	18 068 919	385 919 382	2035,8

Fuente: Elaboración propia a partir de Internet Live Stats.

Más de la mitad del mundo ahora usa un teléfono inteligente, casi dos tercios de la población tiene uno, más de la mitad del tráfico web del planeta proviene de estos dispositivos, más de la mitad de todas las conexiones móviles son de banda ancha y, de cada cinco personas en el globo, al menos una ha comprado en línea durante los últimos treinta días (Kemp, 2017).

Los teóricos de la materia han establecido que, si bien el ciberespacio puede catalogarse como un escenario donde el Estado puede ver amenazada su soberanía, es debido a que de manera similar

a como se constata en los poderes militares preexistentes, al utilizar las tecnologías informáticas como armas en el ciberespacio, se está recreando el tradicional empleo de un dispositivo bélico en una dimensión de conflicto y con el fin de propiciar un efecto en el enemigo (Wilson, 2007). Algo muy cercano a lo observado con Clausewitz (1942) en el capítulo 1.

Cuando se analiza el ciberespacio desde una posición netamente guerrera, no se puede cometer el error de calificarlo de un espacio aislado y distante de la realidad física conocida de otros dominios, como los conflictos terrestres, aéreos o marítimos. Del mismo modo que un enfrentamiento convencional puede llegar a ser catastrófico, la intención del uso de tecnologías es el mismo, causar el mayor daño posible, pero con una diferencia importante: en múltiples casos, pueden existir efectos colaterales, tanto a terceros actores (civiles) como a propios, y el ciberespacio permitiría disminuir casi por completo esta consecuencia al afectar directamente los centros de gravedad del contrario (Ottis, 2010).

Sería una falla por parte de los actores estatales menospreciar los alcances de los enfrentamientos en un contexto ciberespacial. En la actualidad, las estructuras más importantes y sensibles pueden ser manejadas a kilómetros de distancia, lo que pone al alcance dañar centrales nucleares, enviar comandos errados a los medios de transporte y mensajes equivocados a los medios de comunicación, hacer colapsar las entidades financieras, entre otros múltiples efectos devastadores, y en este caso ya no únicamente al sector militar o gubernamental, sino también a la población y al Estado como un todo (Geers, 2009).

En definitiva, un número importante de países se ha percatado de la realidad del ciberespacio como un nuevo campo de batalla. Esta nueva dimensión del poder militar exige una concepción estratégica, operacional y táctica. Además, el desarrollo de una cultura que reconozca la importancia de las tecnologías informáticas en relación con la seguridad nacional. En conclusión, los Estados deben prepararse para librar la ciberguerra y ganarla (Clark y Knake, 2010).

Castells (2004) se ha convertido en un teórico indispensable para entender el mundo anclado a la tecnología, afirmando que existe una relación innegable y casi irrompible entre el comportamiento cotidiano

de todos los actores sociales (Gobierno, sector privado, ciudadanía) y el ciberespacio. Las facilidades que ofrece internet sobre los procesos que podían tardar años, la conexión, la inmediatez, la cercanía, entre otras, han hecho que los sistemas y las redes informáticas sean demandados en cualquier rincón del planeta sin necesidad de insertarlos a la fuerza.

Habiendo generado elementos para sustentar que gran parte de los procesos humanos, no solo la guerra, se enlazaron con las tecnologías informáticas, se retomará el concepto de centros de gravedad para terminar de exponer por qué el ciberespacio se convirtió en un nicho apropiado para una práctica bélica; desde otra perspectiva, en la actualidad, se asume el hecho de que los centros de gravedad no solo podrían ser atacados mediante el armamento convencional, o improvisado de los actores irregulares, sino también mediante computadoras y personas expertas que pueden usarlos en un sentido *violento*.

Desde la perspectiva de Anding, uno de los principios más ampliamente reconocidos del arte operativo es el centro de gravedad. Y aunque sus raíces se encuentren a casi doscientos años en el tiempo, cuando Clausewitz recreó el concepto, este ha perdurado (2007, p. 3).

Recientemente, se redefinió el concepto de centro de gravedad como aquellas características, capacidades o localidades de las que una fuerza militar deriva su libertad de acción, fuerza física o voluntad de luchar, donde el camino más rápido a la victoria es destruyéndola o neutralizándola. El Cuerpo de Marines de los Estados Unidos describe los centros de gravedad como "fuentes importantes de fuerza". Dependiendo de la situación, pueden ser características intangibles como la determinación o la moral, o capacidades tales como fuerzas blindadas o la fuerza de aviación. Pueden ser localidades tales como un pedazo de terreno crítico que ancla un sistema defensivo entero. Pueden ser la relación entre dos o más componentes del sistema, como la cooperación entre dos armas, las relaciones en una alianza o la unión de dos fuerzas. El centro de gravedad es una fuente de fuerza masiva, física o moral, o una fuente de influencia, cuya grave degradación, dislocación, neutralización o destrucción tendría el impacto más decisivo sobre la capacidad del enemigo o su propia capacidad para lograr un objetivo militar determinado (Anding, 2007, p. 4).

De nuevo citando a Anding, se pueden destacar algunas características de los centros de gravedad:

> Los centros de gravedad tienen elementos tangibles e intangibles; cuanto mayor sea el nivel de guerra, menor será el número de centros de gravedad. En general, hay uno a nivel estratégico; los centros de gravedad operacional suelen incluir aspectos más tangibles del poder militar. Los ejemplos incluyen un batallón blindado, un grupo de portaaviones o un sistema de defensa aérea integrado; el número de centros de gravedad operacional está directamente relacionado con el número de objetivos operacionales; finalmente, los centros de gravedad no son lugares ni son capacidades. Poseen capacidades y se benefician de ciertos lugares[12]. (2007, p. 5)

Según Strange, los centros de gravedad poseen una estructura interna de varios componentes que los convierten en sistemas más complejos que protegen de las amenazas. Entre estos componentes, están las capacidades críticas, habilidades primarias que los erigen como tales, y que se relacionan con el poder físico, mental, financiero o legal para realizar una función. Segundo, los requerimientos críticos: estos son condiciones, recursos y medios esenciales para que una capacidad crítica sea plenamente operativa. Tercero, la vulnerabilidad crítica: elementos o componentes vulnerables ante la neutralización, interdicción o ataque (daño moral/físico), con lo que se logran deterioros decisivos (2005, p. 43).

Como se observó, se puede hablar de una clasificación doble para los centros de gravedad: morales y físicos. Los morales comprenden a los líderes, quienes toman las decisiones, y cómo las operaciones pueden hacer cambiar su comportamiento, o pueden ser atacados de forma directa. Y por otra parte, el apoyo público, popular (entendido como la población en general) o nacional (relativo al concepto de nación o Estado como un todo). Los centros de gravedad físicos se dividen en tres categorías. La primera categoría son las Fuerzas Armadas, la fuerza y el poder en todos los niveles de la guerra. Las categorías

12 Traducción del autor.

segunda y tercera pertenecen al nivel estratégico: poder económico o industrial nacional, de modo que son los cimientos de la fuerza física nacional, y el poder proveniente de grandes poblaciones (Strange, 2005, p. 45). Para la ciberguerra, conviene tener en cuenta un aspecto más señalado por Strange:

> Los centros de gravedad morales en todos los niveles, y los políticos a nivel estratégico, hacen que las cosas sucedan en virtud de su voluntad, influencia y liderazgo. Estos están basados en las personas, como individuo y como población. Los centros de gravedad morales y políticos deben poseer cualidades tales como determinación, coraje (moral y físico), y el poder de persuadir, inspirar o intimidar. Los centros de gravedad físicos a nivel estratégico pueden incluir fuentes directas o centros de fuerza militar, así como las principales fuentes indirectas de esa fuerza para incluir el poder económico e industrial y el poder que provienen de las grandes poblaciones nacionales. En los niveles operativos y tácticos, son fuentes primarias y centros de fuerza militar (es decir, unidades y formaciones militares), que hacen que las cosas sucedan en virtud de su poder militar[13]. (2005, p. 47)

Eikmeier expone que los actores político-militares tienen en cuenta cuatro principios para determinar los centros de gravedad en sus enemigos. El primero es determinar la capacidad crítica del enemigo, la función absolutamente esencial que el sistema de este realiza. El sistema puede tener varias capacidades, pero no todas resultan críticas en cada situación. Segundo, identificar la fuente de poder crítico del enemigo, que es su centro de gravedad. Tercero, identificar los requisitos críticos del centro de gravedad. Y, finalmente, identificar los requisitos o componentes críticos que son vulnerables a ataques o interrupciones (2004, p. 3).

Se continuará el análisis de las razones por las que el ciberespacio se ha concebido como la quinta dimensión de la guerra. Los países son pirámides invertidas que descansan precariamente en sus entrañas

13 Traducción del autor.

estratégicas: liderazgo, comunicaciones, producción esencial, infraestructura y población. Si un país está paralizado estratégicamente, es derrotado, y no puede sostener sus fuerzas en el campo, aunque estas estén completamente intactas (Jackson, 2000, p. 3).

Por elementos esenciales del sistema se hace referencia a aquellos atributos que a menudo son necesarios para que el Estado emprenda la guerra. Como señala Warden (1995),

> los principales ejemplos de lo esencial del sistema incluyen la fuente de energía de un Estado, es decir, la electricidad, el petróleo, los alimentos y los recursos financieros. Si bien la destrucción de estos objetos puede privar al Estado enemigo de su capacidad de hacer la guerra, tal destrucción a menudo amenaza la supervivencia de la población civil del enemigo. Es este último punto el que causa las mayores preocupaciones legales y morales al orientar los elementos esenciales del sistema […]. Cobra así relevancia el concepto de infraestructura crítica, el cual se refiere a aquellos atributos que unen el sistema y lo ayudan a funcionar como un único organismo o entidad. Las carreteras, los aeródromos y las fábricas son parte de la infraestructura crítica. (citado por Jackson, 2000, pp. 18-20)

La concepción del centro de gravedad con relación a la infraestructura crítica ha sido tema de interés para los Estados. A manera de ejemplo, el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology [NIST]) define las infraestructuras críticas como aquellos sistemas y activos, físicos o virtuales, tan vitales que su incapacidad o destrucción tendría un impacto debilitante en la seguridad nacional, salud pública o seguridad, o cualquier combinación de estas. Asimismo, la Comisión Europea describe las infraestructuras críticas como instalaciones, redes, servicios y activos físicos y de tecnología de la información que, de ser perturbados o destruidos, tendrían un grave impacto en la salud, la seguridad o el bienestar económico de los ciudadanos o el funcionamiento efectivo de los gobiernos (Colesniuc, 2013, p. 123).

En la misma línea, como lo proponen Alcaraz y Zeadallay (2015), una infraestructura crítica consiste en un conjunto de sistemas y activos físicos o virtuales, tan esenciales para la nación que cualquier

interrupción de sus servicios podría tener un impacto serio en la seguridad nacional, el bienestar económico, la salud pública, o cualquier combinación de estos (p. 53).

En otro sentido, la protección de infraestructura crítica debe asumirse en términos prácticos y concretos, como la protección de la energía, de las telecomunicaciones, el suministro de agua, transporte, finanzas, salud y otras infraestructuras que permiten que una nación funcione. Estas infraestructuras críticas deben ser protegidas contra eventos accidentales y deliberados que les impidan funcionar de manera correcta, afectando así gravemente el bienestar económico y social de esa nación (Kellermann, Martinez, Contreras y Marchiori, 2015, p. 13). En la mayoría de los países, la palabra *crítica* se refiere a la infraestructura que proporciona un apoyo esencial para el bienestar económico y social, la seguridad pública y el funcionamiento de las responsabilidades gubernamentales clave (Organisation for Economic Co-operation and Development [OCDE], 2008, p. 3).

La infraestructura crítica puede incluir comunicaciones, servicios de emergencia, energía, represas, sector financiero, comida, servicios públicos, industria, salud, transporte, gas, comunicaciones públicas, radio y televisión, tecnologías de la información, instalaciones comerciales, centros químicos y nucleares, y agua. Muchos Estados dependen cada vez más de infraestructuras y bienes que se encuentran parcial o totalmente fuera de su jurisdicción y sobre los cuales tienen poco o ningún control (Counter-Terrorism Committee Executive Directorate [CTED], 2017, p. 2).

En un sentido más detallado, siguiendo de nuevo a Alcaraz y Zeadallay, se presentarán los elementos del orden nacional considerados críticos:

- Energía: fuentes energéticas, almacenamiento y distribución (petróleo, gas, electricidad).
- Tecnologías de la información y las telecomunicaciones: sistemas de información y protección de la red (por ejemplo, internet), suministro de telecomunicaciones fijo, prestación de telecomunicaciones móviles, comunicación por radio y navegación, comunicación por satélite, radiodifusión.

- Agua: suministro de agua (por ejemplo, presas) y control de calidad y cantidad de agua.
- Alimentación y agricultura: provisión de alimentos, seguridad y protección.
- Salud y salud pública: atención médica y hospitalaria, medicamentos, vacunas y productos farmacéuticos, biolaboratorios y bioagentes.
- Sistemas financieros: banca, servicios de pago y asignación financiera del Gobierno.
- Administración civil: instalaciones y funciones gubernamentales, Fuerzas Armadas, servicios de administración civil, servicios de emergencia, servicios postales y de mensajería.
- Orden público, ordenamiento jurídico y seguridad: mantenimiento del orden público y jurídico, seguridad y protección, administración de justicia y detención.
- Sistemas de transporte: transporte por carretera, transporte ferroviario, tránsito aéreo, vigilancia de fronteras, transporte fluvial.
- Industria química: producción y almacenamiento de sustancias peligrosas, tuberías de mercancías peligrosas.
- Monumentos e íconos nacionales: monumentos, estructuras físicas, objetos o lugares geográficos reconocidos como representativos de la cultura nacional o que tengan una importancia religiosa o histórica.
- Instalaciones comerciales: centros comerciales, edificios de oficinas, estadios deportivos, cualquier otro lugar que pueda albergar a un gran número de personas.
- Fabricación crítica: transformación de materiales en bienes. Esto incluye todos los procesos involucrados en la fabricación y el equipo de transporte.

- Base de la industria de defensa: instalaciones de producción de recursos militares (por ejemplo, armas, aviones o barcos) y mantenimiento de servicios esenciales (por ejemplo, comunicación) para proteger a una nación.
- Industria nuclear: producción y almacenamiento de sustancias nucleares.
- Espacio: comunicación e investigación.
- Instalaciones de investigación (2015, p. 54).

El lector tal vez se pregunte por la relación de estos elementos con la ciberguerra. El primer aspecto de esta relación ya fue presentado anteriormente y corresponde a la demanda de las TIC en los procesos sociales y cómo se hicieron dependientes estos de las redes tecnológicas. Pero, en segunda medida, esta relación tiene que ver con el hecho de las estructuras precisas que permiten la integración, la modificación y el manejo de los centros de gravedad y principalmente la infraestructura crítica, con el ánimo de mejorar la eficiencia y el control a distancia, la unión de las tecnologías informáticas y el ciberespacio con la humanidad y los actores internacionales.

Esto se ha convertido en una realidad gracias a la invención del sistema de control distribuido (*distributed control system* [DCS]), como lo es el más conocido de todos, SCADA (*supervisory control and data acquisition*). Un sistema SCADA se refiere, básicamente, a una red centralizada para la supervisión y adquisición de datos de subestaciones ubicadas en áreas geográficas grandes y distantes. El centro de control es responsable de regular el rendimiento general de todo el sistema y de gestionar su información sensible. Esta gestión depende de la funcionalidad de un conjunto de servidores. Los accesos externos a estos recursos deben ser debidamente abordados y restringidos a través de mecanismos de seguridad, tales como redes inalámbricas, zonas desmilitarizadas (*demilitarized zone* [DMZ]), sistemas de detección de intrusiones (*intrusion detection system* [IDS]), sistemas de prevención de intrusiones (*intrusion prevention system* [IPS]) o antivirus. Algunos de estos accesos pueden provenir de redes corporativas encargadas de reportar evaluaciones estadísticas o

actualizar planes estratégicos para aumentar la productividad y la producción comercial. Por el contrario, un DCS es un sistema orientado a procesos, cuyo control es limitado desde el punto de vista de la dimensión y distribución geográfica (Alcaraz y Zeadallay, 2015, p. 57).

Hoy en día, las TIC desempeñan un papel crucial en el control y la conectividad entre entidades críticas. Este es el caso de los sistemas SCADA, cuyo control y supervisión dependen, principalmente, de la fiabilidad y seguridad de los canales de comunicación y sistemas de información para enviar, calcular o almacenar comandos, alarmas o mediciones. Se identifican tres principales entidades tecnológicas en esta sección: sistemas de comunicación para grandes distancias, sistemas de comunicación inalámbrica y la influencia de sistema para operaciones de control (Alcaraz y Zeadallay, 2015, p. 59).

En los países desarrollados, y cada vez más en cualquier parte del mundo, las infraestructuras de la información son al mismo tiempo una base fundamental que hace que las sociedades contemporáneas funcionen, así como una fuente de vulnerabilidad. La difusión de las telecomunicaciones, internet y la penetración de las computadoras y las redes informáticas locales aplicadas en tantas facetas de la vida hoy han cambiado todo. Por esta razón, los sistemas de información se consideran un activo crítico, no solo para propósitos de inteligencia tradicionales, sino también para cuestiones de seguridad. Si bien representan una base esencial que permite a las sociedades modernas trabajar y vivir, se han desarrollado sin considerar la seguridad como una prioridad. La recopilación de información ha sido siempre un aspecto crítico e ineludible en la política internacional y las nuevas tecnologías ofrecen herramientas sin precedentes para monitorear los gobiernos, las economías, la defensa y la planificación de la seguridad que pueden convertirse en objetivos de amenazas externas (Colesniuc, 2013, p. 123).

> La infraestructura crítica incluye propietarios y operadores públicos y privados, y otras entidades que desempeñan un papel en la protección de la infraestructura de la nación. Los miembros de cada sector de infraestructura crítica realizan funciones que están respaldadas por sistemas de tecnología de la información

> (TI) y control industrial (*industrial control system* [ICS]). Esta dependencia de la tecnología, la comunicación y la interconectividad de la TI y la ICS ha cambiado y ampliado las vulnerabilidades potenciales y el mayor riesgo potencial para las operaciones. Por ejemplo, a medida que los sistemas de control industrial y los datos producidos en las operaciones de ICS se utilizan cada vez más para prestar servicios críticos y apoyar las decisiones empresariales, deberían considerarse los impactos potenciales de un incidente de seguridad cibernética en los negocios, los activos, la salud y la seguridad de las personas y el medioambiente de una organización. Para gestionar los riesgos de seguridad cibernética, se requiere una comprensión clara de los factores de negocio de la organización y las consideraciones de seguridad específicas para su uso de TI e ICS. Debido a que el riesgo de cada organización es único, junto con su uso de TI e ICS, las herramientas y los métodos utilizados para lograr los resultados variarán[14]. (National Institute of Standards and Technology, 2017, p. 3)

Se considera una serie de factores que aumentan el riesgo de ataque electrónico contra los sistemas informáticos:

- Dificultades inherentes a la seguridad.
- Sistemas insuficientes de concientización y educación de los usuarios y actitudes o prácticas que no cumplen con el manual de procedimientos.
- Disponibilidad de información sobre la penetración de sistemas informáticos sin autorización.
- Reglamentaciones jurídicas poco claras y dificultades jurisdiccionales.
- Intensificación del fenómeno de la globalización (Colesniuc, 2013, p. 124).

14 Traducción del autor.

> La característica más notable de la infraestructura crítica y de las redes informáticas en general es que la seguridad nunca fue una preocupación importante para los primeros desarrolladores e ingenieros de *software*. Si se echa un vistazo a la historia de internet, todo el mundo es consciente de que su protocolo (el TCP/IP[15]) nació "abierto", sin protección o mecanismo de autocifrado. La sencillez y la velocidad eran una prioridad, ya que se suponía que solo una comunidad de científicos muy pequeña la encontraría útil y querría usarla. Sin embargo, cuando llegó el turno para la comunidad de los negocios de acoger y popularizar internet, esas mismas características fueron recibidas con gusto porque significaban más "eficiencia" (desde el punto de vista del tiempo y la velocidad) y menores costos. Las infraestructuras de información crítica son en su mayoría desarrolladas y construidas a nivel nacional, pero también están vinculadas a las infraestructuras de otros países, por lo que el colapso de una parte de la CII (*critical information infrastructure*) de un país tendría un serio impacto en la situación de los vecinos[16]. (Colesniuc, 2013, p. 124).

La etapa inicial de toda futura guerra contra un Estado relativamente moderno implicaría cierta forma de guerra cibernética o, más específicamente, ataques cibernéticos a su CII. Aparentemente, la guerra cibernética no sería tan diferente de la guerra electrónica en el pasado. Pero en algunos aspectos la primera es más grande y ha incorporado la segunda. Primero, la guerra electrónica está dirigida solo a bloquear o interrumpir la comunicación del enemigo; la ciberguerra se dirige a sus centros de gravedad, además de obstaculizar las comunicaciones, también puede impedir la circulación y distribución de divisas, energía, gas, agua y el funcionamiento del control del tráfico aéreo y de los servicios de salud. Además, la guerra cibernética tendría efectos tácticos y estratégicos, dependiendo de los recursos empleados, que

15 *Transmission control protocol/internet protocol* (protocolo de control de transmisión/protocolo de internet).

16 Traducción del autor.

impedirían la comunicación (y los muchos servicios que dependen de ella) en todo el país (Colesniuc, 2013, p. 125).

La gestión y el monitoreo de los sitios web han mejorado para las instalaciones de la infraestructura crítica, ya que se han conectado progresivamente con internet. La conveniencia adicional de la conectividad, sin embargo, ha convertido la superficie de ataque una vez limitada de estas industrias en un paisaje fértil para los ataques cibernéticos. Debido a los potenciales efectos de alto perfil de los ataques a los sistemas de infraestructura crítica, estas industrias se han convertido en objetivos aún más atractivos para los ciberdelincuentes (Kellermann *et al.*, 2015, p. 6).

> Estas infraestructuras han sido protegidas contra ataques físicos y sabotajes durante muchas décadas hasta principios de este siglo. Sin embargo, varios países se dieron cuenta de que muchas de estas infraestructuras críticas también tenían un componente común: dependían en mayor o menor medida de las infraestructuras de información (redes de telecomunicaciones y sistemas informáticos, TIC)[17]. (Kellermann *et al.*, 2015, p. 13)

Es posible llegar a la conclusión de que los centros de gravedad, representados en un concepto más contemporáneo como *infraestructuras críticas*, se han hecho vulnerables cuando se conectaron al ciberespacio para poder actualizar la forma en la que se desarrollaban los procesos a través de las TIC. Además, una vez conocido que los procesos políticos, económicos, militares y sociales en general se podían llevar a cabo sin determinantes de localización, pero, aparte de eso en tiempo real, fue imposible plantear un mundo sin las TIC.

El ciberespacio, más allá de representar un concepto tecnológico y técnico en las ciencias y disciplinas que le competen, termina siendo un constructo más sociológico en el sentido de que representa una dimensión en la cual pareciera que las personas están y seguirán virtualizando las cosas que antes se desarrollaban exclusivamente en la atmósfera real. En términos equitativos, frente a la idea de las

17 Traducción del autor.

dimensiones de la guerra, lo que permite entender por qué el ciberespacio se convirtió en otra dimensión para esta práctica es, primero, que este se ha transformado en un ambiente indispensable para dar vida a un mundo globalizado en todos sus aspectos, por lo cual, y ya que el ser humano en su dimensión física sigue amarrado a las distancias geográficas y temporales de la movilidad a lo largo del planeta, la única forma de hacer posible este deseo humano fue en un plano virtual alimentado por la información. Esto claramente llevó a adaptar las cosas que se utilizan para llevar a cabo los procesos de una forma acorde. Segundo, que parte de los procesos a los que se hace referencia involucran actividades que sobrepasan los contextos propios de los actores conectados al ciberespacio, y se configuran en niveles de los Estados nación, por lo que su afectación sería negativa para una sociedad en general, lo que se definió como centro de gravedad e infraestructura crítica.

Las armas en el ciberespacio

En relación con lo propuesto al inicio del capítulo, solo resta analizar en qué medida se pueden concebir las tecnologías informáticas que permiten la integración al ciberespacio como aquellas capacidades que posibilitan que algunos actores del sistema internacional y actores irregulares puedan atacar la infraestructura crítica en el ciberespacio.

Antes que nada, se debe reconocer que el concepto de *arma* desde el punto de vista de la ciberguerra solo tiene validez cuando se asume desde la intención del ejecutor de un ataque en el ciberespacio. Asumir el concepto arma desde un principio clásico, es decir, armamento cinético que funcione en las cuatro dimensiones de la guerra previas a esta, no es posible. En la ciberguerra, lo que se emplea son dispositivos capaces de crear, procesar, administrar y enviar información, la cual, en sentido automático, debería interpretarse como una especie de munición en sentido analógico.

Vale la pena recalcar que una herramienta o dispositivo que permita conexión en el ciberespacio, con la suficiente capacidad de manejar programas e información nociva (una computadora), puede ser usada con fines violentos y se transformará en un arma que ataque cualquier

conexión, por más pequeña que sea, y se infiltre en sistemas, en apariencia seguros (Stein, 2001). En resumen, se necesita la información que se quiera manejar, un terminal y una conexión a la red, es decir, un sistema que ya está ligado en lo más profundo del funcionamiento estatal y global (Criado, Ramilo y Serna, 2002).

Libicki (2009), dentro de la RAND (Research ANd Development), se ha enfocado en la relación entre el ciberespacio y el sector defensa, afirmando el temor —real— que ya existe: un procesador puede ser una amenaza para los Estados que ya usan las tecnológicas informáticas y de comunicación para atacar. Este autor habla de los dispositivos electrónicos desde tres componentes: la capa física, que es por supuesto la que cualquier persona reconoce al ver un aparato electrónico, y todo lo que dentro de él se puede encontrar; este es el instrumento que permite crear una conexión entre el individuo que la maneja y el ciberespacio.

En un segundo momento, se hace referencia a la necesidad del trabajo humano en los procesos tecnológicos, es decir, un nivel donde se ubican las instrucciones que puede un usuario introducir en el dispositivo que tengan un efecto sobre su entorno cibernético. En tercer lugar, se encuentra probablemente el componente más importante, esencial para el funcionamiento del ciberespacio y recurso vital: la información (Libicki, 2009). Si un actor posee habilidades tecnológicas, con la información maliciosa que puede generar, la convierte en términos sintácticos en la medida en que adquiere la capacidad de establecer comportamientos determinados en el sistema que invade.

Un arma cibernética puede afectar gravemente la infraestructura crítica de un Estado, tal y como se constató con la intrusión del programa Stuxnet en el sistema informático del reactor nuclear de Natanz en Irán; ataque que en la actualidad se le atribuye a Israel. Esta es una clase de ataque que ya ha sido revisada en diversas investigaciones y catalogada como una de las formas más poderosas de emplear la informática como un arma (Libicki, 2010).

Muchos de los analistas de la ciberguerra, el ciberespacio y en general las ciberamenazas han apelado a una novela de ciencia ficción para denotar lo que en realidad significa la cibernética, más que la capacidad de administrar información. William Gibson, autor de *Neuromancer*,

recreó el concepto de ciberespacio para describir cómo las computadoras y su interconexión estaban generando una red artificial de terminales que dominaban exorbitantes cantidades de información, las cuales podían ser empleadas para diversos fines. Pero lo más importante del relato de Gibson es que las acciones que realizan los humanos se traducen en efectos en el mundo real, y viceversa. Además, y más importante aún, el mundo virtual y físico logran converger de forma tal que las acciones desarrolladas en cada uno de estos tienen repercusiones semejantes en el otro (Gibson, 1984).

En concordancia con la realidad, el general al frente del Comando Estratégico estadounidense, Kevin Chilton, para 2009, dio a conocer al público que los Estados Unidos, al establecer sus operaciones en el contexto transnacional, han entendido que se encuentran actuando en un medioambiente globalizado, caracterizado por la interdependencia, la incertidumbre, la complejidad y los continuos cambios. Como se ha establecido en la Estrategia de Operaciones Militares en el Ciberespacio, la seguridad y el desarrollo de la nación en el mundo interconectado dependen claramente de las TI e internet como elementos estratégicos para fortalecer y desarrollar los instrumentos del poder nacional (Chilton, 2009, p. 7).

No cabe duda, entonces, de que, al emplear un ciberataque, el fin buscado es que la agresión se transfiera de forma contundente al mundo real, generando efectos psicológicos, caos organizacional y civil, o un ataque dirigido a la infraestructura crítica y, por ende, sobre la población, si se llegara a poner en riesgo el funcionamiento adecuado de ella (Mills, 2010).

Existe una comparación con el mundo de la biología para explicar el comportamiento del ciberespacio. Gutiérrez (2010) explica que los dispositivos que están conectados al ciberespacio pueden ser contrastados con seres vivos, que son invadidos por actores externos en busca de afectar sus estructuras internas (virus), ya sea mediante el ingreso de información errada o el robo de aquella que le permite funcionar.

Esta filtración es denominada ataque, porque busca desequilibrar y acabar con la armonía del sistema, y se puede definir como "una tecnología informática basada en sistemas del mismo orden (*software*,

hardware y medio de comunicación) que ha sido diseñada para perjudicar y dañar la estructura y el funcionamiento de algún otro sistema"[18] (Lorents y Ottis, 2010, pp. 131-133). En primera instancia, el ataque de negación de servicio consiste en la generación de un código que se envía en forma imperceptible, a través de herramientas como los *virus troyanos* o las *botnet*, a un gran número de computadoras a través de internet (Ghosh, 2004).

Este código, posteriormente, al esconderse en los diversos sistemas interconectados, espera la fecha con la cual fue programado para ejecutar su ataque. Asimismo, transforma la información en una petición de acceso a una página web establecida por el agresor con el fin de que, en el momento de multiplicarse la misma solicitud por el número de computadoras infectadas, el sitio virtual quede deshabilitado para el uso de su administración hasta el punto de imposibilitarlo para seguir prestando sus servicios (Glebocki, 2008).

Otra forma de ataque son las denominadas *weapons of mass distraction* o armas de distracción masiva, las cuales buscan, a través del empleo de las tecnologías informáticas, manipular a la población civil de forma psicológica. Como lo describe Brenner (2009), las armas de distracción masiva pretenden derrumbar la moral civil con la sofocación de la fe ciudadana en la eficacia de sus gobiernos. Dependiendo del tipo de ataque de manipulación, puede resultar como efecto desde la imposición de un perjuicio o la destrucción de la propiedad (p. 45).

Por otra parte, un ataque de negación del servicio (*denial of service* [DDoS]) tiene una intención muy clara: atacar un destino en el ciberespacio con el fin de interrumpir su servicio y buen funcionamiento, saturarlo de solicitudes para vulnerar su protección y causarle fallas hasta llegar a desactivarlo por completo (Rosenfield, 2009). Eso se logra cuando el sitio ve su capacidad sobrepasada y el encargado de manejarlo se vea imposibilitado para manejarlo y lograr una interacción real con cualquier persona que busca acceder a este espacio (Glebocki, 2008).

18 Traducción del autor.

A partir de operaciones furtivas, también existen formas de atacar a un Estado a través de la sustracción o robo de información confidencial acerca de su armamento y sistemas de defensa nacionales, planes de guerra, estrategias militares y planeamiento de operaciones (Carr, 2011).

En última instancia, se encuentran los ataques cibernéticos en contra de la infraestructura crítica del Estado, la cual, en caso de verse afectada como resultado de la alteración de sus sistemas informáticos de control con un código malicioso de comando o la generación de un vínculo de control remoto, podría paralizar un Estado y traer consigo efectos devastadores en la vida de sus ciudadanos (Sierra, 2002).

Tan solo es necesario imaginar lo que pasaría si se inhabilitara la red eléctrica de una ciudad y, por ende, no hubiera forma de poner en marcha las bombas de gasolina que proveen de combustible a sistemas de transporte y medios de abastecimiento de *elementos esenciales*, o que en determinado momento las plantas generadoras de electricidad de los hospitales se agotaran (Ghosh, 2004).

Con lo anterior se entiende el dónde y el con qué, a continuación, se entenderá el cómo, el por qué y, en esencia, el qué. Los siguientes capítulos buscarán exponer cómo se llegó a la ciberguerra y la preparación de los actores para ella, además de sus diversas formas de expresión.

Capítulo III
Revolución de los asuntos militares y creación de cibersoldados

En el capítulo 1, se llegó a la conclusión de que, a partir del desarrollo científico de algún tipo de arma, se podían alcanzar dimensiones para llevar la práctica de la guerra. La misma dinámica se presenta en el caso del ciberespacio y la tecnología que permite ejercer la ciberguerra. Tras recordar que se definió el ciberespacio como una dimensión artificial, no ocurre como en las otras formas de guerra donde solo era necesario esperar el armamento para luchar en la tierra, mar o aire, o desplegando dispositivos en el espacio; para el tema de interés, el origen científico y tecnológico tanto del ciberespacio como de la ciberguerra es el mismo.

Tecnología y conflicto: el nacimiento de la ciberguerra

En el contexto de la Segunda Guerra Mundial, el Ejército del Tercer Reich comenzó a emplear un dispositivo que era capaz de encriptar los mensajes militares de manera compleja para así hacer de su estrategia y operación un elemento desconocido para el enemigo. La máquina Enigma, como se denominó al proyecto alemán, motivó a los Aliados a desarrollar uno de los proyectos científicos y tecnológicos

más revolucionarios de la época: la creación del primer procesador de información del planeta (Silberstein, 1992).

Los Aliados respondieron a esta iniciativa con el desarrollo de Colossus (y su segunda versión, Colossus 2). La máquina Colossus, producida por el Departamento de Comunicaciones del Ministerio de Relaciones Exteriores británico, y puesta en funcionamiento en diciembre de 1943, fue probablemente el primer sistema que implementó los principios computacionales con éxito desde el punto de vista de la tecnología contemporánea (Randell, 1980, p. 1).

Este dispositivo fue capaz de descifrar los códigos de encriptación que la máquina alemana creaba en aquel entonces (a diferencia de los diversos grupos de inteligencia técnica militar que habían intentado —sin éxito— entender el método de encriptación): "Jugó un papel determinante descifrando los mensajes de la fuerza aérea alemana, que atacó instalaciones militares y ciudades por toda Gran Bretaña. En 1943, la máquina ya descifraba un total de 84 000 mensajes del código Enigma al mes" (Bejarano, 2014).

La revelación de los protocolos secretos permitió a las tropas de la coalición asestar golpes sorpresivos a los componentes estratégicos del Eje (Chandler, 1983). Esa computadora fue muy valiosa. "Reveló movimientos de tropas, estado de las reservas, municiones y número de soldados muertos, información vital para la segunda parte de la guerra […]. El Colossus ayudó a acelerar el fin de la Segunda Guerra Mundial hasta en 18 meses" (*Emol.com,* 2007).

En aquella época, el Ejército de los Estados Unidos decidió financiar un nuevo dispositivo para calcular las trayectorias y mejorar la orientación de municiones. En colaboración con varios científicos, se completó el Electronic Numerical Integrator and Computer (ENIAC), un nuevo avance en la tecnología computacional (Lemley, Menell, Merges y Samuelson, 2000). De hecho, la mayor parte del esfuerzo aliado en electrónica se concentró en los programas de investigación del Massachusetts Institute of Technology (MIT) y la experimentación real del poder de cálculo; de allí que, bajo el patrocinio del Ejército estadounidense, John William Mauchly y J. Presper Eckert, de la University of Pennsylvania, produjeron en 1946 la mencionada primera computadora con fines generales (ENIAC). Los historiadores recordarán que el

primer ordenador electrónico "pesaba 30 toneladas, fue construido en módulos de metal de dos metros y medio de altura, tenía 70 000 resistores y 18 000 tubos de vacío, y ocupaba la superficie de un gimnasio. Cuando se prendía, su consumo eléctrico era tan alto que la red eléctrica de Filadelfia titilaba" (Castells, 1999, p. 69). Con esto quedó claro que las computadoras fueron concebidas por la Segunda Guerra Mundial como madre de todas las tecnologías.

Con este antecedente, los procesos científicos en investigación y desarrollo de procesadores informáticos se aceleraron exponencialmente. Se llevó a cabo una segunda revolución industrial que permitió consolidar clústeres para la fabricación de las tecnologías informáticas. Entre las décadas de 1960 y 1970, estos conglomerados crecieron exitosamente en Silicon Valley (Valle de Silicio, en alta correlación con la materia prima de las computadoras), en el valle de California (Nye y Owens, 1996).

Al respecto, como resalta Castells (2001), esta revolución informática no pudo haber sido desarrollada sin la participación directa de las universidades. Allí residía la información, investigación y talento humano para construir esta gigantesca aventura tecnológica. El MIT fue pionero en el tema, junto con otros centros de educación superior. La sinergia entre los intereses militares y académicos permitió el desarrollo de sistemas de cómputo y el diseño de procesadores informáticos que aceleraban el procesamiento de datos. En este ámbito, se consolidaron empresas como IBM y Apple.

Como resultado del diverso número de amenazas a la seguridad nacional que podían prever los Estados Unidos en el contexto de la Guerra Fría y, en especial, ante el dilema de la destrucción mutua asegurada, se generaron las condiciones requeridas para que el conjunto de las tecnologías informáticas se viera complementado (y potenciado, sin duda) por la comunicación en red (Abbate, 1994).

Desde la década de 1960, el Departamento de Defensa de los Estados Unidos (United States Department of Defense [DOD]) y el Pentágono vaticinaron que, si se daba un ataque nuclear en suelo nacional, la cadena de mando y control militar, la comunicación estratégica y operacional e, incluso, la coordinación de la respuesta a la agresión quedarían anuladas y se deshabilitarían los medios de

comunicación existentes, tanto por la destrucción física de las explosiones como por el pulso electromagnético que generan las bombas nucleares en la atmósfera al activarse (Abbate, 1994).

Por esta razón, pusieron en manos de la Defense Advanced Research Projects Agency (DARPA) y los centros científicos del país, como el MIT, el desarrollo de ARPANET (Advanced Research Projects Agency Network) en 1972, el primer modelo de internet (Abbate, 1994). Este se originó en un audaz plan ideado en la década de 1970 por los guerreros tecnológicos del DARPA, para evitar la toma o destrucción soviética de las comunicaciones estadounidenses en caso de guerra nuclear. El resultado fue una arquitectura de red que, como querían sus inventores, no podía ser controlada desde ningún centro, compuesta por miles de redes informáticas autónomas que tienen modos innumerables de conectarse, sorteando las barreras electrónicas. ARPANET, la red establecida por el DOD, acabó convirtiéndose en la base de una red de comunicación global y horizontal de miles de redes (Castells, 1999, p. 32).

Si bien ARPANET no tuvo que ser empleada en el escenario para la cual fue diseñada, conforme fueron avanzando sus desarrollos comunicacionales en la transferencia de datos de manera revolucionaria, esta tecnología empezó a ser implementada masivamente en los sistemas militares y civiles estadounidenses. Para 1974, se conocían las posibilidades de las redes mundiales de cómputo; se marcaría, además, la estandarización entre redes. Vinton Cerf, conocido como el padre de internet, junto con Bob Kahn, publicaron el protocolo para intercomunicación de redes por paquetes, en el cual se especifica detalladamente el protocolo que permitió estandarizar el control de transmisión. Este es conocido como Transmission Control Protocol (TCP). El nuevo protocolo permitió la conexión mediante internet (Ballina, 2008, p. 26).

Los resultados de esta implementación fueron tan contundentes que las facilidades que presentaba la comunicación informática en red se extendieron rápidamente por el mundo empresarial. En consecuencia, el uso de esta tecnología se liberó al uso social, lo que permitió que los países homologaran protocolos de conexión y así comenzaran a configurar lo que se denominó la World Wide Web o red mundial (Rogers, 1998). En 1990, Archie, el primer motor de búsqueda en

internet es desarrollado por Alan Emtage en la Universidad McGill. Y, por su parte, Tim Berners-Lee comienza a escribir un código para un programa de un cliente, un navegador y editor al que llama World Wide Web, en su nueva computadora NeXT. El primer sitio web, *nxoc01.cern.ch*, entra en funcionamiento (Press, 2015).

De cualquier modo, si bien es cierto que para hablar del ciberespacio es necesario el desarrollo y la evolución de las tecnologías informáticas (computadoras e internet), durante la segunda mitad del siglo XX el elemento que verdaderamente logró realizar esta dimensión fue la globalización (Khiabany, 2003).

> Esta nueva forma de hacer funcionar al mundo no se conformó con la integración comercial, sino que pronto comenzó a desbordarse para así globalizar prácticas sociales y humanas a nivel político, social y, claro está, también correspondientes al ámbito militar[19]. (Brooks y Wohlforth, 2007, p. 163)

Todos los antecedentes presentados tuvieron su fase de consolidación en la década de 1990. En primera instancia, hubo una injerencia cuantitativa y cualitativa de las tecnologías informáticas en el campo de batalla, al contar con una red de computadoras de última generación conectadas gracias a internet. Este avance se constató de forma irrefutable en la guerra del Golfo Pérsico mediante el despliegue tecnológico realizado por los Estados Unidos (Boot, 2003).

En segunda instancia, porque, una vez iniciado el proceso globalizador en todos los campos y debido a la dependencia tecnologías de la información y de la comunicación (TIC), los Estados se enfrentaron a la realidad irrefutable de un nuevo campo de batalla: el ciberespacio. En efecto, un mundo globalizado únicamente es posible a partir de tecnologías de la comunicación que posibiliten la transferencia de información que transgrede las fronteras de espacio del planeta. Por ende, los gobiernos usaron este marco tecnológico para controlar la infraestructura crítica estatal y las sociedades para construir un contexto de interacción que dio vida a un mundo virtual (Adams, 2001, p. 98).

19 Traducción del autor.

Una vez llegó la década de 1990, la guerra sufriría un cambio significativo tanto en su naturaleza (*war*) como en los medios y las formas de llevar a cabo el combate internamente (*warfare*). Así lo expuso William Lind en su propuesta de una quinta generación de la guerra (Lind, 2004).

Fue claro que el motor que promovió esta transformación se configuró en la confluencia del campo de batalla y la informática en la guerra del Golfo Pérsico (1990). La materialización de esta sinergia se evidenció en la integración de los dispositivos y mecanismos de este tipo al armamento y vehículos militares (aéreos principalmente) y en el empleo de procesadores de datos (y su recepción y envío) en el campo de batalla por parte de las tropas de tierra de los Estados Unidos (en comparación con otras fuerzas que integraron la coalición que se conformó en torno de la Organización del Tratado del Atlántico Norte [OTAN]) (Toffler y Toffler, 1994, p. 67).

Como lo plantea Holmes (2007),

> la primera guerra del Golfo fue una contienda limitada en que una coalición dirigida por Estados Unidos, que gozaba de una abrumadora superioridad tecnológica, derrotó a las Fuerzas Armadas de Irak en una campaña aérea de seis semanas, coronada con una campaña terrestre de cien horas, con muy pocas bajas de la coalición. (p. 547)

Asimismo, Toffler y Toffler (1994) dedican gran parte de sus estudios a la guerra y sus transformaciones, y son de suma pertinencia para entender lo ocurrido en Irak (y Kuwait) entre 1990 y 1991. Para estos sociólogos, en este marco de conflagración se empleó un armamento propio de la era industrial (el cual se ubica en la teoría de Toffler y Toffler [1994] en lo que ellos denominan la "segunda ola de la guerra"). Desde el primer día, se libró también un tipo radicalmente diferente de guerra.

> El mundo se quedó asombrado desde el mismo comienzo [de la guerra del Golfo Pérsico] ante las inolvidables imágenes en televisión de los misiles Tomahawk y las bombas guiadas por láser que buscaban y alcanzaban objetivos en Bagdad con una sorprendente precisión: el cuartel general de las fuerzas aéreas iraquíes, el Centro de Servicios de la Información, el Ministerio de Interior

> (cuartel de la policía de Saddam), el edificio del Parlamento y el de su partido Ba'ath. (p. 100)

En este primer acercamiento de los investigadores es posible notar la integración de armamento de artillería con las tecnologías informáticas. En efecto, fue el primer momento en que se logró contemplar las capacidades estratégicas y operacionales que aportaba un misil capaz de ser teledirigido hacia un objetivo deseado (Cordesman y Wagner, 1990).

No obstante, y retomando a Toffler y Toffler (1994), es preciso analizar otro fragmento de su investigación para comprender la inmersión de la informática en la guerra del Golfo Pérsico, pues en esta volaron dos de las más potentes armas de información de aque entonces: el Airborne Warning & Control System (AWACS) y el J-Stars. Un Boeing 707 repleto de computadoras, equipo de comunicación, radar y detectores, el AWACS exploraba los cielos en 360º para detectar aeronaves o cohetes enemigos y enviaba datos de localización a los aviones de interceptación y a las unidades terrestres (Cordesman y Wagner, 1990, p. 105).

De igual manera, tomando como referencia que este teatro de guerra también se caracterizó por el empleo de la aeronave furtiva (antidetección y espía gracias a sus adelantos tecnológicos aeroespaciales e informáticos), de la United States Air Force (USAF), el F117A (cuyo primer modelo data de 1975), es contundente cómo y cuál fue la incidencia de la tecnología informática en la guerra del Golfo Pérsico (Richardson, 2001, p. 116).

Por esto, no ha sido contradictorio observar posiciones como la de Campen (1994), quien afirma que "la guerra del Golfo Pérsico fue una contienda en la que unos gramos de silicio en un ordenador pudieron haber tenido un mayor efecto que una tonelada de uranio" (citado por Toffler y Toffler, 1994, p. 104). De allí que, desde un comienzo, la intervención de la tecnología informática en los enfrentamientos en Irak en 1990 trajera consigo una transformación denominada la "revolución de los asuntos militares" (Metz y Kievit, 1995), como se analizará en el siguiente apartado.

En síntesis, cuando se analiza el surgimiento y la evolución de las tecnologías informáticas a partir de Colossus (computadoras) y

ARPANET (internet), es posible establecer que estas están estrechamente vinculadas a los ámbitos de los conflictos armados y así se traducen en elementos para apoyar la estrategia (Segunda Guerra Mundial), con el objetivo final de inhabilitar al enemigo el acceso a la información propia y consolidando efectivos y extensivos canales de mando y control (Guerra Fría).

3De esta manera, el verdadero cambio en la forma y los medios para hacer la guerra lo trajo el uso de la computadora. No fue simplemente establecer nuevos medios para el mando y control, significó el envío de datos a nivel estratégico, operacional y táctico con una inmediatez nunca vista. Esta tecnología permitió procesar información multimediática (imagen y audio) simultáneamente y en tiempo real por medio de internet (Bishop y Goldman, 2003).

Tecnologías informáticas y revolución en los asuntos militares

Consecuentemente, la implementación de estos elementos en la guerra generó una nueva revolución de los asuntos militares. Cada poder militar (tierra, mar, aire y espacio) se ha transformado con el desarrollo de nuevas tecnologías. El caso más patente es el de las TIC. La tecnología informática, con sus debilidades y fortalezas, se ha convertido en un referente fundamental para el desarrollo del ciberespacio como dimensión de interacción social desde la década de 1990 (Castells, 2000).

Como resultado de esta historia, en las décadas finales del siglo XX, se abordó un nuevo enfoque que privilegiaba la evolución tecnológica como factor estratégico para ganar las guerras. De origen ruso, pero llevado a su máxima expresión por los estadounidenses, fue conocido como la revolución de los asuntos militares (*revolution in military affairs* [RMA]), entendido como el estudio científico de la guerra como fenómeno social, que permite comprender el impacto de la inclusión de nuevas tecnologías a nivel estratégico, operacional y táctico (Grinter y Scheneider, 1998). Esta perspectiva ha permitido que la concepción del teatro de operaciones se diversifique (McKitrick, Blackwell, Littlepage, Kraus, Blanchfield y Hill, 2001).

McKitrick *et al.* (2001) concuerdan en que la RAM, desde una perspectiva conceptual y teórica,

> es un cambio importante en la naturaleza de la guerra provocada por la aplicación innovadora de las nuevas tecnologías que se combinan con cambios drásticos en la doctrina militar y las operaciones y los conceptos de organización, ya que altera fundamentalmente el carácter y la conducta de las operaciones militares[20]. (p. 65)

A partir de un análisis retrospectivo de los estadios en los cuales las RAM han impactado las fuerzas militares (observado desde un enfoque teleológico), Grinter y Scheneider (1998) sustentan que una revolución en asuntos militares se da por innovaciones tecnológicas, como sucedió con las armas nucleares al final de la Segunda Guerra Mundial. Otras veces, las innovaciones en el desarrollo estratégico logran transformar la forma de hacer la guerra, como lo hicera la maniobra alemana de la *blitzkrieg*. Y a su vez, los cambios sociales —la "nación en armas" de Napoleón Bonaparte, por ejemplo— también pueden contribuir a la RAM. Así, las revoluciones pueden ser creadas por una combinación de acontecimientos, como el fortalecimiento y la integración de desarrollos operacionales militares (p. 43).

Al profundizar en el punto anterior, Cooper (1997) propone tres modelos distintos para estos tipos de innovación militar fundamental. El primer tipo de RAM está impulsado por una tecnología nueva y netamente militar, inducida por invenciones o desarrollos científicos o tecnológicos fundamentales. Este es el tipo que casi todos identifican como *revolución*, pero realmente son pocos los ejemplos de ella —tal vez el arco y la pólvora son los únicos de este tipo—.

El segundo tipo de RAM es aquel que impulsa la innovación operativa y organizativa para corregir problemas estratégicos y, desde la perspectiva de hoy, puede ofrecer la mejor oportunidad para abordar los problemas a corto y medio plazo. Y el tercer tipo, "del cual la RAM napoleónica es el ejemplo clásico, está impulsado por cambios

20 Traducción del autor.

económicos, políticos y sociales fundamentales fuera del dominio militar inmediato"[21] (Cooper, 1997, p. 118), los cuales permiten una transformación profunda tanto de la naturaleza como de la conducta de la guerra.

Al desagregar los factores generadores de las revoluciones observadas, es claro que el factor tecnológico (informático para el caso) se perfila como uno de estos en las fuerzas militares estadounidenses en 1990 y 1991. Para contribuir al entendimiento de este elemento, Bishop y Goldman (2003) establecen en un principio que

> la tecnología de la información, sin embargo, siempre ha sido definitiva en la guerra y crucial para la mejora de la eficacia militar. El establecimiento de una red telegráfica influyó considerablemente en el desarrollo de operaciones militares y mejoró la eficacia de las fuerzas militares durante la guerra civil estadounidense y las guerras de unificación alemanas. Durante el periodo de entreguerras, el rápido crecimiento en la aplicación de la radio, y más tarde el advenimiento del radar, tuvo una enorme influencia en las operaciones militares. El desarrollo de la *blitzkrieg* del Ejército alemán dependió claramente de las capacidades de la radio para articular las grandes y rápidas operaciones coordinadas entre los mecanizados y la aviación. Paralelo a este hecho, se encuentra la contramedida de Gran Bretaña con sus sistemas de defensa aérea sustentados en el desarrollo del radar. La introducción de la tecnología cableada alrededor del mundo casi a la vuelta del fin del siglo XX también representa un aspecto importante[22]. (pp. 133-114)

Cuando se analiza el postulado de que la información y la tecnología que la transmite han sido determinantes en el accionar militar en los episodios de guerra de los últimos cien años, debe establecerse que la información a partir de la guerra del Golfo Pérsico adquirió un valor exponencial sin parangón alguno. Es evidente que el significado

21 Traducción del autor.

22 Traducción del autor.

que comenzó a adquirir la información en la contienda bélica también fue determinante para la revolución de los asuntos militares (Norman, 1997).

Esta postura expone que la información en la guerra ya dejó de ser interpretada como conducto, y ahora se valora como contenido. A partir del presente postulado, Bishop y Goldman (2003) establecen un paralelo entre Clausewitz y Sun Tzu, para ilustrar el cambio que sufrió la información como valor inmaterial a partir del siglo xx:

> Fue el escepticismo de Clausewitz sobre la fiabilidad de la información y la inteligencia a nivel táctico y operacional lo que lo llevó a destacar, en *De la guerra*, la necesidad de optimizar las tropas en formaciones unificadas en grandes bloques, mantener las reservas y proteger a los comandantes que poseen la intuición y la experiencia. Para Sun Tzu, por otra parte, en *El arte de la guerra*, el engaño, la desinformación y el conocimiento de los pensamientos más íntimos del enemigo, y de los planes, son la clave para la sorpresa y la victoria, quizá incluso una victoria sin derramamiento de sangre[23]. (p. 114)

Al tomar como principio este razonamiento, Arquilla y Ronfeldt (1997) llevan el concepto del *cambio de estimación de la información en el campo de batalla* a otra instancia. Si bien en la década de 1990 se originó un proceso de revolución de los asuntos militares, fue gracias a que la información también sufrió una revolución. Este postulado se sustenta en las características propias que presentó la conjunción de las tecnologías informáticas y el elemento información en el contexto señalado.

La tecnología empleada por primera vez se erigía sobre el principio multimedia, es decir, recepción, procesamiento y envío simultáneo de imagen, video, audio y texto. En segundo lugar, este tipo de datos se transmitió trasgrediendo las barreras de espacio y tiempo gracias a internet (Arquilla y Ronfeldt, 2001). Por esto, Campen (1994) señala que "virtualmente cualquier aspecto bélico se halla ahora automatizado y exige la capacidad de transmitir grandes cantidades de datos

23 Traducción del autor.

en formas muy diferentes" (citado por Toffler y Toffler, 1994, p. 105). Las capacidades comunicacionales, informacionales y de acoplamiento que ofrecen las tecnologías informáticas desde hace veinte años facilitan la transmisión de datos que logró transformar la naturaleza de la guerra, y los medios y las formas para proceder en ella.

Arquilla y Ronfeldt (1993) instauran la idea de que la información debe apropiarse desde una concepción más cercana al "conocimiento". Por otro lado, estos autores reafirman la importancia de usar adecuadamente la información para gestionarla en paquetes de conocimiento. Este proceso, que ha sido analizado por los autores clásicos de la guerra, adquiere una nueva dimensión en el ciberespacio:

> A partir del cálculo de fuerzas, la guerra ya no es principalmente una función de quien dispone de la mayor parte del capital, mano de obra y tecnología en el campo de batalla, sino de quien tiene la mejor información sobre este. Lo que distingue a los vencedores es su dominio de la información, desde el punto de vista mundano de saber encontrar al enemigo, mientras lo mantiene en la oscuridad, y en términos doctrinales y organizacionales[24]. (p. 141)

En definitiva, la RAM se originó debido al nuevo tipo de tecnología y al desarrollo de la guerra y el accionar de los ejércitos (Jablonsky, 1994). Por otra parte, se dio un cambio en la estrategia, el sistema operacional y el táctico conforme a la información (potenciada por las tecnologías en cuestión), que se tradujo en conocimiento (Cebrowski y Garstka, 1998). Wilson entrega una definición de la información mucho más cercana al valor militar que adquirió en las postrimerías del siglo pasado:

> La información es un recurso creado a partir de dos componentes: los fenómenos (o datos) que se observan, además de las instrucciones (sistemas) necesarias para analizar e interpretar los datos que le dan sentido. El valor de la información se ve reforzado por las tecnologías, tales como las redes y bases de datos, que permiten a

24 Traducción del autor.

> los militares crear un mayor nivel de conciencia común, sincronizar mejor la información de mando, control e inteligencia, y traducir superioridad en el poder de combate[25]. (2004, p. 2)

Otro de los aspectos que se enriquecieron mediante el desarrollo de la RAM en la década de 1990 fue la organización y el despliegue de las tropas en sus dimensiones de influencia desde el punto de vista de la estructura de mando, control y comunicaciones, lo que generó una coordinación global de las fuerzas (Manthorpe, 1996).

En los Estados Unidos, esto se constató con la Information Technology Management Reform Act (ITMRA) de 1996, conocida como la Ley Clinger-Cohen, legislación fruto de los esfuerzos iniciados con la Ley de Desempeño y Resultados del Gobierno (Government Performance and Results Act [GPRA]) de 1993. Este marco legislativo determinó los códigos de eficiencia, la interoperabilidad y la explotación efectiva de los objetivos a partir de las demandas de los comandos, las agencias y los servicios del DOD (1996).

En la *Joint Vision 2010*, difundida en 1996 por el Estado Mayor Conjunto del Ejército de los Estados Unidos, se constató que las fuerzas militares en su estructura horizontal de mando y control habían adquirido las tecnologías y el empleo exponencial de la información (Shelton, 1998). Esta directriz, además, determina una serie de niveles: primero, alcanzar el dominio de la maniobra, es decir, poseer el control total de cuándo y dónde se lleva a cabo la batalla; segundo, desarrollar la habilidad de impactar con precisión diversos objetivos; tercero, consolidar una defensa multidimensional, y cuarto, la capacidad para defenderse de todas las amenazas sin tener distinción de su origen. Todas estas acciones se enmarcan en el desarrollo logístico necesario para entregar el material o recurso preciso donde realmente se requiera (Libicki, 1998).

Se puede constatar cómo los procesos de reconfiguración de la estructura organizacional, movilidad y operaciones de los ejércitos en la actualidad solo son posibles gracias a los marcos de arquitectura de las tecnologías informáticas:

25 Traducción del autor.

> En la actual coyuntura histórica, cabe apreciar, en los documentos doctrinales del ejército estadounidense y la Alianza Atlántica, una nueva concepción del ejército: el ejército-red o ejército inteligente, cuya fuente de poder y proyección militar descansa en la información y el conocimiento, en la capacidad organizativa y de decisión con criterio al acometer los diversos y complicados retos de la sociedad global. (Sierra, 2003, p. 259)

Como lo describe Bendrath (2001), este proceso es evolutivo: al inicio de la era informática, el marco se basó en la lógica del C2I (comando, control e inteligencia); posteriormente, se posicionó el C3I (comando, control, comunicaciones e inteligencia), y luego el C4I (comando, control, comunicaciones, computadoras e inteligencia militar).

A partir de la guerra del Golfo Pérsico, se concretó un salto de calidad en este modelo. Los Estados Unidos adoptaron el C4ISR (comando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento). Este modelo instaura un sistema sinérgico de capacidades informáticas nunca visto (Bendrath, 2001). Desde esta perspectiva, se puede hablar de una nueva forma de guerra: la guerra de la información, o *information war* (IW) (Molander, Riddile, Wilson y Williamson, 1998). Toffler y Toffler (1994) describen la nueva tipología de guerra que se inició en la Operación Tormenta del Desierto: "El J-Star o sistema conjunto de radar de vigilancia y ataque al objetivo exploraba el suelo. Fue concebido para contribuir a la detección, el quebrantamiento y la destrucción de los escalones subsiguientes de una fuerza terrestre enemiga"[26] (p. 105).

Finalmente, se evidencia el desbordamiento del fenómeno de la revolución informática y la revolución de los asuntos militares que sobrevino a partir de 1990:

> Se comienza a reconocer en todo el mundo que una economía de fuerza mental, como las de los Estados Unidos, Japón y Europa, supone un estamento militar de base mental. Desde luego, hasta los países de baja tecnología se apresuran a incrementar los

26 Traducción del autor.

> sectores de conocimiento intensivo de sus Fuerzas Armadas[27]. (Toffler y Toffler, 1994, p. 105).

Las tecnologías y la información como armamento en los conflictos armados contemporáneos

La inclusión de una tecnología totalmente novedosa para la época al *teatro de guerra* y, por supuesto, los cambios doctrinales y operacionales de estos nuevos elementos permitieron a las fuerzas militares desenvolverse en un inusitado *teatro de operaciones* (Harshberger y Ochmanek, 1999).

Aunque estos dos elementos de cambio, en gran parte de la literatura en español, se tienden a agrupar al unísono de la atmósfera conceptual de la guerra, debe tenerse en cuenta que el inglés emplea dos conceptos con diferentes significados: *war* y *warfare*. Emplear el enfoque de análisis del término *war* implica interpretar la guerra desde su concepción fenomenológica pura, a partir de su estudio ontológico según los aspectos políticos, históricos, sociológicos, antropológicos, que intervienen en su configuración. En otro sentido, la utilización del *warfare* como marco de comprensión conlleva denotar componentes yuxtapuestos a las estrategias empleadas en el combate por los actores involucrados y, en relación, cómo se despliegan y de qué manera se emplean los recursos para llevar a cabo la confrontación armada (Granada y Sánchez, 2009).

Lo anterior permite agregar al estudio componentes que sustentan el hecho de que, a partir de los cambios descritos, se crearon las condiciones y los escenarios necesarios para propiciar el nacimiento de una nueva tipología de guerra, y la forma de llevarla a cabo, partiendo del principio de que la información se convirtió en un bien (inmaterial) determinante para conducir la guerra. En este ámbito, surgieron las operaciones de la información (OI), en el contexto de una nueva forma de *warfare* (Motoike y Yoshikawa, 1999).

27 Traducción del autor.

Desde esta perspectiva, la IW se fundamenta en el desarrollo de acciones adoptadas en tiempo de crisis o conflicto que afectan la información del adversario. Esta acción complementa el diseño de sistemas de protección de la información relacionada con la seguridad nacional. Es de suma importancia el núcleo operacional de esta nueva forma de hacer la guerra en la alteración o la influencia que se genera en el proceso de toma de decisiones del enemigo (Wilson, 2007).

La inclusión de las tecnologías informáticas en la guerra otorga una superioridad en las capacidades militares, como se constata con los Estados Unidos en la guerra del Golfo Pérsico. No obstante, este tipo de adquisición de capacidades materiales trae consigo un riesgo inminente, una dependencia tecnológica que se constituye como debilidad estratégica (Arquilla, Ronfeldt y Zanini, 2000).

> Si los sistemas informáticos (para los Estados, o sistemas de seguridad nacional en general) se convierten en el *centro de gravedad* para los modernos cuerpos militares, esto se configurará como un blanco lógico para otros; por consiguiente, el advenimiento del *information warfare* se presenta como promisorio y prospectivo[28]. (Libicki, 1998, p. 411)

La información en el ciberespacio ha adquirido la categoría de arma y objetivo en la guerra, lo que ha materializado la alteración e influencia psicológica esperada. Existen operaciones psicológicas, operaciones de engaño, operaciones de seguridad, operaciones de computadoras en red y operaciones electromagnéticas (Wilson, 2004). Concretamente,

> las operaciones psicológicas planean el envío de información seleccionada para influir en las emociones, las motivaciones, los razonamientos objetivos, en última instancia, el comportamiento de gobiernos extranjeros, organizaciones, grupos e individuos […]. Las operaciones de engaño guían al enemigo a la toma de decisiones erróneas mediante la presentación de información falsa, imágenes y declaraciones […]. Las operaciones de seguridad

28 Traducción del autor.

> se definen como un proceso de identificación de información que puede ser crítica para las operaciones coordinadas y combinadas, o que permitirían al enemigo atacar vulnerabilidades propias [...]. Las operaciones de computadoras en red buscan atacar y deshabilitar las redes de datos del enemigo, defender los sistemas militares inherentes y explotar la red de computadoras del enemigo mediante acciones de inteligencia. [Finalmente] las operaciones electromagnéticas son cualquier tipo de acción militar que envuelva el direccionamiento o control de la energía que sustenta el espectro electromagnético para engañar o atacar al enemigo[29]. (Wilson, 2004, pp. 3-7)

De manera concluyente, Bradley entrega su concepto acerca de la IW (forma de operar mediante la información y la tecnología que la controla):

> Las operaciones de la información (OI) no son simplemente atacar los sistemas informáticos. Las OI consisten en analizar la tecnología, los procesos y los factores humanos que afectan la mente de quien toma las decisiones. Las operaciones informáticas pueden ser dirigidas contra líderes o tomadores de decisiones de alto nivel, pero también pueden afectar a cada escalón de la estructura militar, industrial e, incluso, la población en general. Las OI defensivas garantizan acceso a la información oportuna, precisa y relevante, al tiempo que niegan a los adversarios la oportunidad de explotar la información de fácil acceso y los sistemas informáticos para sus propios fines[30]. (2003, p. 4)

La guerra de información como categoría se configura en una línea temporal de esfuerzos conceptuales, que determinaron los cambios estratégicos y operacionales que surgieron por causa de la sinergia entre la tecnología informática y el accionar de los ejércitos en el conflicto.

29 Traducción del autor.

30 Traducción del autor.

Comprensión del cibersoldado

Queda claro que muchas de las redes gubernamentales, militares y privadas de hoy están conectadas a internet o entre sí. Esto es necesario para el acceso y la funcionalidad. Pero también abre un camino a los militares extranjeros u otros actores con intenciones peligrosas. Y entonces este camino puede ser usado para comprometer la infraestructura crítica o la información. Así que la gran necesidad de los Estados ahora es desarrollar nuevos guerreros cibernéticos. Estos tienen que ser capaces de defender tales sistemas críticos y vías, y en algunos casos, de realizar operaciones ofensivas (Allen y Allen, 2012).

Es natural utilizar principios militares y terminológicos para discutir elementos de esta nueva era de creciente vulnerabilidad cibernética. Aunque los involucrados pueden o no usar uniformes, o no luchar a lo largo de fronteras geográficas lineales, hay claramente un alto ambiente competitivo que es conducente a la conceptualización militar bien entendida.

> Por tanto, existen analogías como zonas desmilitarizadas (redes de servicio público moderadamente protegidas), arsenales (mecanismos de protección de datos), perímetros (límites entre diferentes niveles de riesgo de datos), paso seguro (protección de datos a través de dominios desprotegidos) y ciberguerreros (militares profesionales). (Fulp, 2003, p. 261)

A medida que crece la importancia de las operaciones cibernéticas en la guerra, la capacidad de los militares estadounidenses para asegurar una fuerza de trabajo cibernética robusta se hace cada vez más importante para proteger a la nación. Una de las cinco iniciativas principales en la estrategia cibernética del DoD es aprovechar el ingenio de la nación a través de una fuerza de trabajo cibernética excepcional y una rápida innovación tecnológica. El desarrollo y la retención de una fuerza de trabajo cibernética excepcional es fundamental para el éxito estratégico del DoD (Li y Daugherty, 2015, p. 1).

No es en vano, y como se logró ver anteriormente, que los Estados Unidos se convirtió en una cultura doctrinal, a partir de la RAM, logrando adaptar sus Fuerzas Armadas al contexto informacional y

ciberespacial en mayor rigor. Como tal, los soldados estadounidenses han tenido que ser rehechos para encajar, operar y funcionar en esta era tecnológica y ostensiblemente nueva, pues los nuevos tiempos parecen requerir nuevos soldados para el trabajo de defender a la nación (Masters, 2010).

Lo interesante de los Estados Unidos para recrear el tema de los cibersoldados es que, además de reconocer la vitalidad de la cuestión desde el contexto militar o la guerra, también acepta una característica ya analizada del ciberespacio como dimensión; al integrar tantas infraestructuras críticas, no solo intervienen soldados en la ciberguerra, sino también civiles defendiendo a sus Estados de esta:

> Si bien los guerreros cibernéticos son el grupo más altamente especializado de individuos involucrados en la guerra cibernética ofensiva y defensiva, la fuerza de trabajo cibernética es en realidad mucho mayor. Un informe del DoD de 2011 describe una fuerza laboral cibernética de más de 160 000 militares y civiles, más del 5 % de la fuerza de trabajo del DoD. La fuerza de trabajo cibernética es muy diversa e incluye a personas que proporcionan servicios básicos de tecnología de la información (TI), diseñan sistemas, protegen redes y se involucran en la guerra cibernética, entre otras actividades[31]. (Li y Daugherty, 2015, p. 9)

En un intento por describir mejor la fuerza de trabajo cibernética y los deberes laborales que desempeñan estos individuos, el DoD divide la fuerza laboral cibernética en tres grupos: operadores y mantenedores, aseguradores de la información y encargados de operaciones defensivas. El DoD define las operaciones defensivas como contramedidas diseñadas para detectar, identificar, interceptar, destruir o negar actividades dañinas que intentan penetrar o atacar a través del ciberespacio. Casi el 90 % de la fuerza laboral fue designada como operadores y mantenedores, mientras que solo el 9 % se consideró como garante de la información, y solo el 2 % trabajaba en operaciones defensivas (3777 personas) (Li y Daugherty, 2015, p. 11).

31 Traducción del autor.

Desde otro enfoque, es preciso mencionar que existen operadores de ciberguerra, los cuales planean, dirigen y ejecutan actividades ofensivas y defensivas en y a través del ciberespacio; técnicos del ciberespacio que crean, proporcionan y mantienen diversos sectores del ciberespacio; analistas y encargados de la selección de objetivos de ciberguerra que ofrecen apoyo de inteligencia a las operaciones de ciberguerra, y, finalmente, desarrolladores de ciberguerra que diseñan y crean herramientas y armas para la ciberguerra (Páez, 2014, p. 10).

> Los ciberguerreros son aquellos individuos que con su conocimiento pueden diseñar programas y ciberarmas capaces de infiltrar el sistema de una organización o entidad, y con esto acceder a información confidencial, poner bombas lógicas y sabotear el correcto funcionamiento de los flujos de información, desde una página de internet, el funcionamiento de la red eléctrica de una ciudad o hasta de un país entero. Muchos pueden definir a los ciberguerreros como los individuos que realizan estas acciones y están adscritos a la fuerza militar de un Estado determinado. (Vargas, 2014, p. 5)

Para los estadounidenses, los soldados cibernéticos son expertos técnicos altamente calificados que proporcionan inteligencia crucial y soporte de red que protege el dominio cibernético y asegura que los comandantes pueden maniobrar y ganar. Además, establecen que los soldados de otras especialidades del Ejército, como la inteligencia militar, también pueden servir o apoyar a las unidades cibernéticas en ocasiones específicas. Como defensor de la presencia de los Estados Unidos en el ciberespacio, un cibersoldado recopila, analiza y reporta datos digitales, despliega y mantiene herramientas de defensa de la red como enrutadores y *firewalls*, evalúa las operaciones de defensa de la red y responde a incidentes en el ciberespacio (U.S. Army Cyber Command, 2016a).

Al recordar los planteamientos del capítulo 2 acerca del concepto de *ciberarma*, desde esta perspectiva se puede añadir que los guerreros cibernéticos deben comenzar con la comprensión conceptual sólida de que las computadoras son, en última instancia, nada más que las estructuras físicas que proporcionan un medio para que todo aquello que sucede en el ciberespacio sea traído a la vida corporal (Fulp, 2003, p. 263). Asimismo, las tecnologías que permiten ser al cibersoldado

representan la promesa de lograr una mayor letalidad arriesgando menos personas, con menos víctimas y, quizá, a un costo menor. Así, el concepto de *soldado cibernético* podría reducir la necesidad de grandes fuerzas terrestres (Hosek, 2003, p. 183).

Fulp (2003) propone que los cibersoldados se dividen en dos categorías: tácticos cibernéticos y ciberestrategas. Los tácticos cibernéticos se concentrarían en reducir el riesgo de los sistemas existentes sobre el terreno, principalmente mediante la aplicación de salvaguardias apropiadas (por ejemplo, *firewalls*, detección de intrusiones, configuraciones redundantes, respaldos de datos, etc.). Los estrategas cibernéticos se enfocarían en reducir el riesgo de los sistemas futuros, principalmente, a través de la aplicación de técnicas estructuradas y formales de diseño de sistemas que reduzcan las vulnerabilidades (p. 262).

Por su parte, el enfoque del ciberestratega es reducir el riesgo al disminuir las vulnerabilidades del sistema. Un sistema sin vulnerabilidades no da lugar a ningún riesgo, con lo que se niega la necesidad de salvaguardias posteriores. El sistema con cero vulnerabilidades es el ideal perseguido por los ciberestrategas, y el logro de esto requiere un conjunto de habilidades mucho más teóricas que las del táctico cibernético. Mientras el táctico cibernético construye una pared protectora virtual alrededor de sus sistemas, el estratega cibernético edifica un sistema tan fuerte que no necesita protección (Fulp, 2003, p. 271).

Paul, Porche y Axelband evidencian cómo el DoD conformó hace unos años una lista con las funciones que un cibersoldado debe cumplir en la era del ciberespacio, que, por tanto, son necesarias para el buen funcionamiento de las fuerzas militares contemporáneas:

1. Administradores y técnicos:
   Actividades: solucionar problemas técnicos, instalar *hardware* y *software*.
   Capacitación: operar y reparar *hardware,* configurar servidores, etc.

2. Desarrolladores e ingenieros:
   Actividades: diseñar y desarrollar herramientas, *software* y otras tecnologías de la información para apoyar las actividades de la organización.

Capacitación: conocimiento de idiomas y sistemas operativos utilizados. La mayoría de los desarrolladores en organizaciones públicas y privadas tienen una licenciatura en Ciencias de la Computación o ingeniería y maestrías en campos relacionados.

3. Analistas:
   Actividades: reunir información sobre el desempeño de la red para fines forenses.
   Capacitación: supervisada por la organización. Por lo general, una licenciatura en Ciencias de la Computación es un requisito mínimo para las posiciones de la industria.
4. Personal de adquisiciones.
5. Entrenadores y educadores.
6. Planificadores:
   Actividades: planificación de misiones.
   Capacitación: en general, supervisada por una organización de entrenamiento militar.
7. Operadores:
   Actividades: realización de misiones planificadas, tanto ofensivas como defensivas.
   Capacitación: supervisada por la Agencia de Seguridad Nacional (National Security Agency [NSA]) y las escuelas de inteligencia en cada servicio[32]. (2014, p. 25)

Se espera que los guerreros cibernéticos defiendan redes o usen sistemas complejos de armas cibernéticas, por lo que típicamente requieren un entrenamiento extensivo más allá de lo que se proporciona al militar o trabajador civil promedio en el mismo campo. Existe la preocupación de que estos requisitos de formación sustanciales y la rápida ampliación de la mano de obra conducirán a retos que satisfagan las necesidades de mano de obra[33]. (Li y Daugherty, 2015, p. 3)

32 Traducción del autor.

33 Traducción del autor.

La previsión de los expertos para los soldados del siglo xxi es que tendrán que pensar mucho más. Portando sus uniformes perfeccionados, llevarán pequeños ordenadores, instrumentos de telecomunicaciones móviles y armas complejas de tiro casi infalible. Tendrán que ser altamente tolerantes a la ambigüedad y a la incertidumbre, deberán estar también en capacidad de tomar la iniciativa, improvisar e imponer su propio juicio. Su adiestramiento será muy completo y distará mucho de los valores militares que se inculcan actualmente (Cohnen, 2010, p. 18).

Existen diferencias marcadas entre un soldado de corte tradicional y el denominado cibersoldado. El soldado formado bajo las rígidas convenciones castrenses es activo, esquemático, retrospectivo, longitudinal, tiene una visión parcial (dado que maneja información según el nivel en el que se encuentra dentro de la cadena de comando), es predecible, tiene una formación básica en informática (como la tiene cualquier usuario normal y corriente) y el teatro de operaciones donde se prepara para actuar se limita a la tierra, el mar y el aire. El cibersoldado, en cambio, es proactivo, prospectivo, transversal, posee una mayor cosmovisión, es impredecible y disruptivo, posee una avanzada capacidad informática y el teatro de operaciones en el que se desempeña es el ciberespacio o espacio virtual. Desde una perspectiva psicológica, el perfil de un cibersoldado surge a partir de tres ejes principales: una avanzada capacitación en informática, la obtención y el manejo de la información y el poder de análisis de esta con una concepción táctica y estratégica de su uso (Páez, 2014, p. 11).

Tradicionalmente, el término *soldado* estaba confinado a los combatientes, es decir, a los hombres que en realidad participaban en batallas físicas. La fusión con la tecnología ha borrado significativamente esta distinción tradicional, y ahora los civiles pueden ser considerados soldados. El personal militar, que probablemente nunca estará en batalla física, que literalmente se sienta frente a las pantallas de las computadoras, ahora se ha constituido en soldados a través de la interfaz, con lo que se ha ampliado y reconfigurado en efecto las representaciones de los soldados. Estos, tras la transformación tecnológica, casi por definición, nunca tendrán que volver a poner los ojos en su enemigo, la mirada será la del arma, pantalla de computadora y sistemas de orientación por satélite de posicionamiento global. En

el continuo de la despersonalización y la deshumanización discursivas tradicionales, el soldado representa el extremo de la desencarnación abstracta, ya que la disciplina tradicionalmente requerida para alejarse de la realidad de la guerra, si es posible, ya no es necesaria (Masters, 2010). Un gran número de Estados están creando ejércitos de cibersoldados que puedan hacer frente a esta nueva amenaza y lanzar la suya propia:

> Estados Unidos ha reunido un grupo de *hackers* de élite que se estaría preparando para luchar en caso de que se desencadenase una ciberguerra. Es lo que se conoce como Joint Functional Component Command for Network Warfare (JFCCNW), un cuerpo que reúne personal de la CIA, FBI, Agencia Nacional de Seguridad, miembros de los cuatro ejércitos e incluso civiles y militares de los países aliados de los Estados Unidos, y que tiene como función defender a todo el sistema informático de las instituciones del Estado, destruir redes, entrar en los servidores de posibles enemigos para robar o manipular información y dañar las comunicaciones rivales hasta inutilizarlas.
>
> La Unidad Estratégica de Reconocimiento del ejército alemán está coordinando un equipo de soldados para que aprendan a infiltrarse, manipular y explotar las redes informáticas del adversario.
>
> China ha creado una estructura de reserva especializada en telecomunicaciones, que cuenta con el apoyo de un contingente de personal altamente capacitado de expertos en computación, peritos en el monitoreo de redes y unidades de telecomunicaciones por radio. Estas fuerzas de reserva hoy en día tienen capacidad para hacer algo que queda fuera, incluso, del alcance del Ejército de Liberación Nacional (ELN) como es emplear armas electrónicas y de información para alcanzar a un adversario en otro continente. Pero, además, el ELN ha incorporado tácticas de guerra cibernética en ejercicios militares, ha instituido una serie de escuelas que se especializan en la guerra informática y están contratando a graduados en informática para desarrollar sus capacidades en la guerra cibernética y, así, poder configurar un ejército de *hackers*.

> Corea cuenta con una academia militar especializada en guerra informática que está instruyendo en técnicas de creación de virus, penetrar en sistemas, programar sistemas guiados de armas, etc., a 100 cibersoldados cada año.
>
> La OTAN ha creado un centro de excelencia para formar expertos en informática, electrónica y comunicación con el único fin de combatir el ciberterrorismo. (Sánchez, 2009, pp. 236-237).

Como integrante de la modernización de la fuerza del ejército para las operaciones del ciberespacio, las redes de comunicaciones y servicios de información y la guerra electrónica, el Cyber Center of Excellence (CCOE) integra y desarrolla la doctrina, la organización, la capacitación, el material, el liderazgo, el personal y las instalaciones, y coordina con el U.S. Army Intelligence Center of Excellence (USAICOE) el apoyo de la inteligencia institucional a las operaciones del ciberespacio. El CCOE garantiza que las capacidades de operación del Ejército, el combate electrónico y la operación de señales evolucionen con los requisitos y las capacidades de la fuerza conjunta. La Escuela Cibernética establece las bases para el desarrollo de fuerzas cibernéticas capacitadas para cumplir estándares comunes a fin de satisfacer las necesidades actuales y futuras de los comandantes combatientes (U.S. Army Cyber Command, 2016a).

Future Soldier 2030 es un concepto de cómo el futuro soldado podría estar equipado. Este se ajustará a las consideraciones de diseño para cada nombre de área de tecnología, con especial énfasis en el rendimiento cognitivo para mejorar la efectividad del soldado y un aumento en el tiempo operacional. Existen siete áreas principales dentro del Future Soldier y, claramente, una de ellas tiene que ver con el ciberespacio, la ciberguerra y las ciberoperaciones.

Pero el cibersoldado trasciende los límites de la virtualidad del ciberespacio. A partir de que la información se ha integrado con elementos de la guerra que aún funcionan en el ámbito real de la guerra, los nuevos guerreros deberán acostumbrarse a los entornos aumentados y virtuales simultáneamente, pues todas las facetas de la guerra, que incluyen comunicaciones, visualización de datos, control del sistema y entrenamiento, se van a encontrar allí. Los soldados podrán moverse

sin problemas entre entornos reales, aumentados y virtuales. El uso de sistemas de realidad virtual (VR) y tecnologías de juego será el modo primario para la selección y el entrenamiento del personal. El entrenamiento estará integrado y disponible en cualquier momento y en cualquier lugar. El entrenamiento se incrementaría con el uso de agentes de *software* inteligente y herramientas de modelado y simulación residentes en cada tipo de sistema *soldier*, y les dará capacidades analíticas y de toma de decisiones que empequeñecen lo que actualmente está disponible para los principales puestos de mando (Casey, 2009).

> La herramienta militar del futuro más espectacular será el propio soldado. Al menos, eso es lo que pretenden algunos expertos estadounidenses. Su objetivo sería crear una especie de *biorrobot* capaz de funcionar a pleno rendimiento las veinticuatro horas del día. La Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA) es la encargada de desarrollar este inquietante guerrero del siglo XXI. Esta agencia patrocina docenas de proyectos para aumentar la resistencia de los soldados. Combatientes capaces de no dormir durante horas, que puedan nutrirse con alimentos impensables y con un desarrollo celular que aumente su fuerza. (Cohnen, 2010, p. 20)

Capítulo IV
La ciberguerra y sus cuatro teatros operacionales

La ciberguerra desde una perspectiva teórico-conceptual

A partir de la posguerra fría, se plantea una nueva tipología de batalla que se caracteriza por el empleo de las computadoras y la comunicación en red (que integra a las terminales al sistema mundial) para atacar a un enemigo mediante el empleo de información con fines psicológicos y de desarticulación logística, o por hacer uso de las tecnologías de la información para la organización estratégica, operacional y logística de los diversos componentes y recursos de las fuerzas militares a nivel global (Henry y Peartree, 1998).

Esta nueva forma de enfrentamiento solo requiere una computadora conectada a internet y un objetivo. En ese sentido, se aleja de la concepción moderna de la guerra tradicional. En la ciberguerra no es fundamental ni el tiempo, ni el espacio, ni el clima, ni el arsenal, ni el número de tropas, ni la movilización, ni las pérdidas de vidas humanas (Sampaio, 2001). Se requiere, como conclusión de los capítulos precedentes, el ciberespacio como dimensión para la ciberguerra, infraestructuras críticas como objetivos militares, computadoras y redes informáticas para crear y lanzar armas informáticas y cibernéticas, y

cibersoldados para que lleven a cabo las operaciones y tácticas que demanda la ciberguerra. El factor central de la ciberguerra radica en encontrar brechas de seguridad para afectar las redes y los dispositivos informáticos de otros Estados. Los ataques cibernéticos capitalizan las debilidades que tiene el sistema informático para extraer información estratégica o boicotear procesos vitales para la nación.

El uso masivo de las tecnologías informáticas y de las redes de comunicación ha cambiado la forma en que operan los Estados. Por esto, los gobiernos, mediante una compleja red de computadoras, administran los sistemas de tránsito vehicular y aéreo, los sistemas de defensa militar y, en general, toda la infraestructura crítica de la nación (Geers, 2009).

Si bien a estas alturas es claro que se hace un estudio del conflicto en el ciberespacio, es importante estudiar el nacimiento del prefijo *ciber,* raíz de la palabra cibernética. Desarrollada en la próspera era de investigación que siguió a la Segunda Guerra Mundial, la cibernética fue definida como el estudio teórico de los procesos de comunicación y de control en sistemas biológicos, mecánicos y artificiales. Su nombre proviene de la voz griega *kybernetes*, traducida como timonel o gobierno, con lo que la comunicación es asociada con las nociones de control, regulación y dominio (Siles, 2007, p. 88).

La cibernética fue definida como la ciencia del control y la comunicación entre el animal y la máquina, en una palabra, como el arte de la dirección (Velandia, 2006). Consiste en considerar las estructura y el funcionamiento de los seres vivos como sistemas complejos, basándose en los conceptos de la teoría de la información y las neurociencias computacionales. Considera también cómo se llevan a cabo los procesos de comunicación, los mecanismos de control y los conceptos de retroalimentación en los seres vivos y en las máquinas (Jiménez, 2008, p. 53).

> La cibernética es la ciencia que estudia los principios abstractos de organización en los sistemas complejos. No se trata tanto de en qué consisten los sistemas, sino de cómo funcionan. La cibernética se centra en cómo los sistemas utilizan la información, los modelos y las acciones de control para orientar y mantener sus objetivos, al tiempo que contrarrestan diversas perturbaciones. Siendo

> intrínsecamente transdisciplinario, el razonamiento cibernético puede aplicarse para comprender, modelar y diseñar sistemas de cualquier tipo: físicos, tecnológicos, biológicos, ecológicos, psicológicos, sociales o cualquier combinación de ellos. La cibernética de segundo orden en particular estudia el papel del observador (humano) en la construcción de modelos de sistemas y otros observadores[34]. (Heylighen y Joslyn, 2001, p. 1)

La cibernética estudia los flujos de información que rodean un sistema y la forma en que esta información es usada por este como un valor que le permite controlarse a sí mismo. Entonces, la información es para la teoría cibernética un elemento fundamental para la organización del sistema. El concepto de información utilizado por la cibernética tiene su origen en la teoría comunicativa de Shannon y Weaver, que trataba de la transmisión de mensajes, y actualmente está integrada en la teoría de la comunicación. Esta noción de información está basada en la medida de la información a través de unidades elementales de información o bits, muy utilizados en la actualidad en la informática y las telecomunicaciones. A esta dimensión de la información, la cibernética le añade un sentido organizacional. De hecho, un "programa" portador de información lo que hace es comunicar un mensaje a una máquina que computa un cierto número de operaciones (Gros, 2001).

Cualquier ser, biológico, artificial o mecánico, puede ser definido respecto del tipo de intercambios de información que sostenga con su entorno: todos son entes basados en la información. Ante esto, surge la cibernética, con el fin de entender estos comportamientos de intercambio, expresión que terminó entendiéndose como comunicación, concebida como un comportamiento de información, en perpetua reacción con su ambiente (Siles, 2007, p. 89). Wiener afirma que,

> al dar la definición de cibernética en la primera edición, puse en la misma categoría las comunicaciones y el gobierno de las máquinas. ¿Por qué lo hice? Cuando me pongo en contacto con otra persona, le doy un mensaje; cuando responde, me da algo en relación con

34 Traducción del autor.

> lo que dije que contiene informes accesibles a él primordialmente y no a mí. Cuando regulo los actos de otra persona, le comunico un mensaje; aunque esté en modo imperativo, la técnica de la comunicación no difiere de la del que enuncia hechos. Además, si mi regulación ha de ser efectiva, debo tomar conocimiento de cualquier mensaje de él que indique haber comprendido y obedecido la orden. (citado por Castro y Filippi, 2010, p. 160)

Durante la Segunda Guerra Mundial, a Wiener se le encomendó la creación de mecanismos de control para la artillería antiaérea que tuvieran la capacidad de regular su propia trayectoria. Este diseño le condujo al estudio del proceso de regulación de los organismos vivos y lo que Wiener hizo fue extraer los datos que sobre biología se poseían y aplicarlos al diseño de la máquina. Es este un dato muy relevante, pues la comparación funcional entre la mente y la máquina que posteriormente incorporó la psicología cognitiva y la inteligencia artificial encuentran aquí sus orígenes. Pero también es importante porque hasta aquel momento no había habido ninguna relación entre los estudios biológicos y el diseño de máquinas, aspecto presente en la actualidad tanto en el diseño del *hardware* como del *software* (Gros, 2001).

> Mientras que las perturbaciones resistidas en una relación de control pueden originarse dentro o fuera del sistema, funcionalmente podemos tratarlo como si todo él proviniera de la misma fuente externa. Para lograr su objetivo, a pesar de tales perturbaciones, el sistema debe tener una forma de controlar su efecto sobre sus variables esenciales[35]. (Heylighen y Joslyn, 2001, p. 13-14)

Los componentes estructurales de la teoría de control son las tareas, el esquema de actividad, las condiciones, los tipos, los sujetos, los métodos, las formas, los medios, las funciones, los factores que influyen en la eficacia, los principios y los mecanismos de control (Novikov, 2016, p. 35). El control que se ejerce a través de la cibernética tiene ciertos principios esenciales: jerarquía, unificación, decisión, franqueza, eficiencia, responsabilidad, no interferencia, participación y control

35 Traducción del autor.

social y estatal, desarrollo, adaptación, coordinación, ética y descentralización, entre otros (p. 45).

La palabra *cibernética* se utiliza, en primer lugar, asociada al uso de la tecnología informática y, posteriormente, al uso de las redes de comunicación. Esta masividad, sumada a una ausencia de alfabetización tecnológica, ha desatado una degeneración del término. Sin embargo, en este uso más masivo, el propio término se ve mutilado (Gros, 2009, p. 2).

En los últimos quince años, una tendencia moderna en la teoría del control ha buscado dirigirse hacia la "miniaturización", "descentralización" e "intelectualización" en sistemas con muchos agentes autónomos interactivos de naturaleza social, técnica o informacional. Las propiedades inherentes de los sistemas multiagentes (*multi-agent systems* [MAS]) como la interacción descentralizada y la multiplicidad inducen, fundamentalmente, a nuevas propiedades emergentes (autonomía, menor vulnerabilidad a factores desfavorables, etc.) cruciales en varias aplicaciones.

Los MAS se pueden dividir en *hardware* (publicaciones pioneras que se remontan a mediados de la década de 1990) y *software* (desde mediados de la década de 1970). Los primeros incluyen robots móviles (robots con ruedas, vehículos aéreos no tripulados, submarinos autónomos no tripulados, etc.) y sistemas de control de complejos objetos industriales y tecnológicos (sistemas de control asistido por ordenador de procesos industriales). Los últimos incluyen sistemas de control en los que los agentes son *softbots,* es decir, módulos programados autónomos que resuelven problemas de optimización distribuidos según protocolos establecidos (posibles aplicaciones de sistemas logísticos en fabricación y transporte, *softbots* en redes digitales, esto es, programación en tiempo real, asignación de funciones y tareas, y así sucesivamente) (Novikov, 2016, p. 70).

Realizar una arqueología del prefijo *ciber*, teniendo en cuenta su popularidad, es explorar un mundo de teorías y presencias, que ha permitido comprender y problematizar los debates en la concepción misma de la tecnología, la cultura, el tiempo y el espacio, como construcción de realidades y subjetividades. Su uso advierte la emergencia de una cultura ligada a los desarrollos de la cibernética, las nuevas

comprensiones de la biología, la tecnología, la sociología y los usos culturales de la tecnología en la sociedad del conocimiento, pero plantea grandes retos relacionados con la investigación y la construcción de conocimiento transdisciplinar (Téllez, 2016, p. 145).

Si se tiene en cuenta lo anterior, y volviendo al enfoque de la guerra, la ciberguerra se puede definir como "la lucha entre dos Estados o facciones que tiene lugar en el espacio cibernético" (Ortega, 2012, p. 47). También se afirma que es "un ataque digital masivamente coordinado hacia un gobierno por otro, o por grandes grupos de ciudadanos. Es la acción de un Estado nación de penetrar en las computadoras y redes de otra nación con el propósito de causar daño o interrupción"[36] (Schreier, 2015, p. 16). Se puede entender como la guerra basada en ciertos usos de las tecnologías de la información y de la comunicación (TIC) dentro de una estrategia militar ofensiva o defensiva respaldada por un Estado que apunta a la interrupción o el control inmediato de los recursos del enemigo que se libra dentro del entorno informativo, sobre los dominios físicos y no físicos, cuyo nivel de violencia puede variar según las circunstancias (Taddeo, 2012b, p. 114).

La guerra cibernética tiene algunas diferencias claras con la guerra tradicional, pues no es necesariamente un fenómeno de violencia y destrucción extrema; es decir, "puede involucrar a un virus informático capaz de interrumpir o negar el acceso a la base de datos del enemigo y, al hacerlo, causar un daño grave al enemigo sin ejercer fuerza física ni violencia"[37] (Taddeo, 2012a, p. 211). De igual forma, puede no implicar a los seres humanos, lo cual se refiere a que, si bien el hombre puede llevar a cabo la orden, se puede dirigir a través de agentes artificiales, bases de datos o sitios web. Lo anterior no implica que la ciberguerra no deba ser temida tanto como la guerra convencional. Este fenómeno tiene una característica que es casi imposible de identificar en los demás escenarios; para Taddeo, es transversal, puede llegar a escalar de formas no violentas a formas muy violentas.

36 Traducción del autor.

37 Traducción del autor.

Durante la guerra del Golfo Pérsico, las fuerzas militares estadounidenses vieron potenciado el desarrollo de sus operaciones y tácticas en el teatro de guerra y operaciones al incluir en su funcionamiento una colosal estructura de tecnologías informáticas, para llevar a un nuevo nivel el comando, el control y las comunicaciones, así como el envío de datos estratégicos al terreno, el desarrollo de operaciones psicológicas, el empleo de armamento inteligente y sofisticadas aeronaves imperceptibles para el enemigo. En síntesis, la información fue una materia prima para llegar a la victoria de manera menos compleja y sorteando muchas dificultades que ocurrían en escenarios precedentes de conflagración (Wilson, 2007).

En la ciberguerra, la información ya no es simplemente una plataforma para llevar a cabo las acciones de guerra de manera más eficiente y eficaz sobre el terreno. La información se ha convertido en el medio y el fin para hacer las acciones de guerra sin ni siquiera estar en el campo de batalla (Dunn, 2010). Bajo esta doctrina, la información se considera como "la artillería" que viaja a través del ciberespacio hacia su objetivo, que es disparada o desplegada por el armamento cibernético, es decir, las computadoras, y los expertos en su uso (Wander, 2003).

Retomando que, según la lógica del ciberespacio, la infraestructura crítica del Estado, la estructura gubernamental y los sistemas de seguridad y defensa se han integrado a esta dimensión como producto de su sinergia con las tecnologías informáticas, la ciberguerra busca el control de estas instancias. Y como en esta dimensión virtual las variables tiempo y espacio se han reconfigurado, los pilares del Estado nación están al alcance del enemigo tanto como este lo esté de una computadora (Bhattacharjee, 2009).

Si consecutivamente al establecimiento conceptual de la *blitzkrieg*, o guerra relámpago, se prosiguiera con una nueva categoría para entender lo que la ciberguerra representa, sería ahora pertinente entrar a operar con el concepto de la *leitenkrieg*, o *guerra de control* (Arquilla y Ronfeldt, 1993).

Con la ciberguerra, se busca que las hidroeléctricas abran sus compuertas sin aviso para inundar poblaciones aledañas, que reactores nucleares se recalienten y entren en crisis (o que dejen de funcionar), que oleoductos y refinerías ardan en llamas, que los sistemas bancarios y

financieros nacionales sufran desplomes informáticos (que después se reflejan en desplomes reales de la economía), que los controladores aéreos no puedan guiar el tráfico aéreo o que el Gobierno quede incapacitado para prestar servicios y generar vínculos de comunicación de manera efectiva con los ciudadanos (Verising, 2009).

Al afirmar que la ciberguerra se traduce en una *guerra de control,* la guerra cibernética se puede explicar como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para tratar de imponerle la aceptación de un objetivo propio o, simplemente, para sustraerle información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente se ha entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física, sino un ataque informático que le permita obtener una ventaja sobre el enemigo para situarse en superioridad o, incluso, derrocarlo (Wilson, 2007).

Según Shea, se logra precisar el concepto donde se une la guerra en el ciberespacio y la infraestructura vital de los actores. La infraestructura crítica se define como los sistemas y los activos, físicos o virtuales, que son sumamente vitales para los Estados, que, en caso de ser incapacitados o destruidos, los activos tendrían un impacto debilitante en la seguridad, la seguridad económica nacional, la salud o la seguridad pública, o cualquier combinación de estos asuntos (2003, p. 1). El nexo con este escenario de amenaza, en distintos países industrializados, se consolida mediante la inclusión de *sistemas informáticos de control industrial* para formalizar las operaciones de la infraestructura crítica estatal. Tal es el caso de la implementación del Supervisory Control and Data Acquisition (SCADA).

Desde la perspectiva cibernética, SCADA ofrece uno de los objetivos más atractivos para los detractores de la seguridad con miras a alcanzar un evento catastrófico. Con el crecimiento exponencial de las redes de sistemas de información que interconectan el sector productivo, administrativo y de sistemas operativos, la agresión se materializa mediante la intrusión al SCADA a fin de modificar los datos utilizados para la toma de decisiones operativas, los programas que controlan los equipos de industria crítica, o los datos comunicados a los centros de control (Foster *et al.*, 2008).

Durante la primera década del siglo xxi, han existido alrededor del mundo acontecimientos que pueden nombrarse ciberguerra. Se encuentra presente la operación con nombre código Titan Rain, en la cual, durante 2002, un grupo gubernamental de *hackers* chinos entrenados en el ciberespionaje lograron descargar aproximadamente entre 10 y 20 terabytes de información sensible (pero no confidencial) del Departamento de Defensa de los Estados Unidos (United States Department of Defense [DoD]) a través del Non-Secure Internet Protocol Router NETwork (NIPRNET) y, específicamente, del U.S. Army Information System Engineering Command, del Naval Ocean Systems Center, y de la Missile Defense Agency (Carr, 2011).

A manera de conclusión, dando crédito a los casos acaecidos en los cuales los Estados nación han efectuado ataques en el marco de la lógica de la ciberguerra, es posible evidenciar el nuevo valor que toma la información. Durante la década de 1990, la informática fue una materia prima para desarrollar la guerra en su respectivo teatro. Ahora, con la cibernética, como arte del control, la información es un arma para causar un efecto esperado en los sistemas informáticos del enemigo.

Por supuesto que esta nueva forma de combate toma importancia cuando las computadoras y las maniobras u operaciones, que por medio de estos se adelantan, se traducen en un ataque directo a los cimientos de un Estado nación considerado como enemigo desde la perspectiva del agresor. No en vano, la ciberguerra, con bajos riesgos para los cibersoldados, puede ser vista por los niveles decisorios de la guerra como una forma de establecer un objetivo, pero sin disparar una sola arma. Un atacante podría pensar en una ciberofensiva que inhabilite la red de energía eléctrica y además destruya algunos de los componentes principales del sistema informático de ella (el sistema queda inservible por semanas), un movimiento poco antiséptico, un camino para tener las tensiones en sus niveles más bajos posibles. Pero, para millones de personas entrar en un escenario de oscuridad y tal vez de frío, imposibilitados para conseguir alimentos, sin acceso al dinero ni posibilidad de intercambio producto del desorden social, podría ser, en muchas formas, lo mismo que haber lanzado una bomba sobre una ciudad (Clarke, 2009).

Se logró constatar que en el nuevo escenario los ejércitos encontraron una tecnología para ser aplicada en los elementos bélicos, a fin de potenciar los medios y las capacidades de la comunicación. Como se evidenció, mediante el empleo de aeronaves dotadas de todo tipo de dispositivos informáticos, y con los misiles que, al estar integrados con sistemas a base de silicio, se hicieron con la capacidad de la teledirección y precisión en el impacto de blancos (Arquilla y Ronfeldt, 1993).

El teatro psicológico: juego con la información

Irak, en 1990, se convirtió en un teatro de guerra experimental para las TIC. El despliegue de computadoras integradas a sistemas de comunicación en red sobre el teatro de guerra evidenció que se daba paso a un nuevo tipo de guerra, así como a la forma en que se debían conducir las operaciones y establecer su doctrina. Estas transformaciones, que se enmarcaron teóricamente en el enfoque de la revolución de los asuntos militares, dieron paso a las denominadas *information war* e *information warfare* (Glebocki, 2008).

Dentro de este marco, igualmente se detectó la aparición de las denominadas operaciones de información (OI), sustentadas por el empleo de las computadoras y su capacidad de enviar la información por internet y caracterizadas por la utilización de herramientas informáticas que permiten la parálisis, el control o la destrucción de la información y los sistemas del enemigo.

Estas herramientas son reconocidas por tener como objetivo efectos psicológicos en el oponente al desarticular sus canales de comunicación, en los que recae la decisiva toma de decisiones entre el alto Gobierno y el Estado Mayor de las fuerzas militares (verticalmente), y el mando, el control y las unidades desplegadas en los teatros de operaciones (horizontales) (Wilson, 2007).

Al funcionar el mundo bajo un sistema informático global, todo aquello que es considerado como centro de gravedad de un Estado se encuentra bajo amenaza. Por ende, todo actor con un conocimiento en cibernética, y acceso a una computadora, que se encuentre conectado

a internet, tiene la posibilidad de acceder a las redes neurálgicas de una nación, ya sea con intenciones hostiles, ya sea con el objeto de espiar información gubernamental en todos sus ámbitos (Warden, 1995).

> Las campañas de propaganda y desinformación han sido, durante mucho tiempo, elementos básicos de la guerra convencional. En la batalla por los corazones y las mentes, el control de las tecnologías de radiodifusión (televisión, radio) ha sido un objetivo fundamental. En un sentido, nada ha cambiado mucho, pero el panorama se ha vuelto más complicado con la aparición de internet y la World Wide Web, que dan voz a los individuos y grupos más inverosímiles, sus propiedades de comunicación multidireccional dan acceso a audiencias que, bajo las condiciones del monopolio de radiodifusión oligopolísticas, habrían permanecido fuera de su alcance. En la era de la información, el enemigo silencioso puede adquirir fácilmente una voz y amplificar rápidamente su mensaje disidente. Los canales unidireccionales están siendo desplazados por patrones de comunicación, lo que hace que el deseo de controlar y censurar sea casi inútil[38]. (Cronin y Crawford, 1999, p. 258)

A pesar de las diferencias entre los usos de las TIC en la guerra, existe un aspecto que es común a todas las circunstancias, y es el despliegue de estas con una intención disruptiva inmediata, como el uso de armas (semi) autónomas, alguna infraestructura de información o el despliegue de dispositivos digitales para mejorar el desempeño de las fuerzas en el campo de batalla. Este factor común es el primer paso hacia la definición de este nuevo tipo de guerra. La guerra de información es el uso de las TIC con un propósito ofensivo o defensivo para entrometerse, interrumpir o controlar inmediatamente los recursos del oponente (Taddeo, 2012b, p. 109).

La *information warfare* (IW) fue lanzada formalmente en diciembre de 1992 con la difusión de la Directiva 3600 del DOD. En septiembre de 1995, el subsecretario de Defensa para el Comando, Control, Comunicaciones e Inteligencia (Assistant Secretary of Defense

38 Traducción del autor.

(Command, Control, Communications, & Intelligence) [ASD(C3I)]) publicó la definición oficial no clasificada del DoD de IW: medidas adoptadas para lograr la superioridad de la información al afectar la información adversa, los procesos basados en la información y los sistemas de información, al tiempo que se defiende la propia información, los procesos basados en información y los sistemas de información (Fredericks, 1997, p. 80).

Adams (2001) define la guerra de la información como la secuencia de las acciones emprendidas por todas las partes en un conflicto de destruir, degradar y explotar los sistemas de información de sus adversarios. Y también comprende todas las acciones encaminadas a proteger los sistemas de información contra los intentos hostiles a la destrucción, degradación y explotación. Las acciones de guerra de información tienen lugar en todos los lugares de la evolución del conflicto: la paz, la crisis, la escalada, la guerra, la distensión y los posteriores a los conflictos (Delibasis, 2007, p. 6).

La guerra de información es un tipo de guerra electrónica que tiene como objetivo neutralizar y obtener información o monitorear sistemas y redes de información de computadoras enemigas. Además, la capacidad de este tipo de guerra, en un papel defensivo, debe proporcionar una protección adecuada a los sistemas y las redes propios. El DoD *Dictionary of Military and Associated Terms* la define como las operaciones de información llevadas a cabo durante tiempos de crisis o conflicto para lograr o promover objetivos específicos sobre un adversario o adversarios específicos. Es más que el ataque y la defensa de la red informática, más eficaz cuando se realiza de forma sincronizada y coherente, por lo que la gestión del conocimiento lo complementa bien. Todos los componentes de una organización, así como en toda la empresa, deben ser incluidos en un plan de acción. El propósito de la guerra de información es controlar o influir en las acciones del tomador de decisiones. Un área de control puede manipularse directamente, mientras que un área de influencia solo puede manipularse indirectamente. El control y la influencia son la esencia del poder (Khan, 2013, p. 142).

De acuerdo con Cronin y Crawford (1999), la guerra de información es la penetración silenciosa de los sistemas de información y

comunicaciones del objetivo para manejar las percepciones, dar forma a las opiniones, fomentar el engaño y participar en la guerra epistemológica (p. 258). La guerra de influencia y manipulación de la información (*information/influence warfare and manipulation* [IIWAM]) es el uso deliberado de información por una parte de un adversario para confundir, engañar y, en última instancia, influir en las decisiones que hace el adversario. La IIWAM es una actividad no cinética hostil (Lin y Kerr, 2017).

La guerra informática es, en pocas palabras, un subconjunto de operaciones de información que puede definirse como las acciones que se realizan con el fin de alterar la información y los sistemas de información del adversario, mientras se protege la información y los sistemas de información propios. Tales operaciones abarcan, prácticamente, toda medida cuyo objetivo sea descubrir, alterar, destruir, interrumpir o transferir datos almacenados, procesados o transmitidos por una computadora. Pueden efectuarse en tiempo de paz, durante una crisis o en las etapas estratégica, operativa o táctica de un conflicto armado. El logro del propósito mencionado se obtendrá a través de la superioridad informática, ya sea contando con una tecnología superior, ya sea haciendo un empleo más adecuado de las facilidades informáticas propias (López, 2007, p. 219).

El espacio de batalla es el entorno de información, el cual es el agregado de individuos, organizaciones y sistemas que recogen, procesan, difunden o actúan sobre la información. Tiene tres dimensiones interrelacionadas: física, informacional y cognitivo-emocional, en y por medio de las cuales los individuos, las organizaciones y los sistemas interactúan continuamente. El escenario físico está compuesto por los sistemas de mando y control, *software*, tomadores de decisiones clave y la infraestructura. La dimensión informacional es específicamente donde la información es recolectada, procesada, almacenada, diseminada y protegida. Por último, la dimensión cognitivo-emocional comprende las mentes y emociones de aquellos que transmiten, reciben, responden o actúan respecto de la información (Lin y Kerr, 2017).

Las operaciones de este tipo de guerra usualmente aprovechan los sesgos cognitivos en los seres humanos. Estos sesgos resultan del uso humano de estrategias de razonamiento intuitivo en lugar de estrategias

analíticas. Una de las estrategias de razonamiento intuitivas más importantes son las heurísticas, que sustituyen los juicios simples por tareas inferenciales complejas, lo que da lugar a sesgos cognitivos que a veces conducen a conclusiones erróneas. Los sesgos cognitivos sugieren cómo los juicios y las conclusiones de los seres humanos reales pueden diferir de los de una hipotética persona absolutamente racional debido a la dependencia de la heurística mental falible. Pero los factores emocionales también afectan los juicios y las conclusiones que la gente hace. Los sesgos emocionales se pueden ver cuando un individuo tiene una motivación para creer en una respuesta o un resultado particular o una visión que le impide alcanzar los beneficios de la consideración racional (Lin y Kerr, 2017).

Una meta de la guerra de información puede ser la penetración silenciosa del sistema de información y comunicaciones del objetivo para dar forma a las percepciones de la comunidad, fomentar el engaño o la incertidumbre (Cronin y Crawford, 1999, p. 258). La guerra de la información busca evitar la necesidad de recurrir a la fuerza letal poniendo enemigos en posiciones en las que sus recursos de información son inútiles o, peor, poco fiables. En este sentido, aspira a realizar el famoso dicho de Sun Tzu que afirma que someter al enemigo sin luchar es el punto álgido de habilidad (Miller, 1997, p. 158).

La opción de emprender una guerra (clásica) suele implicar un compromiso sustancial, ya que tiene fuertes costos económicos y políticos, sobre todo para la sociedad civil. Estas características de la guerra han sido radicalmente cambiadas por el advenimiento de la guerra de información, que proporciona los medios para llevar a cabo la guerra de una manera completamente diferente. En este escenario, los cambios determinados son de una importancia asombrosa, ya que se refieren tanto a la forma en que los militares y los políticos consideran la guerra y la forma en que se percibe esta en la sociedad civil. Al igual que la guerra tradicional, la guerra de información es muy potente y potencialmente perturbadora. Sin embargo, a diferencia de la guerra tradicional, reduce a la mínima expresión el derramamiento de sangre, es rentable y no es un fenómeno específicamente militar (Taddeo, 2012b, p. 112).

Las operaciones se caracterizarán por la superioridad en la obtención de información en cantidad y calidad, lo que generará un mayor

poder de combate al enlazar a los sensores, los comandantes y los sistemas de armas para lograr una apreciación compartida de la situación, mayor capacidad de mando, un ritmo de operaciones más elevado, mayor letalidad y mayor supervivencia. Además, resulta necesario evaluar los conocimientos y los factores psicológicos como componentes de la relación de fuerzas (López, 2007, p. 220).

Se puede hablar de tres clases de guerra de información. La primera clase describe ataques contra la privacidad electrónica de un individuo. Esto incluye la divulgación de registros digitales y entradas de bases de datos dondequiera que se almacene la información. La persona promedio hoy en día tiene poco control sobre la información almacenada. La segunda clase describe la competencia, mejor dicho, la guerra de hoy entre las corporaciones alrededor del mundo y el robo de información con fines económicos; no es solo acerca de la adquisición de información, también es posible difundir información, real o ficticia. Y la guerra informática global trabaja contra industrias, fuerzas económicas globales o contra países o Estados enteros. No se enfoca mucho en los datos de investigación de un competidor, sino en el robo de secretos y luego en convertir esta información en contra de sus propietarios (Haeni, 1997).

Cuatro procesos interrelacionados apoyan las operaciones de información defensiva: la protección del ambiente de la información, la detección del ataque, la restauración de la capacidad y la respuesta del ataque. Se llevan a cabo en toda la gama de operaciones militares en todos los niveles de la guerra para lograr los objetivos de la misión. Las operaciones ofensivas de información podrían incluir la recopilación activa de información sobre sistemas de información, intrusiones no autorizadas en sistemas de información, introducción de vulnerabilidades en sistemas informáticos, corrupción o negación de datos e inhabilitación o destrucción de sistemas de información (Joyner y Lotrionte, 2001, p. 835).

Empleada ofensivamente, la guerra de información resalta la manipulación de los sistemas electrónicos de información para influir en las percepciones y el comportamiento de un adversario. Esto podría, por ejemplo, implicar la inhabilitación de sistemas militares y civiles de telecomunicaciones a través de virus informáticos. Defensivamente,

la guerra de información requiere una capacidad para detectar y frustrar los intentos de manipular las propias fuentes de información. En el ámbito militar, esto implica asegurar la integridad de los sistemas de mando y control, comunicaciones e inteligencia. También deben protegerse los elementos críticos de la infraestructura civil, como las redes eléctricas, las redes financieras y los sistemas de telecomunicaciones. Además, también postula una capacidad para contrarrestar la propaganda y la desinformación enemigas (Miller, 1997, p. 158).

Se puede clasificar en seis subáreas preexistentes que recientemente se han agrupado bajo el título de guerra de información: seguridad operativa, guerra electrónica (*electronic warfare* [EW]), operaciones psicológicas (*psychological operations* [PSYOP]), engaño, ataques físicos a procesos de información y ataques a procesos de información. Por tanto, la guerra de información ofensiva consiste en la unión de las seis anteriores (Nichiporuk, 1999, p. 180).

La guerra electrónica abarca los conceptos tradicionales de interferencia y falsificación de radares y enlaces de comunicación de radio. Las PSYOP son sobre todo el uso de la diseminación de información para debilitar la moral del enemigo y, en última instancia, para romper su voluntad de resistir. El engaño implica el empleo de medios físicos o electrónicos para camuflar la propia postura de la fuerza en el teatro. El ataque físico es el acto de dañar físicamente o destruir los medios de un adversario de recopilar, procesar y organizar la información. Por último, el ataque informativo implica el uso de tecnología informática para cerrar electrónicamente, degradar, corromper o destruir los sistemas de información de un enemigo en el teatro (Nichiporuk, 1999, p. 181).

Se está desarrollando un fenómeno cibernético en evolución: el concepto de operaciones cibernéticas psicológicas (*cyber psychological operations* [CYOP, pronunciado "PSYOP"]), que son aquellas que atacan e influyen directamente en las actitudes y los comportamientos de soldados y la población en general. Mientras los ejércitos continúan compitiendo en el espacio de batalla digital, las poblaciones locales están ahora atrapadas en batallas espaciales de influencia digital. Las CYOP también están inundadas de consecuencias no deseadas, ya que se ha empezado a entender qué grado de influencia, persuasión, engaño y movilización ofrece el entorno cibernético (Thomas, 2007, p. 30).

Las CYOP se caracterizan por su velocidad, precisión y creatividad. La velocidad se reconoce debido a la rapidez del mecanismo de respuesta de mensajes. Un incidente ocurre y se informa en internet, o por teléfono celular o mensajería de video, antes de que los servicios legítimos de noticias puedan adjudicar su autenticidad. En particular, estos mensajes tienen un alcance infinito, aunque preciso. Se puede dirigir a soldados o enemigos y poblaciones con igual facilidad. Además, la creatividad es un tema emergente. Las tecnologías ofrecen la capacidad de actualizar las técnicas PSYOP probadas con tiempo usando nuevas aplicaciones no probadas o probadas (Thomas, 2007, p. 30).

Se han identificado cinco capacidades básicas para la realización de operaciones de información: 1) operaciones psicológicas, 2) engaño militar, 3) seguridad de operaciones, 4) operaciones de redes de computadoras y 5) guerra electrónica. Estas capacidades están diseñadas para influir en los responsables de tomar decisiones en el extranjero y proteger la toma de decisiones, así como para afectar o defender el espectro electromagnético, los sistemas de información y la información que apoya a los tomadores de decisiones, sistemas de armas, mando y control y respuestas automatizadas (Wilson, 2004).

Las PSYOP se definen como operaciones planificadas para transmitir información e indicadores seleccionados a audiencias extranjeras con el fin de influir en sus emociones, motivaciones, razonamiento objetivo y, en última instancia, el comportamiento de gobiernos, organizaciones, grupos e individuos extranjeros. El propósito de las PSYOP es inducir o reforzar actitudes y comportamientos ajenos a los objetivos del originador (Peña, Casas y Mena, 2009). El engaño guía a un enemigo a cometer errores presentando información, imágenes o declaraciones falsas. El engaño militar se define como acciones ejecutadas para engañar deliberadamente a los responsables militares adversarios con respecto a capacidades militares, intenciones y operaciones amistosas, haciendo que el adversario tome acciones específicas (o inacciones) que contribuyan al éxito de la operación militar amistosa (Wilson, 2004).

La seguridad operacional (*security operations* [OPSEC]) se define como un proceso de identificación y análisis de la información que es crítica para las operaciones e incluye 1) identificar qué información

puede ser observada por los sistemas de inteligencia del adversario, 2) determinar indicadores que los sistemas hostiles de inteligencia podrían reunir a fin de obtener información crítica a tiempo para ser útil a los adversarios y 3) seleccionar y ejecutar medidas que eliminen o reduzcan la vulnerabilidad de las acciones a la explotación del adversario (Wilson, 2004).

Las operaciones de red informática están compuestas de tres áreas de misión específicas pero complementarias. Implican la capacidad de atacar e interrumpir las redes informáticas enemigas, proteger los sistemas de información militar y explotar las redes informáticas enemigas a través de la recolección de inteligencia. El ataque a redes de computadoras se define como las operaciones para interrumpir, negar, degradar o destruir la información residente en los ordenadores y redes de ordenadores, o las computadoras y las redes en sí. La defensa de redes de computadoras se define como medidas defensivas para proteger y defender la información, computadoras y redes de interrupción de la negación, degradación o destrucción. La explotación de redes de computadoras involucra el espionaje, que en general se realiza a través de herramientas de red que penetran en los sistemas adversos para devolver información o copias de archivos que, individual o colectivamente, permiten a los militares obtener una ventaja sobre el adversario (Wilson, 2004).

La guerra electrónica se define como cualquier acción militar que involucre la dirección o el control de la energía del espectro electromagnético para engañar o atacar al enemigo. La guerra electrónica ha sido un componente importante de las operaciones aéreas militares desde los primeros días del radar, y los ingenieros y científicos han desarrollado los conceptos para incluir ahora nuevas técnicas de sigilo (Wilson, 2004).

Se han enumerado cinco principios de la guerra de información:

- negación;
- mejora de fuerza;
- conciencia situacional de supervivencia;

- comando, control y comunicaciones;
- nivel (Sulaiman, 2005).

La información sobre la fuerza y debilidad del enemigo y las fuerzas propias es importante para ganar una guerra. La negación de esa información a los comandantes enemigos los pondría en la oscuridad. Por tanto, los centros de mando y control y los sistemas de apoyo a la toma de decisiones y comunicaciones deben ser los objetivos principales y todos los sensores hostiles deben ser suprimidos o destruidos antes de participar en combate (Sulaiman, 2005).

El segundo principio es la mejora de la fuerza. Las tropas sobre el terreno necesitan la información tanto como sus comandantes. El flujo de información de arriba abajo debe ser lo más sutil posible para reducir o evitar riesgos adicionales para las tropas (Sulaiman, 2005).

La descentralización es importante para garantizar la supervivencia. La política y la estrategia deben centralizarse en el nivel superior, pero se debe dar un margen de maniobra al nivel inferior para planificar y ejecutar sus misiones. La interoperabilidad es otro aspecto para asegurar la supervivencia. Todo el sistema de información y comunicación debe ser capaz de hablar entre sí para permitir el máximo intercambio de información (Sulaiman, 2005). El último principio de la guerra de la información es el nivel, según el cual toda la tecnología disponible debe ser usada contra las capacidades materiales e inmateriales del enemigo. La intensidad de los conflictos de la guerra de información debe contener todos los esfuerzos.

La guerra psicológica abarca el uso de información contra la mente humana. Hay cuatro categorías de guerra psicológica: 1) operaciones contra la voluntad nacional, 2) operaciones contra comandantes opuestos, 3) operaciones contra tropas y 4) conflicto cultural (Libicki, 1998, p. 34).

El elemento cibernético permite que las operaciones psicológicas penetren no solo unos cuantos kilómetros en el territorio enemigo, sino que lleguen directa y profundamente a las casas de las poblaciones objetivo. El elemento cibernético lo hace en privado y en silencio, e invade no solo las computadoras y los teléfonos celulares, sino también el bienestar psicológico de la población (Thomas, 2007, p. 30).

En la actualidad, se dispone de una amplia variedad de herramientas de guerra de información, tanto defensiva como ofensivamente, para llevar a cabo ataques de este tipo. Estas armas incluyen:

- Un *sniffer*, ejecutado desde un sitio remoto por un intruso, que permitiría a este recuperar usuarios y contraseñas a medida que atraviesa la red. Se tiene así acceso a información sensible relacionada con la defensa nacional, información corporativa o secretos comerciales.

- Un caballo de Troya, instalado de forma remota, que permite a un extraño controlar la red y causar que funcione mal en el comando.

- Una puerta trampa, utilizada para obtener acceso y control no autorizado de los sistemas de control (Joyner y Lotrionte, 2001, p. 836).

- Un virus, que es un fragmento de código que se copia en un programa más grande y lo modifica. Un virus se ejecuta solo cuando el programa donde fue instalado comienza a ejecutarse. El virus se replica entonces e infecta otros programas a medida que se reproduce.

- Un gusano, que es un programa independiente. Se reproduce copiándose a sí mismo de una computadora a otra, por lo general a través de una red. A diferencia de un virus, no modifica otros programas.

- Una bomba, que es un tipo de caballo de Troya, usado para liberar un virus, un gusano o algún otro ataque al sistema. Es un programa independiente o un pedazo de código que ha sido plantado por un desarrollador del sistema o programador (Haeni, 1997).

Paralelamente, en la medida en que la naturaleza de las tecnologías informáticas se fundamentó en su capacidad de transmitir datos (multimedia) por todo el planeta, que transgrede las barreras espaciotemporales a través de internet, la organización y doctrina de los ejércitos

obtuvo nuevas capacidades para plantearse modelos de doctrina, organización, movilización y operaciones de prolongación planetaria.

El elemento que mayor relevancia denota en este acápite de colofón es el valor que obtuvo la información durante 1990 y 1997. Se hace referencia al hecho de que, aceptando que la información fue uno de los catalizadores del proceso de transformaciones reseñado (el otro factor fue la tecnología), no perdió en ningún sentido su carácter de "complemento" para hacer la guerra.

Aunque mediante las operaciones de la información se plantearon formas de actuar por medio de los ataques informáticos a los sistemas del adversario, precisamente nunca sobrepasaron la lógica de romper el vínculo de este actor con su información y la capacidad de recepción, procesamiento y difusión de esta. Por esto, debe recordarse que su objetivo es llegar a la mente del rival y desmoralizarlo a través de la manipulación de la comunicación. En tal distinción, radica el hecho de que en este capítulo no se aborde aún el estudio de fenómenos como la ciberguerra.

Bajo esta tipología de guerra, que bien podría considerarse como una generación más avanzada de la guerra de la información, aunque también se emplean ataques informáticos, como su nombre lo indica, es un combate de carácter cibernético o de control. Y ya no se busca dejar al enemigo sin la información que le permite actuar doctrinalmente, sino que se atacan los sistemas informáticos de control y funcionamiento.

Se trata de atacar los pivotes de un Estado nación para paralizarlo o destruir parte de este, tan solo empleando computadoras para transmitir la información hasta los sistemas que controlan, por ejemplo, la infraestructura crítica del Estado o hurtar secretos nacionales y así poner en peligro la subsistencia de una sociedad.

En enero de 1998, por ejemplo, las tensiones surgieron entre los Estados Unidos e Irak en relación con los inspectores de armas de la Organización de Naciones Unidas (ONU). Saddam Hussein expulsó a los inspectores de la ONU de Irak, lo que precipitó una crisis y empujó a los Estados Unidos al borde de una nueva acción militar en el golfo Pérsico. El primer lunes de febrero, los analistas del Centro Nacional de Monitoreo de Computadoras de la Fuerza Aérea (NORAD) detectaron una serie inusual de banderas de advertencia rojas en sus pantallas que indicaban intrusiones no autorizadas en por lo menos seis redes

electrónicas en todo el país. Varias decenas de sistemas informáticos en instalaciones militares y de gobierno de los Estados Unidos fueron comprometidos con éxito por intrusos, lo que provocó una respuesta a gran escala del Departamento de Defensa de los Estados Unidos (United States Department of Defense [DoD]), conocida ahora como operación Solar Sunrise. El ataque contra los sistemas informáticos violó sistemas pertenecientes a la Marina y la fuerza aérea, así como a los laboratorios de investigación financiados por el Gobierno federal (Joyner y Lotrionte, 2001, p. 839).

Los sistemas tecnológicos avanzados deberían magnificar los tipos de efectos psicológicos producidos por la campaña aérea de la coalición contra las fuerzas terrestres iraquíes durante la guerra del Golfo Pérsico. La campaña aérea intensificó las deficiencias en la motivación y la moral, ya presentes en las filas iraquíes antes del estallido de las hostilidades, por 1) convencer a los oficiales iraquíes y alistados de la supremacía aérea de la coalición, 2) probar la insuficiencia de la defensa aérea iraquí, 3) confirmar la inevitabilidad de la derrota iraquí, 4) intensificar las penurias de las tropas iraquíes y 5) aumentar los temores de los soldados iraquíes sobre su supervivencia personal y la seguridad de sus familias en el país (Hosmer, 1999, p. 234).

Durante la Operación Libertad Iraquí (Operation Iraqi Freedom [OIF]), se dejaron caer panfletos que llevaban el mensaje oficial: "Cualquier guerra no es contra el pueblo iraquí, es para desarmar a Hussein y poner fin a su Gobierno". Mensajes de difusión similares fueron enviados desde el Air Force EC-130E, y de los buques de la Marina que operan en el golfo Pérsico. Las fuerzas estadounidenses también enviaron una avalancha de correos electrónicos, faxes y llamadas telefónicas a numerosos líderes iraquíes que los alentaban a abandonar el apoyo a Saddam Hussein (Wilson, 2004).

En un ataque a los estadounidenses, los agresores accedieron a los sistemas de logística, administración y contabilidad clasificados que controlaban la capacidad de los Estados Unidos de manejar y desplegar sus fuerzas militares. Obtuvieron acceso privilegiado a las computadoras mediante el uso de herramientas disponibles en un sitio web de una universidad e instalaron programas *sniffer* para recopilar contraseñas del usuario. Además, crearon una puerta trasera para volver a

entrar en el sistema en cualquier momento y luego utilizaron un parche disponible en un sitio web de la universidad para cerrar la vulnerabilidad (Joyner y Lotrionte, 2001, p. 840).

En octubre de 1999, Mitchael A. Vatis, director del Centro Nacional de Protección de Infraestructuras (National Infrastructure Protection Centre [NIPC]) del Federal Bureau of Investigation (FBI), testificó ante un subcomité del Senado la primera confirmación pública sobre la investigación del FBI realizada durante todo un año, llamada Moonlight Maze. Esta reveló el ataque de computadora más extenso dirigido al Gobierno de los Estados Unidos. Según los informes, los piratas informáticos que trabajan desde Rusia penetraron en las computadoras del DOD durante más de un año y robaron grandes cantidades de información confidencial. Los expertos en seguridad descubrieron por primera vez las insinuaciones en enero de 1999 cuando los investigadores de la fuerza aérea y del departamento de crimen informático del Ejército rastrearon los ataques a un proveedor de servicios de internet en Rusia. Según los funcionarios del Pentágono y del FBI, la piratería fue una campaña de inteligencia rusa patrocinada por el Estado para descubrir la tecnología estadounidense, no solo apuntando al DOD, sino también al Departamento de Energía (United States Department of the Energy [DOE]), a la Administración Nacional para la Aeronáutica y el Espacio (National Aeronautics and Space Administration [NASA]), y a contratistas y universidades militares vinculadas (Joyner y Lotrionte, 2001, p. 840).

Experimentos con el uso de la guerra de información ocurrieron durante la crisis de Kosovo. El 30 de marzo de 1999, tres días después de que la Organización del Tratado del Atlántico Norte (OTAN) comenzara sus misiones de bombardeo sobre Serbia y Kosovo, los *hackers* iniciaron un programa coordinado para interrumpir el sistema de comunicaciones por correo electrónico de la OTAN al sobrecargarlo. Aunque las identidades de los *hackers* no fueron determinadas, las autoridades occidentales sospechan que eran miembros de la Crna Ruka que atacaron el sitio web de información de Kosovo en octubre de 1998 (Joyner y Lotrionte, 2001, p. 842).

> Grupos como Al Qaeda e Hizbulá han desarrollado CYOP de su propio género. Estos grupos tratan de cambiar actitudes y

> comportamientos a través de la intimidación, el temor cibernético o el odio racial o religioso. Por supuesto, su CYOP no solo está dirigido hacia afuera, sino también al interior de su población. A menudo, se dirige a los descontentos en el Medio Oriente, tratando de reclutar a aquellos que se sienten privados de sus derechos. Las fuerzas de la coalición no han realizado suficientes esfuerzos para neutralizar estas actividades terroristas/insurgentes en Irak y Afganistán como cabría de esperarse. La doctrina de operaciones informáticas de los Estados Unidos es débil (de hecho, casi inexistente) en la cuestión de la contrapropaganda, lo cual se refleja en las operaciones de la coalición[39]. (Thomas, 2007, p. 32)

El líder del clan somalí Mohamed Fará Aidid parece ser un maestro de los usos de la guerra psicológica. En un enfrentamiento que costó la vida de diecinueve soldados estadounidenses, el lado de Aidid perdió quince veces ese número, aproximadamente un tercio de su fuerza. Las fotografías de los somalíes arrastrando cadáveres de soldados estadounidenses por las calles de Mogadiscio transmitidas por CNN en los Estados Unidos terminaron convenciendo a las audiencias de televisión en ese país que no debían permanecer en Somalia. Las fuerzas estadounidenses se fueron, y Aidid, en esencia, ganó la guerra de la información (Libicki, 1995, p. 35).

Durante la revolución egipcia de 2011, las fuerzas gubernamentales del presidente Hosni Mubarak apagaron internet en lo que pudo verse como un intento de control cibernético total. Como la herramienta más fuerte de los revolucionarios estaba en el ciberespacio, el objetivo del Gobierno era evitar que los manifestantes en la plaza Tahrir y otros sitios alrededor de Egipto se comunicaran con las audiencias locales, regionales y globales, lo que influyó en su decisión de actuar. En la noche del 27 al 28 de enero, en lo que el Gobierno consideró claramente un escenario casi perfecto, las cuatro principales líneas de comunicación en el país eran controladas por el Gobierno y las fuerzas del régimen ordenaron a los proveedores de servicios de internet cerrar toda conectividad (Crowell, 2017, p. 20).

39 Traducción del autor.

La oposición egipcia disputó con éxito el control cibernético gubernamental. En lo que se puede considerar como una maniobra para lograr objetivos, la oposición egipcia utilizó hábilmente la conectividad selectiva para mover contenido y disputar el control cibernético gubernamental. El uso de la conectividad técnica humana y limitada a través de teléfonos (tanto celulares como fijos) y las redes sociales ayudaron a la oposición egipcia a superar las fuerzas gubernamentales. Las llamadas telefónicas se hicieron al país para averiguar lo que estaba sucediendo, estas fueron grabadas y el contenido fue traducido para luego ser publicado en distintos medios de comunicación social (Crowell, 2017, p. 20).

En 2013, un misterioso grupo de *hackers* autodenominado The Shadow Brokers robó una serie de discos llenos de secretos de la Agencia de Seguridad Nacional (National Security Agency [NSA]). Desde 2016, han puesto estos secretos a disposición de internet para ser descargados. Han avergonzado públicamente a la NSA y han deteriorado sus capacidades de recopilación de información de inteligencia, al mismo tiempo que han preparado sofisticadas armas cibernéticas y las han puesto en manos de cualquiera que esté interesado en ellas. Además, han expuesto las principales vulnerabilidades en los servidores de enrutadores Cisco, Microsoft Windows y Linux, obligando a esas empresas y sus clientes a enfrentarlos (Schneier, 2017).

En total, el grupo ha publicado cuatro conjuntos de material de la NSA: un conjunto de herramientas de piratería contra los enrutadores, una serie de dispositivos que pueden redirigir datos a través de redes de computadoras y contra servidores de correo, una colección contra Microsoft Windows y un directorio de trabajo de un analista de la NSA que irrumpe la red de la Society for Worldwide Interbank Financial Telecommunication (SWIFT) (Schneier, 2017).

El teatro de los centros de gravedad: contra la infraestructura crítica

Como a la seguridad nacional se le ha asignado la más alta prioridad, el término *infraestructura crítica* se ha convertido en una importante

preocupación política. En la Orden Ejecutiva 13 010, firmada por el presidente Bill Clinton el 15 de julio de 1996, que establecía la Comisión Presidencial sobre protección de infraestructuras críticas, se hizo alusión a lo que constituye una infraestructura crítica: ciertas infraestructuras nacionales que son tan vitales que su incapacidad o destrucción tendría un impacto debilitante en la defensa o la seguridad económica de los Estados Unidos (Moteff, Copeland y Fischer, 2003, p. 2).

> El término *infraestructura* es evolutivo y a menudo ambiguo. Se define tradicionalmente como cualquier activo físico que puede ser utilizado para producir servicios o para apoyar la estructura y el funcionamiento de una sociedad o empresa. Hoy en día, la noción de *infraestructura pública* se ha ampliado y abarca estructuras tales como carreteras, puentes, aeropuertos e instalaciones de vías aéreas, sistemas de transporte colectivo, plantas de tratamiento de residuos, instalaciones energéticas, hospitales, edificios públicos e instalaciones espaciales o de comunicación.
>
> El entorno operativo para la infraestructura crítica es cada vez más complejo, impulsado por una serie de factores, que incluyen la globalización, la evolución de la tecnología y la naturaleza interconectada de las cadenas de suministro de infraestructuras críticas, redes y sistemas. Esta complejidad, en particular, afecta la capacidad de entender y manejar las dependencias intersectoriales. Las computadoras, las comunicaciones y las mismas infraestructuras críticas vinculan cada vez más a otras infraestructuras. La interconexión creciente de la red significa que una interrupción en una red puede conducir a la interrupción en otra. Esta dependencia de los ordenadores y las redes aumenta la vulnerabilidad de las infraestructuras críticas a los ataques cibernéticos[40]. (Simon, 2017, p. 2).

El hecho de que las infraestructuras críticas de las naciones estén altamente interconectadas y sean mutuamente dependientes de formas complejas, tanto físicamente como a través de una serie de tecnologías

40 Traducción del autor.

de la información y de la comunicación (TIC) (los llamados sistemas cibernéticos), es más que un concepto teórico abstracto. Lo que sucede con una infraestructura puede afectar directa e indirectamente a otras infraestructuras, a grandes regiones geográficas, y causar daños a toda la economía nacional y global (Boaru y Badita, 2008, p. 130).

> Las dependencias de infraestructura crítica con el ciberespacio se extienden más allá de las fronteras soberanas y se convierten en globales. Estas son áreas en las que un grupo diverso de actores, muchos con muy diversos intereses e incentivos, interactúan y compiten en un espacio predominantemente comercial, entonces, es mucho más que solo los gobiernos; tanto en el sector público como en el privado están íntimamente ligados, les guste o no. Estas interdependencias complejas a nivel mundial están redefiniendo lo que constituye la infraestructura crítica. Ellos desafían los conceptos de soberanía nacional y nos obligan a considerar las tensiones inherentes a un sistema altamente optimizado aún frágil de conexiones físicas, lógicas y sociales[41]. (Clemente, 2013, p. 1).

Identificar, comprender y analizar tales interdependencias son desafíos significativos. Estos desafíos se ven amplificados por la amplitud y complejidad de las infraestructuras nacionales críticas. Estas infraestructuras, que afectan a todos los ámbitos de la vida cotidiana, incluyen la producción y distribución de energía eléctrica, gas natural y petróleo, telecomunicaciones (información y comunicaciones), transporte, abastecimiento de agua, banca y finanzas, servicios de emergencia y gubernamentales, agricultura y otros sistemas fundamentales y servicios que son críticos para la seguridad, la prosperidad económica y el bienestar social de la nación (Boaru y Badita, 2008, p. 131).

Estos vínculos pueden ser físicos, cibernéticos, relacionados con la ubicación geográfica o de naturaleza lógica. Las infraestructuras interdependientes también muestran una amplia gama de características espaciales, temporales, operativas y organizativas, que pueden afectar su capacidad de adaptación a las condiciones cambiantes del sistema.

41 Traducción del autor.

Y, finalmente, las interdependencias y las tipologías de infraestructura resultantes pueden crear interacciones sutiles y mecanismos de retroalimentación que a menudo conducen a comportamientos no intencionados y consecuencias durante las interrupciones (Boaru y Badita, 2008, p. 132).

Estas dimensiones y sus componentes son descriptivos y están destinados a facilitar la identificación, la comprensión y el análisis de las interdependencias, las cuales varían ampliamente y tienen sus propias características y efectos sobre los agentes de la infraestructura. Se pueden establecer cuatro clases principales de interdependencias: física, cibernética, geográfica y lógica. Aunque cada una tiene características distintas, estas clases de interdependencias no son mutuamente excluyentes:

- Interdependencia física: dos infraestructuras son físicamente interdependientes si el estado de cada una depende de las salidas materiales de la otra. Como su nombre lo indica, una interdependencia física surge de un enlace físico entre los insumos y los productos de dos agentes: una mercancía producida o modificada por una infraestructura (una salida) es requerida por otra infraestructura para que funcione (una entrada). De esta manera, las perturbaciones en una infraestructura pueden irrumpir en otras infraestructuras. En consecuencia, el riesgo de falla o desviación de las condiciones normales de operación en una infraestructura puede ser una función del riesgo en una segunda infraestructura si ambas son interdependientes.

- Interdependencia cibernética: una infraestructura tiene una interdependencia cibernética si su estado depende de la información transmitida a través de la infraestructura de información. Las interdependencias cibernéticas son relativamente nuevas y son el resultado de la generalizada informatización y automatización de las infraestructuras en las últimas décadas. En gran medida, el funcionamiento fiable de las infraestructuras modernas depende de sistemas de control computarizados, desde los sistemas SCADA (*supervisory control and data acquisition*) que controlan las redes eléctricas hasta los sistemas

computarizados que gestionan el flujo de vagones y mercancías en la industria ferroviaria. En estos casos, las infraestructuras requieren información transmitida y entregada por la infraestructura de información. En consecuencia, los estados de estas infraestructuras dependen de los productos de la infraestructura de la información. Las interdependencias cibernéticas conectan las infraestructuras entre sí a través de enlaces electrónicos informativos; los productos de la infraestructura de la información son insumos para la otra infraestructura, y el "producto básico" pasado entre las infraestructuras es la información.

- Interdependencia geográfica: las infraestructuras son geográficamente interdependientes si un evento ambiental local puede crear cambios de estado en todas ellas. Una interdependencia geográfica se produce cuando elementos de múltiples infraestructuras están en estrecha proximidad espacial. Dada esta proximidad, eventos como una explosión o un incendio podrían crear alteraciones o cambios correlacionados en estas infraestructuras geográficamente interdependientes. Tales cambios correlacionados no se deben a conexiones físicas o cibernéticas entre infraestructuras, sino que surgen de la influencia que el evento ejerce sobre todas las infraestructuras simultáneamente. Nótese que más de dos infraestructuras pueden ser geográficamente interdependientes en función de su proximidad física.

- Interdependencia lógica: dos infraestructuras son lógicamente interdependientes si el estado de cada una depende del estado de la otra a través de un mecanismo que no es una conexión física, cibernética o geográfica. Las interdependencias lógicas pueden ser comparadas más estrechamente a un esquema de control que conecta un agente en una infraestructura a un agente en otra infraestructura sin ninguna conexión física, cibernética o geográfica directa (Boaru y Badita, 2008).

Una infraestructura crítica se identifica a menudo como una infraestructura cuyo funcionamiento incorrecto, incluso durante un periodo limitado, puede afectar la economía de individuos o grupos individuales,

con pérdidas económicas e, incluso, exponer a personas y cosas a un riesgo de seguridad (Montanari y Querzoni, 2014, p. 5).

> Las infraestructuras críticas son esencialmente procesos físicos controlados por computadoras en red. Son, por lo general, tan vulnerables como cualquier otro sistema informático interconectado, pero su fracaso tiene un alto impacto socioeconómico. Internet hoy es una red de dispositivos sofisticados, fibras y señales electromagnéticas, que interconectan los sistemas computacionales y electrónicos de todo el mundo e hicieron que la sociedad y la economía mundial evolucionaran. Sin embargo, los límites de esta web están ampliando su alcance a las infraestructuras físicas, como la energía, el agua, el gas, el petróleo y el transporte. Por tanto, la amenaza ya no es contra los sistemas con un valor económico limitado, sino contra las infraestructuras que soportan la vida moderna[42]. (Bessani, Sousa, Correia, Neves y Veríssimo, 2008, p. 18)

Existen numerosas definiciones nacionales e internacionales de la infraestructura crítica. Aunque las similitudes entre las definiciones tienden a pesar más que sus diferencias, los matices son reveladores. Un informe de la Asamblea Parlamentaria de la OTAN señala que en algunos países esos criterios destacan la finalidad o el propósito de la infraestructura (es decir, la infraestructura es fundamental, ya que realiza una función que es vital para la sociedad), mientras que en otros subrayan la gravedad de los efectos de la interrupción o destrucción de una infraestructura determinada en la sociedad (es decir, la infraestructura es fundamental, ya que su pérdida sería muy perjudicial) (Clemente, 2013, p. 13).

Una de las razones por las que la seguridad de las infraestructuras críticas es una cuestión compleja y urgente es que existen varios actores, como los siguientes, que representan una amenaza, posiblemente más que en los sistemas informáticos tradicionales:

1. Los Estados nación son un conjunto importante de actores en el paisaje de los ciberataques contra las infraestructuras críticas.

42 Traducción del autor.

Su importancia deriva del hecho de que son los propietarios de estas estructuras, las cuales son el objetivo más relevante en la ciberguerra moderna. Una extensión de esta categoría de actores incluye aquellos atacantes que son patrocinados por Estados nacionales, es decir, un sujeto externo pagado o apoyado por los gobiernos de la nación para comprometer las infraestructuras críticas de otra nación.

2. Los grupos de amenaza organizados no estatales en general etiquetados como "ciberterroristas" también están causando amenazas. El potencial de la guerra asimétrica se deriva de la facilidad de atacar las infraestructuras críticas a través de medios de guerra cibernética (Montanari y Querzoni, 2014).

Los actores antes mencionados están impulsados por dos amplias categorías de motivaciones:

- Guerra política y estratégica: de la cantidad de información confiable que circula en relación con los ataques contra infraestructuras críticas, se puede concluir que la mayoría de los ataques tienen motivaciones estratégicas. Otro tipo de ataque tiene el objetivo de filtrar información secreta. Por el momento, no se puede establecer con certeza cuál es el uso final de dicha información; sin embargo, se puede argumentar que las principales motivaciones son de naturaleza política. Actores como Estados nacionales y hacktivistas caen en esta categoría.

- Financiera: los actores orientados a los negocios y los Estados nacionales también están impulsados por razones económicas. Esta categoría de motivación ha existido siempre. Sin embargo, golpear la infraestructura crítica valiosa puede resultar en un impacto financiero sustancialmente más alto que golpear a los sistemas tradicionales de tecnologías informáticas (Montanari y Querzoni, 2014).

Las redes informáticas de soporte inciden directamente en el funcionamiento de los sistemas de infraestructura como agua, alcantarillado, energía eléctrica. Estos, además de la gestión del transporte

público, se engloban en una categoría conocida como sistemas de control industrial (*industrial control system* [ICS]). Esta categoría incluye "varios tipos de sistemas, como el control de supervisión y adquisición de datos (*supervisory control and data acquisition* [SCADA]), sistemas de control distribuido (*distributed control system* [DCS]) y los controladores lógicos programables (*programmable logic controller* [PLC]), todo diseñado para gestionar los equipos industriales esenciales para los servicios prestados" (Reu, Shakarian y Shakarian, 2013, p. 200).

Identificar, entender y analizar las interdependencias entre infraestructuras ha adquirido una importancia creciente en la última década. Los cambios tecnológicos, económicos y regulatorios han alterado radicalmente las relaciones entre las infraestructuras, y la revolución de la tecnología de la información ha dado lugar a lo esencial de las infraestructuras más interconectadas y complejas en general con mayor centralización del control (Rinaldi, Peerenboom y Kelly, 2001, p. 24). De hecho, la tendencia hacia una mayor interdependencia de la infraestructura se ha acelerado y muestra pocas señales de disminuir.

La comunidad de la infraestructura crítica incluye a los propietarios y operadores públicos y privados, y a otras entidades con un papel dentro de la infraestructura de la nación. Los miembros de cada sector de la infraestructura crítica realizan funciones que son compatibles con la tecnología de la información (TI) y los ICS. Esta dependencia de la tecnología, la comunicación y la interconectividad de las TIC y los ICS ha cambiado y ampliado las posibles vulnerabilidades y un mayor riesgo potencial de operaciones. Como los sistemas de control industrial y los datos producidos en operaciones de ICS se utilizan cada vez más para entregar servicios críticos y apoyar las decisiones de negocios, el impacto potencial de un incidente de seguridad cibernética en una organización empresarial, los activos, la salud y la seguridad de las personas y el medioambiente deben ser considerados (National Institute of Standards and Technology, 2014, p. 3).

La ciberguerra se ha convertido en un peligro actual con el descubrimiento del gusano Stuxnet en junio de 2010, el cual fue pionero en el ataque coordinado contra la infraestructura crítica o los sistemas de control de una nación. Los ataques clandestinos estadounidenses contra

los sistemas informáticos de las instalaciones iraníes de enriquecimiento nuclear en 2012, así como los ataques cibernéticos rusos contra los sitios web y las infraestructuras de redes de Estonia y Georgia, se clasifican como tácticas de la ciberguerra (Simon, 2017, p. 4).

Mientras transcurría abril de 2007, se desarrolló una pequeña disputa interna entre el Gobierno estonio y los habitantes rusos en este país por un monumento soviético ubicado en la capital (*The Economist*, 2007). Esta tensión condujo, aparentemente, a que el país europeo fuese víctima de un ataque a su infraestructura de información, que sentó precedentes al ser el primer ataque cibernético que se ha dirigido a la seguridad nacional de un país (Ashmore, 2009, p. 4). Los daños se dieron, principalmente, en los sitios web del Gobierno y de los bancos, que sustituyeron la información oficial y lograron la incomunicación y problemas para cumplir con sus funciones.

Para mayo, los ataques ya eran graves, los cuales llegaron a causar una disfunción total, tanto para los trabajadores del Gobierno que querían comunicarse como para los usuarios de páginas de compras y de libre acceso. Esto se extendió por un par de días y causó problemas tanto políticos como económicos (*The Economist*, 2007).

El ataque Distributed Denial of Service (DDoS) fue dirigido con éxito a los sitios web de todos los ministerios del Gobierno, dos de los principales bancos y varios partidos políticos. Los *hackers* fueron, incluso, capaces de desactivar el servidor de correo electrónico parlamentario y desactivar tarjetas de crédito y cajeros automáticos. Uno de los bancos de Estonia víctima de los ataques calculó las pérdidas estimadas del ciberataque en alrededor de un millón de dólares en daños y perjuicios (Kozlowski, 2014, p. 248).

El 20 de julio de 2008, la página web del presidente georgiano fue objeto de un ataque de denegación de servicio cibernético. El ataque cerró la página web durante 24 horas y fue un precursor de un ataque cibernético más grande que vendría menos de un mes más tarde. El 8 de agosto de 2008, un ataque de denegación de servicio coordinado se hizo en contra de los sitios web del Gobierno de Georgia, al mismo tiempo que las fuerzas rusas estaban comprometidas en el combate con las fuerzas georgianas. A medida que los ataques terrestres aumentaron lo hicieron los ataques cibernéticos. Esta fue la primera vez

que un ataque cibernético fue realizado en conjunto con el conflicto armado (Ashmore, 2009, p. 20).

Había transcurrido poco más de un año cuando otro país de la región se vio afectado en el sector informático. Georgia vio cómo, mientras enfrentaba una guerra tradicional contra el Ejército ruso por Osetia, sus páginas web militares y políticas eran paralizadas (Korns y Kastenberg, 2009). Las intenciones más probables de este ataque era desinformar a la comunidad y desestabilizar las capacidades de mantener el orden por parte del Gobierno, lo que traería a su vez como consecuencia una disminución en la habilidad de responder ante el conflicto físico en la frontera ruso-georgina (Kuehl, 2009).

> El ataque ruso en redes militares y gubernamentales a Georgia tuvo un gran éxito. Al parecer, 54 sitios web en Georgia relacionados con las comunicaciones, las finanzas y el Gobierno fueron atacados por elementos corruptivos desde Rusia. Así como tanques y tropas estaban cruzando la frontera y misiones de bombarderos sobrevolaban, los ciudadanos georgianos no podían acceder a los sitios web para obtener información e instrucciones. Las autoridades de Georgia descubrieron que su acceso a internet y las redes de comunicación eran excepcionalmente vulnerables a la interferencia de Rusia[43]. (Hollis, 2011, p. 2)

Con el fin de la primera década del siglo xxi, llegó un momento trascendental en el ámbito de la guerra cibernética. Los investigadores de seguridad de VirusBlockAda encontraron un *malware* en una planta de tratamiento de uranio en Irán, un gusano informático denominado Stuxnet, diseñado exclusivamente para hacer funcionar incorrectamente cualquier equipo industrial que se viera infectado. Este ataque fue catalogado por expertos en seguridad informática como un acontecimiento sin precedentes (Shakarian, 2011, p. 50).

Esta herramienta tecnológica entró en el sistema por un procesador a través de conexiones de usb, y se difundió con impresionante velocidad, llegando a países como China y la India (Kuehl, 2009).

43 Traducción del autor.

Fue programado para buscar los sistemas informáticos que estaban al mando del reactor nuclear de Bushehr. Quienes se encargaron dentro del Gobierno iraní de investigar el fenómeno tuvieron que mantener bajo absoluta reserva el alcance definitivo de Stuxnet, por lo que a partir de este punto no hubo más que desinformación (Kerr, Rollins y Theohary, 2010). Hasta ese momento el gusano era, por lejos, el arma más potente en el escenario cibernético:

> El incidente dañó casi 1000 tubos de centrifugación en la instalación iraní de Natanz. Esta cifra es significativa a la luz del número total de tubos instalados (9000) y la porción de los alimentados con uranio (4000). Una disminución del 23 % en el número de centrifugadoras de funcionamiento desde mediados de 2009 hasta mediados de 2010 puede haber sido debido al ataque Stuxnet[44]. (Gamero-Garrido, 2014, p. 22)

Al 25 de septiembre de 2010, Irán había identificado las direcciones IP de 30 000 sistemas informáticos industriales que habían sido infectados por Stuxnet, según Mahmoud Liaii, director del Consejo de Tecnología de la Información de Industrias y Minas del Ministerio de Irán, quien argumentó que el virus está diseñado para transferir datos sobre las líneas de producción de las plantas industriales a lugares fuera de Irán (Kerr, Rollins y Theohary, 2012, p. 3). Es posible asegurar que antes de Stuxnet no había sucedido un ataque con un impacto semejante. Desde un principio, mantuvo como objetivo la infraestructura crítica nuclear iraní (Porteus, 2010), y por primera vez, un ataque diseñado y ejecutado exclusivamente en el ciberespacio tuvo alcances reales y físicos.

El hacktivismo surgió a finales de la década de 1980 en forma de virus de internet y gusanos de propagación con propaganda política y mensajes de protesta. El grupo Worms Against Nuclear Killers (WANK) es un ejemplo de hacktivismo temprano; en 1989, estos hacktivistas antinucleares con sede en Australia instalaron gusanos en las redes de la NASA y el DOE para protestar por el lanzamiento de un transbordador

44 Traducción del autor.

espacial que transporta plutonio radiactivo. A mediados de la década siguiente, los ataques DOS se hicieron comunes, a menudo tomando la forma de mensajes o tráfico de información que superaba las capacidades; por ejemplo, en 1994, el grupo Zippies envió mensajes de correo electrónico en el Reino Unido para protestar contra un proyecto de ley que prohibía los festivales de música de baile al aire libre. El término hacktivismo fue acuñado en 1996 por el grupo de *hackers* Cult of the Dead Cow (culto de la vaca muerta), y el término adquirió ímpetu en los medios durante el conflicto de Kosovo de 1998-1999, cuando se lanzaron ataques de DOS contra sitios web en los países miembros de la OTAN. El hacktivismo se ha convertido en un medio común de protesta: existen grupos en todo el mundo, algunos se asocian con un país específico, como Siria anónima; otros se asocian con un Gobierno particular o un grupo político, como el califato cibernético, mientras que otros no expresan ninguna lealtad particular, tal como Anonymous (Simon, 2017, p. 2).

> Anonymous, un grupo organizado de activistas *hackers* conocidos por usar las máscaras de Guy Fawkes, ganó popularidad con el lanzamiento del Proyecto Chanology, protestas lanzadas contra lo que el grupo identificó como censura en internet por la Iglesia de Cienciología. Desde entonces, el grupo ha sido responsable de ataques cibernéticos y hacktivismo contra gobiernos, organizaciones terroristas (que incluyen el Estado Islámico de Irak y Levante), corporaciones, grupos religiosos y presuntos delincuentes sexuales, entre otros. Los hacktivistas, además de los ataques DOS y los sitios web defectuosos, a menudo se apropian de las cuentas de Twitter y Facebook, hacen un uso extensivo de las redes sociales para promover sus acciones, robar y revelar información sensible de los sistemas que penetran. (Simon, 2017, p. 3)

Los *hackers* criminales (motivados por ganancias económicas a través de la penetración ilegal de redes informáticas y de naturaleza relativamente no violenta) operan en todo el mundo y han reemplazado las formas tradicionales de delincuencia. Se estima que han costado a la economía mundial un estimado de USD 445 000 millones. En términos generales, el delito cibernético incluye el fraude, la venta en contrabando

y los artículos falsificados y las estafas en línea. Luchar contra el cibercrimen es particularmente complicado, porque los crímenes a menudo impugnan los límites jurisdiccionales. Un *hacker* criminal puede sentarse en un país, usar un servidor alojado en otro y hackear sistemas alojados en un tercero, lo que hace que los componentes legales y geográficos del delito sean un desafío para investigar, y mucho más para procesar (Simon, 2017, p. 3).

El espionaje cibernético es una estrategia dirigida a la obtención de información crítica gubernamental o corporativa. China ha sido particularmente activa en la piratería estatal. Según un estudio, casi la mitad de todos los ataques de ciberespionaje en el mundo provienen de Asia oriental, en particular de China y Corea del Norte. Este último ha emprendido ataques de denegación de servicio contra Corea del Sur en la década reciente. También, Irán fue culpado en 2013 por atacar a Aramco, la compañía petrolera de Arabia Saudita, al borrar datos de aproximadamente 30 000 computadoras y penetrar en las redes de la Royal Saudi Navy y Marine Corps (Simon, 2017, p. 3).

El 27 de agosto de 2011, un internauta iraní recibió una advertencia de un certificado inválido de su navegador cuando visitó el sitio web de Gmail. Informó este incidente a Google. El certificado fue generado el 10 de julio de 2011. Durante las semanas siguientes, se hizo evidente que el certificado fraudulento fue emitido por DigiNotar, un proveedor de certificados de seguridad holandés, después de una intrusión exitosa en sus servidores. El papel importante que DigiNotar cumple en los Países Bajos es triple. En primer lugar, DigiNotar es uno de los proveedores de certificados de seguridad para el Gobierno holandés. En segundo lugar, es un emisor de certificados para la Public Key Infrastructure (PKI) nacional holandesa (PKIoverheid). En tercer lugar, DigiNotar emite certificados para firmas calificadas. El marco para las firmas cualificadas es un intento por parte de la Unión Europea (UE) de otorgar un mayor valor jurídico a las firmas digitales. Poco a poco, quedó claro que los tres sistemas se habían visto comprometidos durante el robo. Esto implicaba que la confianza ya no podía situarse en la confidencialidad o integridad de los datos o comunicaciones que se habían obtenido con un certificado DigiNotar (National Cyber Security Center, 2014, p. 7).

El viernes 25 de noviembre de 2011, se produjo un error de *hardware* en el proveedor de servicios de Tieto. Una parte central de un gran sistema de almacenamiento de datos en una instalación de Estocolmo sufrió un cierre de emergencia. En primer lugar, se perdió un importante componente del sistema. En ese momento, todavía habría sido posible recurrir a un sistema de respaldo que estaba en espera y listo para tomar el relevo. Sin embargo, después de un corto tiempo el sistema de respaldo también funcionó mal, lo que hizo que el almacenamiento de datos para los sistemas de servidor conectados no fuera funcional. La interrupción afectó a cerca de 50 clientes de Tieto, que incluyen empresas, agencias gubernamentales y municipios (National Cyber Security Center, 2014, p. 19).

El 16 de agosto de 2012, Symantec y Kaspersky Lab, seguidos de otros vendedores e investigadores, describieron un nuevo gusano de computadora modular, que fue denominado Shamoon. El *malware* fue parte de una serie de ataques de espionaje y sabotaje cibernéticos en Oriente Medio. Si bien no es notable por sus mecanismos de propagación, que explotan unidades compartidas y carpetas, lo es por su carga útil bastante única. Una vez que un sistema está infectado, Shamoon reúne archivos desde ubicaciones específicas del sistema, envía la información recolectada al atacante y reemplaza los archivos y los registros centrales del sistema con una imagen de una bandera americana en llamas. El grupo denominado Corte de Espada de Justicia reclamó la responsabilidad de usar Shamoon contra 30 000 estaciones de trabajo de Saudi Aramco (empresa de petróleo estatal de Arabia Saudita), lo que ocasionó que la compañía pasara una semana restaurando sus servicios. Sorprendentemente, el ataque no afectó ninguno de las computadoras y redes de control de producción, y se limitó a los sistemas administrativos (Montanari y Querzoni, 2014, p. 37).

En septiembre de 2012, Deutsche Telekom AG, un ISP (*internet service provider* 'proveedor de servicios en internet'), fue atacado por adversarios desconocidos. El ataque de denegación de servicio fue un intento de bloquear el sistema de nombres de dominio del proveedor. Desde un punto de vista práctico, una interrupción del DNS (*domain name system* 'sistema de nombres de dominios') causaría una interrupción de internet para la mayoría de los clientes de ese proveedor. La

telecomunicación e internet pertenecen a la infraestructura crítica de un país. Su interrupción podría tener efectos adversos significativos en el mismo. Para este ataque, el adversario utilizó la infraestructura de servidor de otro proveedor de alojamiento web (National Cyber Security Center, 2014, p. 15).

En diciembre de 2014, el Bundesamt für Sicherheit in der Informationstechnik (BSI) del Gobierno alemán publicó su informe anual de conclusiones. En un caso, notaron que un actor malicioso se había infiltrado en una instalación de acero. El adversario usó un correo electrónico de *phishing* para ganar acceso a la red corporativa y luego se trasladó a la red de la planta. Según el informe, el atacante mostró conocimiento en sistemas de control industrial y fue capaz de causar fallas en múltiples componentes del sistema. Esto afectó específicamente componentes críticos del proceso para no seguir las indicaciones programadas, lo que generó un daño físico masivo (Lee, Assante y Conway, 2014, p. 1).

En el transcurso de 2017, se presentó el *software* malicioso WannaCry, el cual afectó al NHS (National Health Service 'Servicio Nacional de Salud'), algunas de las compañías más grandes de España, que incluyen Telefónica, así como a computadoras en Rusia, Ucrania y Taiwán, lo que llevó a que la información fuera robada y guardada por los atacantes para luego pedir rescates económicos. Este *ransomware* utilizó una vulnerabilidad revelada por primera vez al público como parte de una filtración de documentos de la NSA para infectar las computadoras con sistema operativo Windows y cifrar sus contenidos, lo que les permitió exigir pagos de cientos de dólares con el fin entregar las claves para descifrar los archivos. El ataque coordinado logró infectar grandes cantidades de computadoras en todo el NHS en menos de seis horas después de que los investigadores de seguridad lo notaran por primera vez, debido a su capacidad de propagarse a través de las redes de computadora a computadora (Gibbs y Hern, 2017).

El teatro robótico: llega la automatización

Cuando los historiadores analicen las cuestiones de defensa en esta primera mitad del siglo XXI, observarán que los robots militares trajeron

algo nuevo al mundo de la guerra y constituyeron un cambio aún más radical que la invención de las armas nucleares, ya que estos "no solo afectan a las modalidades de la guerra en constante cambio (cómo emprender la guerra), sino también a su esencia básica (quién hace la guerra)"[45] (Danet y Hanon, 2014, p. 13).

Un sector donde se ven claramente reflejadas las características positivas y facilidades que ha ofrecido la evolución tecnológica es por supuesto la robótica, principalmente en el ámbito militar, sin dejar de lado los demás, pero aclarando que casi siempre la seguridad y defensa son pioneros en avanzar en temáticas que faciliten sus procesos. Las armas no tripuladas mandan la parada en los conflictos de la actualidad para los ejércitos de países que pueden financiarlos, probarlos y usarlos: "Al contrario de las armas convencionales donde se arriesga uno o más soldados, los robots son manejados a kilómetros de distancia"[46] (Leveringhaus y Giacca, 2014, p. 6).

En términos generales, un robot militar se define con más frecuencia como un "sistema que posee capacidades de percepción, comunicación, toma de decisiones y acción; es supervisado por combatientes humanos o actúa de manera autónoma de acuerdo con reglas preestablecidas de comportamiento y es capaz de mejorar su propio funcionamiento con aprendizaje automático" (Danet y Hanon, 2014, p. 17).

Entre las principales características que posee, o debería poseer un robot, se encuentra su movilidad, no poseer humanos en su interior, ser capaces de tomar ciertas decisiones por su cuenta (geolocalización, navegación, enrutamiento), ser un recurso que puede reemplazarse con facilidad, y estar aptos y capacitados para actuar según las instrucciones recibidas y el contexto en el que se encuentren (Lin, Bekey y Abney, 2008).

El nombre detrás de la idea de inteligencia artificial es John McCarthy, quien comenzó la investigación sobre el tema en 1955 y asumió que es posible describir cada aspecto del aprendizaje y otros dominios de inteligencia con tanta precisión que pueden ser simulados

45 Traducción del autor.

46 Traducción del autor.

por una máquina. "La inteligencia artificial describe los procesos de trabajo de las máquinas que requerirían inteligencia si las realizaban los humanos" (Wisskirchen, Biacabe, Bormann, Muntz, Niehaus, Soler y Von Brauchitsch, 2017, p. 9). El término *inteligencia artificial* significa, por tanto, investigar el comportamiento inteligente de resolución de problemas y crear sistemas informáticos inteligentes.

Las tecnologías emergentes tienen distintos alcances en el desarrollo de la guerra. Pueden hacer más fácil, eficaz y con tasas de daños colaterales menores; estos sistemas pueden ser tremendamente costosos de construir y de implementar, y por supuesto, como todos los demás avances tecnológicos, crearán una relación dependiente aumentando los riesgos para la seguridad del actor que los implemente (Grauer, 2013).

La principal motivación detrás del desarrollo de armas autónomas tiene que ver con la distribución de la fuerza militar. La esperanza es que tales armas permitan a los comandantes desplegar su personal y su poder de fuego de una manera nueva e increíblemente efectiva. El DoD, por ejemplo, está desarrollando actualmente tecnologías para la tierra, el mar y el aire. En un escenario futuro, un pequeño número de pilotos supervisarían una gran flota de letales aviones autónomos. En otro escenario, los robots autónomos acompañarían a las tropas estadounidenses en la batalla. Estos robots podrían identificar la fuente de fuego hostil y tomar represalias inmediatamente, sin autorización humana:

> Un argumento para las armas autónomas tiene que ver con la velocidad y la complejidad de la guerra moderna. La guerra es una carrera contra el tiempo. Quien sea capaz de pensar más rápido, tomar decisiones más rápido e iniciar operaciones militares inteligentes más rápido que sus enemigos, por lo general gana. Los militares tecnológicamente avanzados recurren cada vez más a las computadoras para compilar y analizar rápidamente cantidades masivas de información, que luego sirven de base para las decisiones estratégicas[47]. (Danish Institute For International Studies, 2017, p. 2)

47 Traducción del autor.

Desde las dagas, espadas y lanzas a los arcos, la artillería y las armas de fuego en los aviones, los misiles de crucero y los misiles balísticos intercontinentales, las mejoras en el diseño de armas a lo largo del tiempo han permitido a los combatientes identificar y aniquilar a los otros a cada vez mayores distancias. La característica actual que ha facilitado y marcado un hito en la guerra moderna es la autonomía, pues no requiere la presencia en el campo de batalla, lo que aminora considerablemente los daños. La autonomía se define como la capacidad de sentir, decidir y actuar sin un comando humano. Es importante aclarar que aún ningún arma cuenta con autonomía total, pero sí con algún grado de ella como bombas inteligentes con GPS (*global positioning system* 'sistema de posicionamiento global') y mecanismos de control para actuar con precisión (Asaro, 2012).

> Sin embargo, todavía los agentes humanos que controlan el sistema de armas deciden la selección de un objetivo y la determinación de su ubicación, el valor y los riesgos. Aún más autónomos son los sistemas que utilizan sensores de análisis sofisticados para seleccionar los objetivos apropiados por su cuenta y tomar decisiones sobre la idoneidad de las distintas acciones en respuesta a su situación. Las tecnologías emergentes de plataformas de armas robóticas incorporan algunas o todas estas características, el uso de procesamiento de imágenes para identificar objetivos y la selección de una amplia gama de acciones ofensivas y defensivas contra sus objetivos. Estas son las capacidades tecnológicas que ya existen y están comenzando a ser implementadas en varios países[48]. (Asaro, 2012, p. 258)

Los robots, edificios inteligentes, automóviles que se conducen solos o aviones que vuelan de forma automática en un espacio aéreo controlado son ejemplos de sistemas ciberfísicos. Hoy, "los sistemas ciberfísicos pueden encontrarse en industrias tan diversas como la industria aeroespacial, automoción, energía, salud, manufactura, infraestructura,

48 Traducción del autor.

electrónica de consumo y comunicaciones"[49] (Steering Committee for Foundations for Innovation in Cyber-Physical Systems, 2012, p. 2).

El principal cambio es el aumento y la rápida proliferación de los sistemas no tripulados. Estos ya han reformado profundamente la estrategia de defensa y prioridades de adquisiciones estadounidenses y son cada vez más importantes en las Fuerzas Armadas de todo el mundo. Otras tecnologías emergentes que pueden perturbar el equilibrio militar mundial así son informática avanzada, inteligencia artificial, sensores densamente interconectados, armas eléctricas tales como energía dirigida, armas de riel electromagnético y armas de alto poder de microondas, fabricación de aditivos, la impresión 3D, biología sintética, entre otras (Work y Brimley, 2014). Todas estas tecnologías, impulsadas principalmente por la demanda y los avances en el sector comercial, están surgiendo hoy y tienen el potencial de provocar una nueva revolución técnico-militar.

La categorización de los robots no es muy precisa. No existe una tipología universalmente aceptada, y un análisis pone de manifiesto múltiples clasificaciones de diferentes tipos: clasificaciones técnicas (basadas en el tamaño de las plataformas robóticas) y clasificaciones funcionales o clasificaciones operativas (de acuerdo con las misiones o tareas de robots). Todas las caracterizaciones insisten en dos de las dimensiones fundamentales de la robotización del campo de batalla: "El grado de autonomía del robot y la perspectiva más o menos inminente de ver a los robots actuar en grupos. Por tanto, el robot debe ser considerado como una máquina autónoma o como un sistema de máquinas"[50] (Danet y Hanon, 2014, p. 17).

Los conflictos requieren procesamiento de la información y respuestas mucho más rápidas, y frente a eso, los robots tienen una clara ventaja sobre las capacidades cognitivas limitadas y falibles de los humanos. No expandirían el espacio de batalla por alcanzar grandes áreas, también serían un multiplicador de fuerza, haciendo el trabajo de muchos soldados humanos, de modo que serían inmunes a la

49 Traducción del autor.

50 Traducción del autor.

privación del sueño, fatiga, baja moral, perceptual y retos de la comunicación en la "niebla de guerra", y otras condiciones que obstaculizan el rendimiento (Lin, Bekey y Abney, 2008, p. 1).

El principal interés militar en los robots proviene del hecho de que ayudan a salvar vidas, en cualquier caso, es el credo de los fabricantes y uno de los factores impulsores en el uso de robots en las Fuerzas Armadas. Los robots son ante todo percibidos como herramientas que aumentan la eficiencia operativa de las fuerzas militares. Un robot no está sujeto a lapsos de concentración, ni a las mismas limitaciones fisiológicas que el cuerpo humano. No tiene hambre, no se asusta, ni se olvida de las órdenes. Y, por último, desde un punto de vista económico, el coste de un robot es menor que el de un soldado en funcionamiento. Un soldado estadounidense enviado a Afganistán equivale a un costo de USD 1 millón por año, incluido el entrenamiento. En comparación, un PackBot cuesta alrededor de USD 150 000, y un MARCbot, unos USD 5000 (Tisseron, 2014).

Vale la pena considerar las expectativas de los sistemas robóticos:

1. En primer lugar, los robots se utilizan para la protección, es decir, para reducir la exposición de un soldado a los riesgos. Asistencia en el desminado, ayuda en el reconocimiento de misiones, protección de convoyes en zonas de riesgo, limpieza de áreas CBRN (*chemical, biological, radiological or nuclear* 'químico, biológico, radiológico y nuclear'). Ellos crean una mayor distancia con las amenazas de combate, son los primeros en asumir el choque antes de la infantería y pueden detectar la ubicación exacta desde donde se hacen los disparos. Pueden responder en tiempo real en unos pocos milisegundos, como lo hacen los sistemas de mortero de artillería Counter Rocket, con un sistema integrado de toma de decisiones.

2. Los robots también están para aumentar la efectividad de un soldado que lucha, con lo que traen ventajas tácticas en la ejecución de su misión. Se utilizan sobre todo para extender las áreas de control y cobertura de una unidad táctica. Esto se hace mediante el uso de efectores remotos, sensores y armas colocadas a bordo de cada robot. En cierto sentido, son los

"órganos remotos" de los ojos, los oídos, los brazos, el tacto e, incluso, la boca de un soldado.

3. Los robots pueden tener velocidades de despliegue mucho más altas que el hombre. Esto puede ayudar a anticipar las acciones del enemigo o a reaccionar inmediatamente a una amenaza con mayor eficiencia. Los robots también pueden ayudar en las maniobras mediante la identificación de las características del terreno para facilitar la progresión, la preparación del terreno o la seguridad de un área determinada.

4. Finalmente, los robots son una ayuda para reducir el uso de la energía humana: pueden reemplazar a los soldados en tareas repetitivas y tediosas (misiones de vigilancia y patrullas regulares, logística de transporte y suministros generales), y dejar espacio para que las fuerzas operativas actúen cuando sea necesario. Los robots también pueden ayudar llevando suministros, municiones e, incluso, armas durante misiones de larga distancia (nivel de la red de tierra). A un nivel más estratégico, los robots reducen el desgaste a medida que continúan las operaciones de combate, con lo que permiten a las unidades combatientes mantenerse en el campo de batalla mucho más tiempo que antes (De Boisboissel, 2014).

Esta tendencia no quita la importancia de la participación humana, pero sí cambia las funciones y los requisitos para los nuevos conjuntos de habilidades. Además, como los sistemas ciberfísicos son dependientes de los procesos computacionales, se vuelve cada vez más importante que estén diseñados para ser confiables y seguros. Los avances científicos y de ingeniería del futuro que amplían la conectividad de estos sistemas y ofrecen una mayor fiabilidad podrían abrir nuevas posibilidades para tomar ventaja de las propiedades únicas de sistemas ciberfísicos (Steering Committee for Foundations for Innovation in Cyber-Physical Systems, 2012, p. 3).

Como se ha dicho, los robots podrían llevar a cabo los trabajos más difíciles, arriesgados o arduos, de una forma tremendamente más eficiente. También podrían reducir drásticamente el comportamiento

poco ético y los altos costos del desplazamiento de tropas y armamento a grandes distancias (Lin, Bekey y Abney, 2008).

> Los militares pueden usar vehículos aéreos no tripulados (UAV '*unmanned aerial vehicle*') para la vigilancia, pero también para bombardear blancos en el suelo. Hoy en día, muchos países producen y utilizan drones. Se han utilizado drones en Afganistán, Pakistán, Yemen y Somalia. Han matado tanto a combatientes como a civiles, no solo unos cuantos, sino cientos. Las principales razones por las que la tecnología es utilizada por los militares es que ayuda a lograr una táctica clave y un objetivo militar estratégico en tiempos de guerra: inflige tanto daño al enemigo mientras intenta arriesgar el menor número posible de personal y recursos[51]. (Coeckelbergh, 2013, p. 87)

La robótica autónoma tiene muchas aplicaciones en la partida militar, algunas de las cuales incluyen protección para los soldados que promueven condiciones de vida más seguras, mientras que otras están siendo diseñadas como sistemas de armas completamente operacionales. La robótica utilizada para la seguridad incluye la detección y destrucción de bombas. En la última década, los Estados Unidos han enviado más de 6000 dispositivos robóticos a Irak y Afganistán para ayudar a los soldados con la vigilancia y la gestión de las bombas. Los sistemas de armamento, sin embargo, aún están en desarrollo y llevarán años antes del despliegue, pero el consenso es que estas armas harían la guerra más segura poniendo menos soldados en peligro y limitando las bajas civiles (Clark, 2015).

La evolución de la robótica es sorprendente. George Devol fue quien creó brazos mecánicos en la década de 1960, pero no fue sino hasta 1980 que los modelos robóticos con cierto grado de autonomía llamaron la atención de algunos científicos. Los primeros robots creados por Grey Walter ya poseían características como sensores de luz y motores recargables (Lin, Bekey y Abney, 2008, p. 11).

51 Traducción del autor.

Desde 2002, y tras la muerte en Yemen del terrorista Abu Ali al-Harithi, asesinado por un misil de un UAV Predator de la Agencia Central de Inteligencia (CIA 'Central Intelligence Agency'), el uso ofensivo de vehículos aéreos no tripulados se ha vuelto cada vez más frecuente para asesinatos selectivos. Los Estados Unidos dependían tanto de los UAV que, para el exdirector de la CIA, Leon Panetta (2009-2011), los UAV armados parecían ser la única arma eficiente para combatir a Al Qaeda en todo el mundo (Tisseron, 2014, p. 3).

Los avances más grandes en robótica se han hecho en vehículos aéreos no tripulados, con los Estados Unidos en la delantera, Israel detrás, y al menos otros 40 países tratando de ponerse al día. En el momento de la guerra de Irak en 2003, los Estados Unidos habían puesto en marcha seis grandes UAV: el Predator de la Fuerza Aérea, el Global Hawk, el Hunter, el Shadow, el Pioneer y el Dragon Eye. Estos variaban en tamaño, del Global Hawk de GBP 27 000 (comparable a un jet de Lear) al Dragon Eye de GBP 5 (más bien como un aeroplano modelo). Lo que tenían en común era que estaban diseñados como sistemas de vigilancia. Pero en un patrón que hace eco de la historia del vuelo tripulado, los UAV como el Predator pronto se dispusieron a trabajar atacando posiciones enemigas (Boot, 2006, p. 23).

Los teatros de operaciones iraquíes y afganos han constituido vastos centros de experimentación al aire libre para los robots del mañana. El Big Dog, un robot cuadrúpedo capaz de acompañar a los soldados de infantería en terrenos accidentados y montañosos, para llevar equipo y otras cargas pesadas (hasta 150 kg) a una velocidad de 4 km/h, es uno de esos robots que han sido enviados y probados en Afganistán. Otro ejemplo es el robot móvil SWORDS (*special weapons observation reconnaissance detection systems*), armado con ametralladoras, desplegado en 2007 en Irak, que también fue desplegado en Afganistán. Su sucesor, el MAARS (*modular advanced armed robotic system* 'sistema robótico modular avanzado armado'), es de hecho una unidad más pesada. Puede ser equipado con una gama de armas diferentes: ametralladora, lanzagranadas, lanzacohetes, junto con altavoces para alentar al enemigo a rendirse o pedir a la población que abandone el área. También puede programarse para definir "zonas de disparo" y "zonas de exclusión" (Tisseron, 2014, p. 4).

El uso de armas robóticas en el campo de batalla es otra manera de utilizar las TIC en la guerra. Se trata de un fenómeno cada vez más generalizado en el Ejército de los Estados Unidos, que desplegó 150 armas robóticas en la guerra de Irak en 2004 que culminó con 12 000 robots para 2008. Hoy en día, varios ejércitos de todo el mundo están desarrollando y utilizando armas robóticas teleoperadas, que han sido desplegados en Irak y Afganistán, y las máquinas más sofisticadas están siendo utilizadas en las fronteras entre Israel y Palestina en la denominada "zona de muerte automática". Estos robots son capaces de detectar con precisión la presencia de enemigos potenciales, mediar la acción de los soldados humanos y disparar sobre blancos potenciales de enemigos cuando estos están dentro del rango patrullado por los robots. Varios ejércitos también invirtieron sus recursos para desplegar vehículos no tripulados, como los depredadores MQ-1, los cuales se han utilizado para golpear objetivos en tierra y desarrollar vehículos aéreos de combate no tripulados, que están diseñados para entregar las armas y potencialmente pueden actuar de forma autónoma, como el EADS Barracuda y el Northrop Grumman X-47B.5 (Taddeo, 2012, p. 109).

Israel está a la vanguardia en el campo de la robotización del campo de batalla, con trabajos que se basan directamente en los recientes combates. A su regreso de los 34 días de enfrentamientos violentos en el Líbano durante el verano de 2006, las unidades israelíes comprometidas informaron de sus dificultades para expulsar a los combatientes de Hizbulá afianzados en una red de refugios fortificados subterráneos construidos bajo la dirección de ingenieros iraníes y norcoreanos. Investigadores de la Universidad Ben Gurion, en colaboración con los del Israel Institute of Technology (Technion), desarrollaron un robot-serpiente de dos metros de longitud, capaz de arrastrarse por estrechos túneles. La cabeza de este robot está formada por sensores y cámaras que envían información a los soldados. También puede utilizarse para colocar una carga explosiva. En cuanto a la frontera con el Líbano y la franja de Gaza, para limitar los ataques a las tropas de patrulla, la vigilancia es proporcionada por un dispositivo controlado a distancia llamado el Guardium. Los robots son un recurso tecnológico que toma su lugar junto a las cercas o los muros de las fronteras cerradas (Tisseron, 2014, p. 4).

Uno de los últimos tipos de arma robótica SGR-A1 se ha desplegado por Corea del Sur para patrullar la frontera con Corea del Norte. Este robot tiene una cámara de luz baja y un *software* de reconocimiento de patrones para distinguir a los humanos de los animales u otros objetos. También cuenta con una cámara en color, que puede localizar un objetivo a 500 m y, si es necesario, puede disparar su ametralladora incorporada. Hasta ahora, las armas robóticas fueron teleoperadas por militares sentados a millas de distancia de la zona de combate. En general, los hombres eran los que decidían si se debía disparar al objetivo y maniobrar el robot en el campo de batalla. El caso de SGR-A1 constituye toda una novedad, ya que tiene un modo automático, en el que se puede abrir fuego en el objetivo dado sin esperar a que el soldado humano valide la operación (Taddeo, 2012, p. 109).

El nuevo destructor DD(X) tendrá una sala de máquinas completamente controlada por sensores remotos y cámaras. O, para tomar otro ejemplo, considérese la evolución del bombardero de largo alcance desde el B-29, que tenía una tripulación de 11, hasta el B-2, que puede alcanzar muchos más objetivos, pero tiene una tripulación de solo dos, que pasan gran parte su tiempo supervisando las funciones del piloto automático (Boot, 2006, p. 23).

El teatro cíborg: modificación del cuerpo humano

Por otra parte, se ha llegado a interpretar la ciberguerra desde otro enfoque. El cuerpo humano está transformándose en una maquinaria de poder que lo explora, lo rompe y lo reorganiza. Una anatomía política, que es también una mecánica del poder, está naciendo, la cual define cómo se puede gobernar sobre los cuerpos de otros, no solo para que puedan hacer lo que se desea, sino para que puedan operar como se desea, con las técnicas, la velocidad y la eficiencia determinada (Masters, 2010). Una meta de larga data en la ingeniería es explotar los diseños únicos del cuerpo para guiar el desarrollo de apéndices artificiales antropomórficos que exhiben la estabilidad, la

fuerza y la velocidad de tipo humano en una variedad de entornos naturales (Herr, Whiteley y Childress, 2003, p. 103).

Los científicos empezaron trabajando y pensando en dos grandes oleadas de investigación innovadora: el trabajo en computación y procesamiento electrónico de datos y el trabajo en cibernética, en la ciencia del control y en la comunicación en animales y máquinas. El camino por seguir sería combinar enfoques cibernéticos y computacionales para crear híbridos hombre-máquina, sistemas artefacto-organismo, en los que los dispositivos electrónicos implantados usaran señales corporales de retroalimentación para regular automáticamente la vigilia, el metabolismo, la respiración, la frecuencia cardiaca y otras funciones fisiológicas en maneras convenidas a un cierto ambiente extranjero (Clark, 2015, p. 13).

En el contexto contemporáneo, el cuerpo humano sigue siendo un lugar clave para el injerto tecnológico en el Ejército. Hoy en día, la moneda básica de la guerra, el cuerpo humano, es el sitio de estas modificaciones, ya sea del *wetware* (la mente y las hormonas), el *software* (hábitos, habilidades, disciplinas) o el *hardware* (el cuerpo físico). Sin embargo, estos argumentos no captan completamente la reconfiguración del soldado cíborg del siglo xxi. Algunas modificaciones son necesarias para seguir, complicar y contextualizar las reconfiguraciones contemporáneas de la subjetividad dentro del ejército (Masters, 2010).

Los seres biológicos y los sistemas informáticos comparten algunas bases físicas comunes. La comunicación tanto en sistemas nerviosos biológicos como en sistemas informáticos, por ejemplo, depende de las señales eléctricas. Sin embargo, la brecha entre estas dos clases de sistemas es obvia. Gracias a los nuevos desarrollos en tecnologías de neuroimagen, como la resonancia magnética funcional, la magnetoencefalografía y la tomografía por emisión de positrones, la brecha ya no es insuperable. Estas tecnologías permiten observar, en niveles crecientes de resolución y fidelidad, el funcionamiento interno del cerebro y revelar su estructura y función. Además, el progreso en las interfaces cerebro-máquina en la última década ha hecho posibles vías de comunicación directa entre el cerebro y los sistemas artificiales en la señal. Estos nuevos desarrollos representan avances significativos en la inteligencia

cíborg. La inteligencia del cíborg intenta integrar estrecha y profundamente la inteligencia artificial con la inteligencia biológica, conectando los sistemas informáticos y sistemas biológicos, realzando fortalezas y compensando las debilidades de ambos al combinar las capacidades perceptivas y cognitivas de los sistemas biológicos con la energía computacional de los sistemas informáticos. En términos más generales, los cíborgs se refieren a sistemas simbióticos biológicos-mecánicos, compuestos por componentes tanto orgánicos como informáticos (Zeng y Wu, 2014, p. 3).

La palabra cíborg (del acrónimo en inglés *cyborg*: *cyber*, cibernético, y *organism*, organismo), es decir, organismo cibernético, se utiliza para designar una criatura compuesta por elementos orgánicos y dispositivos mecánicos para mejorar las capacidades biológicas a través de la tecnología. En otras palabras, es un individuo en parte hombre y en parte máquina (Mestres y Vives-Rego, 2016, p. 228).

El *Oxford English Dictionary*, por su parte, define el cíborg más explícitamente desde el punto de vista de aumento: como una persona cuyas tolerancias físicas o capacidades se extienden más allá de las limitaciones humanas normales por una máquina u otro dispositivo externo que modifica el funcionamiento del cuerpo, un sistema integrado hombre-máquina (Wittes y Chong, 2014, p. 9).

La cibernética ha dado el término cíborg, una unión de "organismo cibernético", que significa un organismo que es parte humano, parte máquina. Un cíborg es un individuo cuyas funciones biológicas son ayudadas o controladas por dispositivos tecnológicos, particularmente por implantes biónicos (Brey y Mitcham, 2005, p. 1529).

El término cíborg se ha definido como un ser humano cuyo funcionamiento fisiológico es mejorado por dispositivos mecánicos o electrónicos, una definición que parecía incluir individuos con cualquier número de implantes médicos en uso clínico común, tales como marcapasos cardiacos, pero el término usualmente se toma para involucrar mejoras más avanzadas, tales como prótesis neurales o implantes cerebrales (Doyle, 2014, p. 14).

En general, se usa el término *tecnología cíborg* para referirse a la tecnología integrada en el cuerpo humano que no solo restaura la función perdida, sino que realza las capacidades anatómicas,

fisiológicas y de procesamiento de la información del cuerpo (Barfield y Williams, 2017).

Manfred Clynes y Nathan S. Kline en 1960 usaron el término en referencia a un humano mejorado que podría sobrevivir en entornos extraterrestres. Llegaron a esa idea después de pensar sobre la necesidad de una relación más íntima entre los humanos y las máquinas en un momento en que empezaba a trazarse la nueva frontera representada por la exploración del espacio. Los creadores del término cíborg pensaban en un proceso de autoconstrucción y mejora humana, y no en un proceso de creación *de novo* total y externo al propio hombre (Mestres y Vives-Rego, 2012, p. 229).

El acrónimo cíborg representa el organismo cibernético u organismo cibernéticamente controlado; se trata de un término destinado a captar tanto la noción de fusión de la máquina humana como la naturaleza más bien específica de la fusión prevista. Los cibernéticos estaban en especial interesados en los sistemas autorreguladores. "Estos son sistemas en los que los resultados de la propia actividad del sistema se retroalimentan para aumentar, detener, iniciar o reducir la actividad según lo dicten las condiciones"[52] (Clark, 2003, p. 15).

Como máquina autorreguladora del hombre, el cíborg fue diseñado para proporcionar un sistema de organización en el cual los problemas, así como lo hacen los robots, sean solucionados de forma automática e inconsciente y dejen al hombre libre para explorar, crear, pensar y sentir. El cíborg es presentado como "la realización de una meta transhumanista concreta: el hombre liberado de las limitaciones estrictamente mecánicas de su organismo y las condiciones de su entorno por medio de la mecanización"[53] (Wittes y Chong, 2014, p. 6).

En los últimos años, se ha observado la aparición de la teoría del cíborg, o *ciborgología*, como el estudio multidisciplinario de los cíborgs y su representación en la cultura popular. Los estudios en la teoría del cíborg tienden a utilizar la noción del cíborg como metáfora

52 Traducción del autor.

53 Traducción del autor.

para entender aspectos de la relación de la sociedad contemporánea con la tecnología, así como del cuerpo humano y del ser humano en general. En esta teoría, la noción de cíborg se refiere a los organismos híbridos, a los seres humanos contemporáneos con prótesis o implantes, así como a los seres humanos (contemporáneos) en general, que se piensa que son cíborgs en el sentido de ser inherentemente dependientes de la tecnología, como también se destaca en las teorías protésicas de la tecnología (Brey y Mitcham, 2005, p. 1531).

> En primer lugar, consideramos que la vestimenta debe incorporarse como un primer criterio de "cyborización" bajo la consideración de que constituye un elemento de mejoramiento que desde hace miles de años ha permitido al hombre adaptarse a diversos ambientes. Son particularmente evidentes los casos de vestimenta técnica en el ejército o en el mundo del deporte, donde protege del clima, de los accidentes o de las acciones agresivas de humanos u otros animales. De hecho, los trajes protectores y el concepto de esqueleto externo o exosqueleto en los humanos actuales son una versión moderna de las armaduras clásicas que asumieron funciones de protección. Por otra parte, la idea de un esqueleto externo para acarrear cargas pesadas o para personas tetrapléjicas es relativamente reciente, y sus orígenes se remontan al "Hardiman" de 1966, construido por el ingeniero Ralph Mosher, que trabajaba para la empresa General Electric, aunque esa forma primitiva no fue exitosa, debido a su peso y a la brusquedad de sus movimientos. (Mestres y Vives-Rego, 2012, p. 230)

La definición del cíborg puede ser sostenida por una clasificación basada en el criterio de propósito o aplicación. En un grupo, están los cíborgs encargados de compensar cierta deficiencia física. Estos son predominantemente cíborgs médicos. En la vida real, abundan los seres humanos que se convirtieron en cíborgs por razones médicas. El segundo grupo consiste en seres humanos que han incorporado las partes mecánicas para realzar su potencial corporal. Estos son llamados cíborgs experimentales. Las desventajas físicas no los han obligado a aceptar elementos inorgánicos dentro de su organismo. Ellos han optado por hacerlo con fines de experimento científico o en forma de

presentaciones artísticas, pero principalmente para ilustrar las implicaciones éticas o políticas de este acto (Glavanakova, 2006).

Las capacidades de la "tecnología cíborg" tienen varias características: 1) la tecnología es actualizable, lo que permite que las mejoras de *software* y *hardware* sean aplicables al cuerpo en ciclos de tiempo cada vez más cortos; 2) la tecnología ofrece al cuerpo capacidades computacionales adicionales, con lo que lo transforma en una tecnología de procesamiento de información; 3) la tecnología cíborg se integra con el cuerpo mediante sistemas de realimentación, y 4) es cada vez más controlable por el pensamiento. Si estas tendencias de la innovación y la investigación continúan, pronto será posible encontrar un tipo nuevo de humano con capacidades muy diferentes (Barfield y Williams, 2017).

La fusión de lo humano con lo tecnológico, que ahora es un hecho social que cobra cada vez más ímpetu, forma parte de visiones distópicas del futuro lejano y no tan lejano, así como una resistencia a la dominación de la información. Esta tecnoansiedad, asociada al mal uso de las máquinas con fines de coerción, dominación y vigilancia de los seres humanos, resurge como tema central en el debate sobre el destino de la ciudadanía. El grado de control sobre los seres humanos mediante el empleo de tecnologías digitales es más notable en dos figuras: los militares y los cíborgs de vigilancia. La guerra posmoderna está fuertemente influenciada por la tecnociencia y depende de los cíborgs. Ahora los militares estadounidenses producen continuamente soldados más fuertes y más eficientes mediante el uso de instrumentos mecánicos y digitales (Glavanakova, 2006).

Recientes áreas de investigación de inteligencia cíborg han incluido los siguientes temas:

- Animales como sensores y actores.
- Máquinas controladas por la mente.
- Neurochips, chips diseñados para conectarse a células neuronales; por ejemplo, chips de memoria para reemplazar la corteza de memoria para su restauración y mejora.

- Prótesis inteligentes, dispositivos que reemplazan una parte del cuerpo perdida o dañada usando el sistema nervioso humano y la interfaz del cerebro para aumentar la precisión y lograr la comodidad de los movimientos.
- Neuromorfos, sistemas de *software* análogos, digitales y mixtos que implementan modelos de sistemas neuronales (como la percepción, el control motor y la integración multisensorial).
- Cognición simbiótica, integración de funciones cognitivas biológicas con modelos computacionales de cognición (Zeng y Wu, 2014, p. 3).

Las tecnologías cíborg se pueden dividir en cinco categorías: tecnologías que interfieren externamente con el cuerpo, implantes dentro del cuerpo, tecnología que modifica las actividades cerebrales, tecnología informática que mejora la calidad de vida y exoesqueletos (Barfield y Williams, 2017).

Las mejoras externas generales al organismo incluyen las prótesis para reemplazar o restaurar funciones perdidas, las cuales son cada vez más controlables mediante el uso de principios de la teoría de control, y están integralmente conectadas al cuerpo, son actualizables y, bajo ciertas circunstancias, controladas por el pensamiento a través de una interfaz cerebro-computadora. Y por otro lado, se encuentran los accesorios de computación como mejora, ya que, al incrementar los recursos computacionales a través de la tecnología directamente integrada con el cuerpo, permiten escalar capacidades, sentidos e interacción con el entorno y con tecnología externa. En la medida en que la computación portátil se integra con los sentidos y responde a los pensamientos, representa un movimiento significativo hacia convertirse en un cíborg (Barfield y Williams, 2017).

En segundo lugar, se encuentran las tecnologías de mejora implantada dentro del cuerpo de tres tipos. El implante pasivo cíborg, si bien no puede interactuar con el cuerpo a través de un bucle de retroalimentación, puede ser llevado en el cuerpo, o recolectando o almacenando información. Los implantes activos o sensores sí cuentan con realimentación en circuito cerrado, junto con capacidades computacionales que proporcionan información médica, interacción tecnológica y

entrada extrasensorial. Y la interfaz con el sistema nervioso está completamente integrada con el cuerpo y proporciona mayores niveles de integración con el usuario. A través de dicha integración, los circuitos de retroalimentación que sus sistemas crean pueden considerarse extensiones artificiales del cuerpo (Barfield y Williams, 2017).

Como tercera categoría, se encuentran las mejoras o modificaciones del cerebro. En el neurocontrol, se hace referencia a interfaces con menor especificidad, en general usadas para suprimir grandes grupos neuronales afectados por alguna enfermedad. En la lectura de la mente, la actividad de la neurona se mide por primera vez, luego se traduce por una computadora y finalmente se envía como una forma de salida. Por último, las tecnologías que influyen en la memoria pueden crear y desmantelar la identidad, así como curar enfermedades degenerativas, ayudar en el aprendizaje y ampliar las bases de conocimiento (Barfield y Williams, 2017).

Las últimas clases incluyen exoesqueletos y ayudas a la movilidad. Las prótesis de función aumentada, si bien no están técnicamente separadas en la clasificación cíborg de las prótesis normales, tienden a ser menos antropomórficas, tienen funciones de control del pensamiento y especificaciones de diseño destinadas a mejorar ciertas habilidades, y los exoesqueletos están diseñados alrededor de las extremidades existentes para aumentar la movilidad. Estas mejoras pueden aumentar considerablemente las capacidades naturales o restaurar la funcionalidad perdida. Todos son sistemas de retroalimentación de circuito cerrado con el cuerpo y, además, los exoesqueletos poderosos contienen sistemas computacionales que aumentan su nivel de mejora (Barfield y Williams, 2017).

El soldado de tierra cíborg del siglo xxi estará equipado con tecnologías que en esencia reemplazan sus sentidos a través de prótesis tecnológicas que replican los sentidos biológicos mientras evitan las limitaciones biológicas humanas: visión, oído y discernimiento deficiente. Su casco estará equipado con micrófonos y auriculares para la comunicación, gafas de visión nocturna y sensores de imagen térmica para ver en la oscuridad, junto con una pantalla de avisos delante de sus ojos para mostrarle dónde está en el suelo y darle constantes actualizaciones sobre inteligencia.

La DARPA (Defense Advanced Research Projects Agency 'Agencia de Proyectos de Investigación Avanzados de Defensa') también está desarrollando tecnología que puede regular las emociones al enlazar directamente al sentido y controlar remotamente el desempeño de un soldado; se podrían eliminar sentimientos de miedo, vergüenza o agotamiento. Lo que una vez se consiguió al enviar soldados con anfetaminas ahora se puede hacer a distancia con mayor precisión. Con tales desarrollos, los "ojos" y "oídos" de los militares ya no serían susceptibles al error humano y a la emoción, porque las computadoras no están a merced de las funciones corporales, incluso mientras no funcionan sin la presencia de los seres humanos. Los programadores informáticos que manejan computadoras siempre pueden ser reemplazados con relativa facilidad y sin interrumpir sus capacidades. Además, la computadora recomienda los objetivos que deben ser atacados e, incluso, vigila los cielos desde lejos (Masters, 2010).

El cibersoldado 2030 propone elementos ergogénicos y monitorización que pueden ser proporcionados por la corriente del cíborg y harán al combatiente mucho más eficiente, como lo son:

- El exoesqueleto integrado basado en la nanotecnología: velocidad, fuerza y agilidad mejoradas.
- Potenciadores cognitivos (nutricionales, nootrópicos u otros fármacos inteligentes).
- Mejoradores físicos (nutricionales, farmacéuticos).
- Prótesis neurales (ahora controvertidas, pero quizá omnipresentes en 2030).
- Comportamiento neural.
- Análisis interno (detección de oxigenación sanguínea y glucosa).
- Un modelo predictivo individual del desempeño en función de variables de estado (Casey, 2009, p. 4).

El cíborg se puede leer fundamentalmente como poshumano y representa significativamente una profunda rearticulación de lo político; en

otras palabras, la constitución del soldado cíborg se puede leer como una rearticulación radical de la subjetividad humana. Esta subjetividad poshumana está representada a través del cíborg en los procesos mismos de transferir el razonamiento humano y el pensamiento de sujetos humanos a la tecnología (Masters, 2010). La fusión de la tecnología con la capacidad de razonar y pensar, sin ser interrumpido por emociones como la culpa o las limitaciones corporales como la fatiga, es indicativo de la constitución del cuerpo carnoso como incapaz de producir y proyectar los requerimientos deseados.

En la neurociencia, ha habido experimentos espectaculares en los últimos años que están rompiendo los esquemas de los cíborgs en la ciencia ficción. Por ejemplo, los sistemas BCI (*brain-computer interface* 'interconexión cerebro-ordenador') se empezaron a experimentar en la Universidad de California en la década de 1970. Estos consisten en una comunicación por cableado entre el cerebro y una computadora externa que permite la interacción biyectiva. Con esta conexión, se podría modificar las imágenes-datos que se ven en la computadora, y viceversa, a partir de instrucciones a esta para poder cambiar funciones motoras, sensitivas y emocionales (Mestres y Vives-Rego, 2012, p. 232).

Kevin Warwick puede ser la persona más conocida al unir estos dos mundos. El 24 de agosto de 1998 fue objeto del experimento Cyborg 1.0, donde se le implantó debajo de la piel un chip RFID (*radio frequency identification*) con el cual fue capaz de controlar puertas, luces, calentadores y computadoras solo con la señal emitida por el chip. Un segundo experimento fue el Cyborg 2.0, realizado el 14 de marzo de 2002. Un chip de mayor complejidad fue implantado en el sistema nervioso de Warwick por medio del cual fue capaz de mover una mano cibernética utilizando la interfaz neuronal. Además, se le implantó también a su esposa un microchip, con el objetivo de crear alguna clase de telepatía o empatía, lo que permitió la primera comunicación puramente electrónica entre dos sistemas nerviosos humanos (Mestres y Vives-Rego, 2012, p. 233).

El estadounidense Michael Chorost, nacido en 1964, tenía graves pérdidas auditivas debido a la rubeola. Su audición fue parcialmente restaurada con un implante coclear y se "convirtió" en un cíborg el 1 de octubre de 2001. Posteriormente, escribió una memoria de la

experiencia titulada *Rebuilt: How Becoming Part Computer Made Me More Human* ('Reconstruido: Cómo convertirme en parte computadora me hizo más humano'). Allí describe cómo su cuerpo se volvió desconcertantemente mecánico, pues su audición está rutinariamente actualizada con un nuevo *software* (Glavanakova, 2006).

Un reciente ejemplo de un cíborg militar es un anuncio publicado en los sitios web del Gobierno estadounidense por la DARPA, en el que se afirma que está en busca de propuestas innovadoras a fin de desarrollar tecnología para crear cíborgs de insectos, mediante la implantación de pequeños dispositivos en sus cuerpos. El objetivo era crear tecnología que pudiera lograr la llegada de un insecto a menos de 5 m de un objetivo específico utilizando control remoto electrónico o GPS (*global positioning system* 'sistema de posicionamiento global'). Agregado a esto, el insecto debía permanecer inmóvil indefinidamente o hasta que se instruyera de otra manera y también debía ser capaz de transmitir datos de los sensores pertinentes del DoD que incluyen sensores de gas, micrófonos, video, etc. (Glavanakova, 2006).

Ejemplos de prótesis pueden ser DEKA Arm, un brazo controlado por el cerebro, un telescopio implantado en miniatura para el tratamiento de la DMAE (degeneración macular asociada a la edad), el Argus II Retinal Prosthesis System, un dispositivo implantado para tratar a adultos con retinitis pigmentosa grave y el MED-EL's Synchrony, implante coclear. Entre los accesorios tecnológicos, ahora es posible encontrarse USB (*universal serial bus* 'conexión de serie universal') como reemplazos de prótesis de dedos (USB Fingertip), una cámara que se lleva delante del ojo para grabar la escena disponible a la vista junto con una pantalla para superponer imágenes generadas por computadora en la escena original disponible (EyeTap); las Google Glass, un aparato diseñado para percibir los colores mediante ondas sonoras en tiempo real (*eyeborg*); y un monitor sobre la piel, capaz de dar al hombre una sensación constante de ubicación (Barfield y Williams, 2017).

En cuanto a tecnologías implantadas, se encuentran los chips RFID (*radio frequency identification* 'identificación por radiofrecuencia'), una tecnología inalámbrica capaz de identificar automáticamente, transferir datos de una etiqueta electrónica a través de un lector con

el propósito de rastrear a la persona y guardar su información vital (Ajami y Rajabzadeh, 2013, p. 809).

También se incluyen monitores de marcapasos y desfibriladores cardiacos para una función cardiaca correcta, estimuladores de nervios que interactúan entre el sistema inmunológico y el nervioso para tratar una amplia gama de enfermedades relacionadas con la inflamación, desde la diabetes hasta la insuficiencia cardiaca congestiva. Los sensores implantables miden y transmiten los niveles de glucosa; el Circadia de Tim Cannon mide la temperatura; el sensor sísmico de Moon Ribas vibra para predecir los terremotos; la implantación de micrófonos y altavoces en los dientes; un controlador inalámbrico activado por el cerebro; la investigación de Kevin Warwick le permitió controlar un brazo robot y crear una sensación nerviosa artificial, entre otras (Barfield y Williams, 2017).

Respecto de temas de manejo e influencia en el cerebro, ya hay avances importantes. Theodore Berger, ingeniero biomédico y neurocientífico de la Universidad del Sur de California en Los Ángeles, ha diseñado chips de silicio para imitar el procesamiento de las señales que hacen las neuronas interrumpidas tras haber sufridos daños por alzhéimer, accidentes cerebrovasculares o lesiones, cuando funcionan correctamente, que permiten recordar experiencias y conocimientos (Cohen, 2013).

La DARPA ha reconocido la TBI (*traumatic brain injury* 'lesión cerebral traumática') como una causa grave de discapacidad en los Estados Unidos. Se ha diagnosticado a más de 270 000 miembros del servicio militar desde 2000 y ha afectado a un estimado de 1.7 millones de civiles estadounidenses cada año. La TBI frecuentemente resulta en una capacidad deteriorada para recuperar recuerdos formados antes de la lesión y una capacidad reducida para formar o retener nuevos recuerdos después de ella. Actualmente, existen pocas terapias eficaces para mitigar las consecuencias a largo plazo en la memoria. A través de la RAM (Restoring Active Memory), la DARPA busca acelerar el desarrollo de una tecnología capaz de abordar este desafío de salud pública y ayudar a los miembros de los servicios y otros a superar los déficits de memoria mediante el desarrollo de nuevas neuroprótesis para cerrar las brechas en el cerebro lesionado. El objetivo final de la

RAM es desarrollar y probar un dispositivo médico de interfaz neuronal totalmente implantable para el uso clínico humano. La DARPA apoya el desarrollo de modelos computacionales de múltiples escalas con alta resolución espacial y temporal que describen cómo las neuronas codifican los recuerdos declarativos. Los investigadores también explorarán nuevos métodos para el análisis y la decodificación de señales neurales a fin de entender cómo la estimulación dirigida podría ser aplicada para ayudar al cerebro a restablecer una capacidad para codificar nuevos recuerdos después de una lesión cerebral (Sánchez, 2017).

El desarrollo cíborg ha llegado hasta el punto del manejo de algunos aspectos cerebrales. Los neurocientíficos del Massachusetts Institute of Technology (MIT) han demostrado que pueden plantar falsos recuerdos en el cerebro de los ratones y encontraron que muchos de los rastros neurológicos de estos recuerdos son idénticos en naturaleza a los de memorias auténticas. El estudio también proporciona pruebas adicionales de que los recuerdos se almacenan en redes de neuronas que forman rastros de memoria para cada experiencia y muestra que se podía identificar las células que forman parte de un engrama (recuerdos) para una memoria específica y reactivarla usando una tecnología llamada optogenética (Trafton, 2013).

Biomechatronics de Hugh Herr ha desarrollado prótesis de rodilla adaptativas para amputados transfemorales y órtesis de tobillo-pie de impedancia variable para pacientes que sufren la pérdida de sus pies, patología de la marcha causada por accidente cerebrovascular, parálisis cerebral y esclerosis múltiple. También ha diseñado sus propias extremidades biónicas, como la primera pierna biónica del mundo, llamada BiOM® Ankle Foot System. Esta ha demostrado clínicamente ser la primera prótesis de pierna que logró la normalización biomecánica y fisiológica y permitió a las personas con amputación de piernas caminar con los niveles normales de velocidad y metabolismo como si las piernas fueran biológicas de nuevo (MIT Media Lab People, s. f.).

California suitX está encaminado en conquistar la industria del exoesqueleto. No solo la compañía ha desarrollado su exoesqueleto Phoenix, que es el menos caro y más ligero entre los exoesqueletos médicos disponibles, sino que suitX también ganó el premio de USD 1 millón

en AI & Robotics for Good de los Emiratos Árabes Unidos con su propuesta para un exoesqueleto médico pediátrico, y superó a otras 659 entradas en la categoría internacional del evento. suitX fue fundada por Homayoon Kazerooni, quien tiene más de treinta años de experiencia en ingeniería mecánica y un doctorado del MIT. De hecho, Kazerooni, incluso, fue cofundador de Ekso Bionics (Talking Exoskeletons with suitX Founder Dr. Homayoon Kazerooni, 2016).

Los cuatro teatros donde se desarrolla la ciberguerra, todos ellos expuestos para facilitar su comprensión, son una clara muestra sobre varias cosas: en primer lugar, que la ciberguerra y el ciberespacio ya han permeado todos los sectores de la vida política, económica, militar, social y cultural a nivel internacional; pues, si bien hay lugares con mayor penetración que otros, una gran parte de los procesos humanos ahora dependen de las conexiones a internet, que, si bien han facilitado la vida de muchos individuos, también han abierto caminos para aprovechar las vulnerabilidades que se crean.

Y en segundo lugar, los tipos de ciberguerra demuestran que esta no es una sola a la que el ciberespacio le otorga la cualidad de transformarse y adaptarse a la necesidad del atacante y a las debilidades del adversario, que, si se tiene el dinero, la voluntad de los dirigentes o líderes y la información, la ciberguerra se convierte en una oportunidad de un gran valor para cualquiera que tenga un interés, una herramienta y conocimientos cibernéticos y ciberespaciales.

Capítulo V
La "ciberguerra irregular": guerra en red y nuevos actores

Se han desarrollado procesos de transformación organizacional que se han desatado en los Estados nación, y sus sociedades, a partir del desmantelamiento de la bipolaridad política y en materia de defensa y seguridad nacional que se planteó durante la Guerra Fría. Uno de los fenómenos más representativos e influyentes para entender las dimensiones bélicas adquiridas por las tecnologías informáticas es, sin duda, la transformación en la naturaleza de la guerra a partir de la década de los cincuenta (Münkler, 2005).

La guerra se ha transformado. El enfrentamiento de los Estados nación que fue el núcleo básico de la guerra moderna es cada vez menos frecuente. Ahora, la seguridad estatal se ve amenazada por una inusitada diversidad de enemigos. Asimismo, los objetivos de los conflictos ya no se desarrollan solo por diferencias políticas, sino también por diferencias étnicas, religiosas y económicas, entre otras (Fojón, 2006).

Los esfuerzos conceptuales para entender el cambio en el carácter de la guerra se configuran a partir de la crisis del paradigma fundacional de la política moderna: el Estado nación. Precisamente, este es el argumento central de Van Creveld (1991) para explicar la transformación de la guerra. A este planteamiento se suman Kaldor (1998), con su concepto de nuevas guerras; Lind, Nightengale, Schmitt, Sutton y

Wilson (1989) y las guerras de cuarta generación; y Toffler y Toffler (1994), con las olas de la guerra, entre muchos otros que articulan sus planteamientos a la idea de que el Estado ha cedido terreno a favor de múltiples actores emergentes que le compiten para obtener sus intereses particulares: "La guerra de cuarta generación marca la más radical transformación desde la paz de Westfalia. En la cuarta generación de la guerra, los Estados pierden su monopolio de la guerra"[54] (Lind, 2004).

La guerra en red

La *netwar* se ubica cada vez más "en el extremo social del espectro donde el lenguaje ha sido normalmente sobre conflictos de baja intensidad, operaciones distintas de la guerra y modos no militares de conflicto y delincuencia"[55] (Arquilla, Ronfeldt y Zanini, 2000, p. 81). Uno de los actores que han emergido con fuerza en este nuevo escenario son las organizaciones terroristas. Si bien el terror se ha empleado a lo largo de la historia, es a partir de la mitad del siglo xx cuando este elemento se comienza a usar como forma de acción política (Laqueur, 1987).

Para entender la relación que presentan los actores no estatales en estos conflictos con las tecnologías informáticas, debe establecerse como punto de partida que:

1. La materialización de esta concomitancia fue un proceso equidistante en el tiempo, que ha venido perfeccionando los cuerpos militares constitucionales del Estado nación desde la revolución de los asuntos militares de la década de 1990.

2. A partir del planteamiento de Lind acerca de la desventaja que enfrenta el Estado respecto de las amenazas, se debe expresar que la revolución de la información ha sido capitalizada por todo tipo de organizaciones tanto legales como ilegales.

54 Traducción del autor.

55 Traducción del autor.

Para comprender este contexto, Arquilla y Ronfeldt (2001) exponen que la revolución de la información está alterando la naturaleza del conflicto en todo su espectro. Se llama la atención sobre que la revolución favorece y fortalece las formas de organización en red, lo que a menudo les otorga una ventaja sobre las formas de organización jerárquicas. El auge de las redes ha determinado que se dé una migración del poder a los actores no estatales, ya que están siendo capaces de organizarse de manera rápida en extensas *redes multiorganizacionales* (en especial bajo la forma de organización en red denominada All-Channel, en la cual todos los nodos se conectan con todos los nodos a la vez), a diferencia de las estructuras jerárquicas de los actores estatales. Esto significa que los conflictos cada vez más pueden ser llevados a cabo por redes, quizá más que por jerarquías. También significa que aquel que domine las formas de red se beneficiará de la ventaja (p. 1).

A partir de lo anterior, es posible afirmar que las organizaciones que consolidan sus estructuras en forma de red desarrollan tres características básicas, como lo plantean Zanini y Edwards (2001). En primer lugar, la comunicación no se desarrolla a través de intercambios de información en relaciones jerarquizadas, sino que fluye dentro de una red que se adapta al objetivo por alcanzar. En segundo, las conexiones internas de una red particular se vinculan con individuos externos a la organización y amplían el radio de impacto de la comunicación.

La tercera característica se relaciona con la flexibilidad de las relaciones de la red. Estas relaciones no se encuentran erigidas sobre imposiciones burocráticas, sino por valores y normas compartidos; por ejemplo, la confianza mutua. De esto se deriva que la organización interna se rige según la autogestión de grupos, mientras que la externa se determina mediante la confluencia de esfuerzos y aportes de una gran diversidad de componentes y "empresas" (Edwards y Zanini, 2001). De este ámbito, emerge el concepto de *netwar* o de guerra en red:

> Para ser precisos, la guerra en red se refiere a un modo emergente de conflicto (y crimen) en los niveles de la sociedad en ausencia de la guerra militar tradicional, y donde sus protagonistas se

> configuran en formas de red mediante la integración de sus doctrinas, estrategias y tecnologías en sintonía con la era informacional. Estos protagonistas prefieren configurarse en organizaciones dispersas, pequeños grupos e individuos que se comunican, coordinan y conducen sus campañas bajo la lógica de internet, y a menudo sin un mando central definido […]. Así, por ejemplo, la guerra en red se trata más de los Zapatistas que de los Fidelistas, de Hammas que de la Organización para la Liberación de Palestina (OLP)[56]. (Arquilla y Ronfeldt, 2001, p. 6).

El ciberterrorismo

En efecto, Mayntz (2004) construye un vínculo entre los grupos terroristas y su capacidad de organización en redes, para denotar la cercanía que se configura de conceptos más cercanos a la transnacionalización que a la internacionalización. Por esto, grupos terroristas como Al Qaeda o las organizaciones palestinas se diferencian de aquellas como la Fracción del Ejército Rojo Alemán o las Brigadas Rojas Italianas, que, en su momento de aparición, durante la Guerra Fría, no contaron aún con el andamiaje global de comunicación informática que explotan los primeros con eficiencia. En ese sentido, se puede indicar cómo las organizaciones terroristas presentan una reconfiguración en su capacidad de extensión y actuación geográfica como resultado de las formas de organización en red y su sustento en las tecnologías informáticas. De esta manera, acciones y capacidades como atacar objetivos en otros países con el propósito de promover los principios de la organización, desarrollar formas reducidas de militancia internacional con el fin de consolidar redes de apoyo para la recolección de fondos y otro tipo de recursos para la organización permitieron que los terroristas se ubicaran incipientemente en un espacio extrafronterizo. Ahora, mediante la organización en forma de red y el empleo de las tecnologías de la información, las organizaciones de este orden no solo potencian los logros alcanzados, sino que adquieren connotaciones trasnacionales para su accionar (Enders y Sandler, 2000).

56 Traducción del autor.

No en vano, bajo este nuevo marco, los grupos terroristas, gracias a las nuevas formas de interacción, tienden a hacerse compatibles. Así, al integrarse los esfuerzos de redes terroristas de diversos países simultáneamente, se puede dar paso a la concepción del terrorismo internacional (Mayntz, 2004). Además de los factores de comunicación y coordinación, la revolución informática también cobra suma relevancia para las organizaciones terroristas. Sin embargo, por su ilegalidad y asimetría con el Estado, estas no desarrollan operaciones de información, debido a que no cuentan con la infraestructura necesaria.

No obstante, no se puede obviar que estas organizaciones han consolidado un *modus operandi* informático, el cual intenta imitar los sistemas de procesamiento y transmisión de las fuerzas militares, tal como lo evidencia Zanini (1999) en sus estudios acerca de los grupos terroristas africanos como el Armed Islamic Group (GIA).

En consecuencia, durante la década de 1990, el terrorismo realizó su primer contacto con las computadoras y la comunicación a través de internet. Como lo establece Jain (2005), es un tipo de violencia premeditada y políticamente motivada y perpetrada contra objetivos no combatientes, por grupos subnacionales o agentes clandestinos, a través de los programas informáticos y los mecanismos de transferencia de datos como internet. Por tanto, los malintencionados actos cometidos a través de la red, tales como pornografía infantil, correos electrónicos con información dañina para los sistemas, colgar contenido ofensivo y el robo de información bancaria, hacen parte de estas acciones.

En los conflictos contemporáneos, las amenazas se multiplican, así como los actores. Los Estados nación dejaron de ser los únicos responsables de conflictos armados. Los nuevos actores ocuparon este rol, unos que, en palabras de Lind (2004b), pertenecen a la guerra de cuarta generación, o las *nuevas guerras* de Kaldor (1998), o a las guerras de la tercera ola que conceptualizaron Toffler y Toffler (1994).

La diversificación de los actores ilegales, así como de sus objetivos, ha determinado una nueva asimetría. Se han multiplicado las campañas contraestatales o contrainstitucionales que emplean el terrorismo cibernético como una de sus tantas formas de lucha. En la década de 1990, aún no se percibía que estos dispositivos representaban una nueva clase de armamento que se encontraba al alcance de los terroristas

(Lewis, 2002). Antes de contar con estas tecnologías, los medios de comunicación limitaban la información relacionada con el accionar de su organización.

El ciberespacio posibilitó el crecimiento exponencial de la información de diversos temas que no se encontraban en las agendas de los medios de comunicación. Los efectos mediáticos de internet son abrumadores. Su capacidad de acceso y la democratización de la información permitieron eliminar una serie de intermediarios entre el emisor y el receptor de los mensajes (Sierra, 2002). Tan solo basta contar con una computadora para expresarse abiertamente y de esta forma expandir el universo de datos disponible.

Estas organizaciones ya no dependen de la difusión de sus acciones por los medios de comunicación tradicionales para que el objetivo psicológico del terrorismo se cumpla. Internet ha multiplicado exponencialmente su auditorio y, por ende, el impacto de las acciones de los terroristas. Este hecho es relevante para comprender cómo estos grupos se han adaptado a una sociedad interconectada digitalmente para cumplir con sus objetivos.

Las organizaciones terroristas han crecido fértilmente en el ciberespacio. Sus ataques se han convertido en una amenaza crítica para los Estados. Su mensaje llega a más personas y su capacidad de causar daño se multiplica (Green, 2002). Los terroristas, que usan este tipo de herramientas tecnológicas, forman organizaciones con alcance global. John Arquilla, David Ronfeldt y la RAND Corporation han llamado a este fenómeno la guerra en red o *netwar*.

Siguiendo los principios de la guerra en red, el terrorismo y sus estructuras organizacionales se configuran como células o pequeñas unidades dispersas por el teatro de guerra (el cual, conforme los fines terroristas y políticos de la organización en cuestión, puede ser global —Al Qaeda—, regional —Hamás— o nacional —ETA[57] o EZLN[58]—) con la capacidad de interconectarse efectivamente para coordinar de su accionar (Arquilla y Rondfeldt, 2001). Parte de lo anterior se puede

57 Euskadi Ta Askatasuna.

58 Ejército Zapatista de Liberación Nacional.

observar en la facultad de generar ataques cibernéticos. Los terroristas desarrollan diversidad de apoyos y capacidades que aportan para la realización de los objetivos que estos grupos establecen en sus conflictos. Atraen nuevos integrantes, obtienen presupuesto y difunden su mensaje a todos los rincones del planeta (Sánchez, 2008).

El terrorista ha consolidado medios de reclutamiento, de financiación, de guerra política, de comunicación y coordinación, de entrenamiento y adoctrinamiento en el ciberespacio (Joshi, 2000). El ciberterrorismo, si bien se presenta como una amenaza mediante la cual un actor propio de esta categoría puede desarrollar un ataque cibernético a un Estado enemigo, al traducirse, a su vez, a una forma en la cual el terrorista emplea el ciberespacio para mejorar sus capacidades de organización, claramente se ha encontrado, a través de esta dimensión, una forma de sopesar la asimetría que lo describe frente a las fuerzas oficiales que lo combaten (Wolthusen, 2003).

El ciberterrorismo es un fenómeno que hace presencia en los conflictos armados contemporáneos. La globalización de las tecnologías informáticas a partir de la década de 1990, sus bajos costos y fácil acceso en los mercados comerciales, permite que las organizaciones terroristas se valgan del ciberespacio para sopesar las desventajas propias de la asimetría del conflicto.

En la historia, las agrupaciones subversivas que emplean el terrorismo como estrategia para apoyar sus guerras y alcanzar sus objetivos políticos han detectado como una herramienta fundamental para su accionar los medios de comunicación masiva. Siguiendo el recorrido del terrorismo a lo largo de los años, es posible observar cómo este fenómeno se vale de medios como la radio, la prensa y la televisión para difundir la consumación de hechos fastuosos en pro de radicar el miedo en distintas sociedades como mecanismo de presión política hacia las instancias gubernamentales que pueden cumplir sus demandas.

El escenario y la lógica que trae consigo la implementación de las tecnologías informáticas y el ciberespacio han logrado dar un giro importante en el *modus operandi* de estos actores. En primera instancia, porque, a diferencia de los medios de comunicación precedentes, el terrorista ya no depende de que las cadenas de noticias decidan captar sus actos de agresión ni de qué es divulgado de todo lo que sucede.

Por otra parte, este no ha sido el único rédito que los terroristas logran obtener del ciberespacio. Debido a las bondades ya expresadas, estos actores de los conflictos asimétricos pueden establecer mecanismos de coordinación de sus operaciones de manera globalizada, han construido sitios en el ciberespacio donde generan mecanismos de guerra política contra la institucionalidad, constituyen medios para que los partidarios de sus causas hagan donativos mediante dinero electrónico, reclutan y entrenan a sus integrantes. En síntesis, usan herramientas que permiten sopesar su asimetría frente a la contraparte.

De hecho, debe decirse que el ciberterrorismo se ha configurado en mayor medida como el empleo del ciberespacio para potenciar actividades logísticas, propaganda y coordinación de las organizaciones terroristas, diferenciándose de los ataques cibernéticos en la mayoría de los casos. No obstante, los desarrollos tecnológicos, en especial los relacionados con internet y otras tecnologías de la información, han repercutido en especial en las estructuras organizacionales del terrorismo, cuyo modelo clásico, altamente jerarquizado y centralizado, "se sustituye hoy por esquemas en red, sumamente flexibles y descentralizados, lo que lleva a los Estados a tomar medidas contra los riesgos de la coexistencia de los terroristas en el ciberespacio" (Molano, 2009, p. 24).

En consecuencia, cuando se retoma teóricamente el fenómeno del ciberterrorismo, es posible establecer que esta cara del terrorismo se fundamenta, por una parte, como medio logístico para potenciar las prácticas tradicionales de la agrupación al trasladarlas al ciberespacio mediante el empleo de las tecnologías informáticas. Y, en segundo lugar, como un medio estratégico operacional y táctico para llevar a cabo ataques directos a los Estados, sus infraestructuras críticas y su población.

De acuerdo con lo anterior, el propósito es tomar como referencia de análisis los elementos más significativos del fenómeno del ciberterrorismo. En primera medida, la incidencia comunicacional que trajo consigo el ciberespacio para los terroristas y, posteriormente, las nuevas capacidades adquiridas por estos actores en esta misma dimensión, claro está, mediante el empleo de las tecnologías informáticas.

Finalmente, se advierte que este capítulo parte de la premisa de la organización en red, que fue observada en el primer capítulo del libro. Del mismo modo en el que la ciberguerra se ha consolidado como una nueva generación de lo que fue la guerra informática, el ciberterrorismo inicia su camino de desarrollo cuando los grupos terroristas generan esa primera armonía con las tecnologías como un medio para organizarse de tal manera que superaran la asimetría en la guerra.

Guarín (2009) menciona el principio de que la acción política, cualquiera que sea su signo ideológico, "busca la captación de los ciudadanos para acceder al poder, influenciarlo o ejercerlo […]. Acudiendo a mensajes, símbolos y actos con contenido político se consigue el consentimiento ciudadano, o bien la coacción, ambas caras del poder político" (p. 118).

La lógica del terrorismo, y tal vez con más rigor que otras formas de expresión política, se ha tenido que acoplar a este canon. Una de las definiciones más completas de terrorismo la ofrece Andrés Molano Rojas, abogado experto en temas de seguridad y defensa. Según Molano (2009), el terrorismo es un método de acción política violenta que tiende a articularse en procesos de larga duración, para compensar asimetrías en el contexto de un conflicto, que opera provocando una destrucción o caos suntuario, según un modelo eminentemente transitivo, cuyo efecto psicológico es superior a sus efectos materiales (por cuanto elige objetivos con alto valor histórico), a efectos de transmitir un mensaje para afectar grandes audiencias, cuyos agentes impulsan principalmente determinadas pretensiones políticas (p. 105).

Los anteriores hechos se sustentan, como lo expresa Guarín (2009), en que la relación específica entre los grupos terroristas y los medios de comunicación ha sido connatural a su nacimiento y su naturaleza. La prioridad del terrorista está en el pensamiento y este se crea a partir de la información que los ciudadanos reciben por parte de los medios de comunicación. Si se examina con cuidado, se identifica que la comunicación es el hilo conductor de la lógica terrorista. No sirve de nada cometer el atentado y mucho menos amenazar con su realización si la población no llega a conocer ni lo uno ni lo otro. La eficacia del empleo de la violencia en este caso depende de que el mayor número de personas conozca el hecho. Así, sin medios de comunicación, no existe la cadena de consecuencias buscada por los terroristas (p. 120).

Claramente, cuando se analiza el escenario en el cual los grupos de esta naturaleza trascienden a emplear medios de comunicación mucho más poderosos que la radio, la prensa y la televisión, como lo es de manera evidente el ciberespacio, los resultados propios de la interacción entre el *fenómeno* y el *canal* logran sobrepasar sus propias fronteras (Castells, 2004).

Al retomar a Ortiz (1996), los factores que hicieron del ciberespacio una verdadera revolución para los conflictos armados, y en especial para actores propios como los grupos terroristas, han sido, por una parte, que las tecnologías informáticas poseen bajos costos y se adquieren fácilmente en el comercio civil o los mercados *online*, y, en segundo lugar, que los usuarios de estas tecnologías tienen la potestad de crear contenidos o alterar el ciberespacio según sus criterios.

Por ende, a partir de la conformación del ciberespacio, la tecnología que permite acceder a él no ha dejado de potencializar sus herramientas y, por supuesto, crear constantemente nuevas aplicaciones. Sumado a este factor, la modernización de los equipos informáticos les ha permitido a los usuarios del ciberespacio establecer sus labores y estrategias propias en las nuevas formas de uso y potencialidades de internet. Esta es la lógica bajo la cual se suscriben las agrupaciones terroristas, y así se da paso al fenómeno del terrorismo ciberespacial (Torres, 2010).

A diferencia de las dinámicas mediáticas del siglo precedente, cuando los terroristas dependían de que los medios llevaran a cabo la transmisión televisiva de su atentado para cumplir el objetivo, ahora los terroristas tienen el control de internet y, por ende, pueden modificar el ciberespacio convenientemente (Nagpal, 2002).

Por esto, los grupos terroristas peruanos, como Sendero Luminoso y el Movimiento Revolucionario Túpac Amaru, emplean este espacio virtual para generar terrorismo a través de la divulgación de contenidos alusivos a la violencia, como imágenes y videos con argumentación política de odio y terror, con el fin de construir mecanismos de ataque psicológico que desvirtúen la mentalidad de la comunidad global frente a su verdadero *modus operandi* (Boyd, 2009).

De la misma manera, explorando las abismales posibilidades del ciberespacio, las redes del terrorismo de la *yihad* islámica han llegado

a consolidar efectivas herramientas para su causa. De la mano de partidarios o militantes "civiles" a nivel mundial, las células yihadistas que coexisten en África, Medio Oriente y Asia han logrado concretar mecanismos complejos para "externalizar" su trabajo propagandístico a través de la divulgación de videos de ejecuciones y ataques terroristas consumados, los cuales son colgados y administrados, por sus colaboradores, en foros y páginas de la red que hoy en día han alcanzado una estabilidad, reconocimiento y eficacia sin precedente (Echavarría, 2009). Esto no es más que la divulgación del terror y los alcances violentos de estos actores a través del ciberespacio.

Ejemplo fehaciente de este tipo de uso del ciberespacio, entre otros tantos, al igual que las ejecuciones de Nicholas Berg, Eugene Armstrong y Jack Hensley, fue el lamentable caso de ejecución tortuosa que se le dio al periodista de *The Wall Street Journal*, Daniel Pearl, por parte de una célula terrorista paquistaní en la ciudad de Karachi en 2002, la cual se documentó en un video que mostraba su decapitación por integrantes de esta célula terrorista. Dicho video fue rápidamente difundido por la red con el fin de transmitir un mensaje de terror al pueblo norteamericano por la incursión armada que llevaba a cabo el Gobierno en Pakistán (*El Mundo*, 2002).

A partir de diversas perspectivas, el ciberterrorismo otorga a los terroristas la posibilidad de existir en un mundo globalizado y con objetivos globalizados (en algunos casos). A partir de las asimetrías connaturales de los conflictos irregulares, el ciberespacio permite a agrupaciones terroristas como Al Qaeda funcionar en red a lo largo del mundo o a organizaciones de carácter más regional conectarse con el mundo entero e intercambiar elementos con organizaciones del mismo tipo (Wilson, 2005).

Al entrar en una perspectiva mucho más profunda en materia cibernética en torno al terrorismo, se puede anticipar que ya no solo se trata del empleo de un medio de comunicación, sino de la consolidación eficiente y efectiva de herramientas a través del ciberespacio que aportan importantes elementos de subsistencia y éxito a la causa de estos actores. En consecuencia, son elementos que acercan al terrorista un paso más a sus objetivos en los escenarios reales de los conflictos, es decir, la perpetración de acciones propias de esta doctrina.

Como lo formuló Barry Collin, del Institute for Security and Intelligence en California, partiendo del hecho de que los grupos terroristas saben explotar a cabalidad las cualidades del mundo informático, y concretamente el ciberespacio como un escenario en el cual se pueden traslapar diversas formas de lucha, el ciberterrorismo debe entenderse como la sinergia entre cibernética y terrorismo (Kushner, 2003).

Finalmente, y de forma complementaria, Pollitt (1998) afirma que el ciberterrorismo es el ataque premeditado, sobre una base política, en contra de la información, los sistemas de los procesadores, los programas de los procesadores y datos, lo cual se traduce en violencia en contra de objetivos no combatientes, por acción de grupos subnacionales o grupos clandestinos (p. 2).

Desde esta lógica, se hace alusión a la manera en que el hecho de trasladar prácticas, como la obtención de información estratégica, la guerra psicológica, el reclutamiento, el financiamiento y el adoctrinamiento al ciberespacio, permite a los actores en mención potenciarlas en consonancia con las características de este escenario virtual de alcance global, que rompe las barreras del tiempo y el espacio que maneja uno de los bienes más preciados en la actualidad: la información (Matusitz, 2005). Por supuesto, una de esas potencialidades que han obtenido los grupos terroristas en el ciberespacio es la coordinación de acciones a nivel global.

Otro caso que da cuenta de la especialización y estructuración que llevan a cabo los terroristas en internet es la creación del comité de comunicación y publicidad que la organización Al Qaeda ha conformado para manejar específicamente sus operaciones en este espacio. Cabe mencionar que es tal la importancia que se le otorga a esta comisión que se encuentra jerárquicamente un escalón abajo del emir-general y de la asamblea consultiva (Guarín, 2009).

Haciendo alusión de nuevo a Al Qaeda, no podía obviarse el acontecimiento que de forma más concreta atentó contra la seguridad y defensa de un Estado: el ataque al World Trade Center de los Estados Unidos el 11 de septiembre de 2001. Este acontecimiento ha sido la muestra más representativa de cómo una agrupación terrorista emplea el ciberespacio para coordinar un atentado a gran escala.

Bajo esta égida, la búsqueda de las escuelas de aviación que entrenaron a los suicidas islámicos, la reserva y compra de los pasajes de avión de las compañías American Airlines y United Airlines en su sitio web y, sobre todo, la coordinación de toda la estratagema y fases del atentado fueron planeadas a través de cuentas de correo electrónico del dominio de Yahoo, Hotmail y chats (Thomas, 2003), claro está, haciendo uso de métodos de encriptación de la información implementados por la organización para no ser detectados por los organismos de seguridad del país norteamericano (Carrillo, 2006). La coordinación y comunicación mundial también permite que importantes líderes terroristas ya no tengan que tomar el riesgo de ser capturados o eliminados al programar reuniones presenciales en algún lugar del mundo. Por lo anterior, los mensajes cifrados a través de cuentas de correo electrónico se han convertido en el pilar de esta práctica.

Ha sido tan importante este factor para las organizaciones terroristas que sus encargados y expertos en tecnologías informáticas dedican grandes esfuerzos por implementar sistemas para evitar la interceptación de sus mensajes, tales como la encriptación, el empleo de páginas web privadas donde se infiltran mensajes y, por último, técnicas como la estenografía (Thomas, 2003).

El ciberterrorismo, en su papel de reclutamiento y adoctrinamiento, también se enfoca en proporcionar la información necesaria a sus militantes y componentes armados para que no pierdan el valor militar y los valores políticos y simbólicos de su causa. Desde esta línea, se busca poder difundir canciones y documentos de carácter político que enaltecen el movimiento, revistas *online*, programas de radio e imágenes (Tibbetts, 2002). Estos elementos, en la mayoría de los casos reseñados, van acompañados de una estrategia lingüística que busca traducir estos contenidos a idiomas foráneos al que emplea la organización y, así, poder generar una captación y aceptación social al nivel mundial (Joshi, 2000).

Si se parte de que las Fuerzas Armadas Revolucionarias de Colombia (FARC) llevan un arduo recorrido de explotación del ciberespacio, se puede esgrimir que el sitio web ANNCOL se ha conformado como su página oficial, lo que les ha permitido divulgar videos, música, documentos e información que tergiversa las acciones del

Estado y las Fuerzas Armadas, así como comunicados de prensa que buscan enaltecer en la sociedad no solo su causa subversiva, sino gobiernos y movimientos políticos internacionales que han demostrado estar en contravía de la soberanía e intereses nacionales de Colombia (Cohen-Almagor, 2000).

Además, el uso que esta agrupación le da a su red de comunicación en el ciberespacio contribuye a diversas actividades como su cobro de impuesto revolucionario, la compra de armamento en el mercado negro y ciertas actividades del orden diario que facilita sus métodos administrativos (Sánchez, 2008). Otra de las expresiones del ciberterrorismo se configura en torno a la facilidad de obtención de información de inteligencia (teniendo las diferencias naturales del concepto, por supuesto), y métodos de entrenamiento.

Cualquier usuario de internet puede testificar que dentro de la información que se encuentra en la red se ofrece contenido personal de los objetivos humanos de estas redes, también fotografías, mapas y planos de lugares y estructuras que podrían ser punto de ataque (Tibbetts, 2002). De igual manera, programación y ubicación de actividades políticas de alto impacto, lo cual para los terroristas se traduce en un sistema que los nutre de una gran cantidad de información en el momento de planear sus operaciones (Conway, 2002).

Paralelamente, no se puede obviar que, en cuanto a medios de entrenamiento, el ciberterrorismo se vale de complejos y eficientes canales de comunicación entre la organización y sus militantes, como lo son foros secretos y encriptados, con el fin de informar a su estructura organizacional las directrices políticas y operativas de la organización, la difusión de manuales para la construcción de artefactos explosivos, información referente a cómo se debe escapar de un teatro de operaciones después de realizado el atentado, cómo llevar a cabo secuestros efectivos o procedimientos específicos en caso de detención policiaca, entre otras formas de acción (Weimann, 2004). A partir del principio de que dimensiones como el ciberespacio difícilmente pueden controlarse respecto de la información que los usuarios difunden a través de esta, los grupos ciberterroristas no han encontrado ningún obstáculo para establecer mecanismos de guerra política (Perešin, 2007).

A través de la guerra política en la red, el terrorismo está ganando una importante ventaja frente a los Estados y fuerzas institucionales que los combaten. Los grupos terroristas están consiguiendo difundir una imagen de impunidad y fortaleza en el mundo entero, lo que, en términos concretos, significa, según Vázquez (2000), una deslegitimación del Estado frente a sus campañas antiterroristas y la consolidación del temor permanente en las personas.

Otro factor que merece ser resaltado para comprender la inmersión del terrorismo en el ciberespacio es la consolidación de fuentes de financiamiento de causas. Se ha logrado establecer que agrupaciones como el IRA (Irish Republican Army) ponen en práctica mecanismos, a través de sus páginas web, para que los visitantes de estas hagan donaciones mediante el uso de sus tarjetas de crédito. Otras como Hamás, por su parte, recaudan fondos de financiamiento por medio del sitio web diseñado para su organización benéfica, Holy Land Foundation for Relief and Development. Por último, en los terroristas chechenos, se empleó el método de la publicación en el ciberespacio de los números de diversas cuentas bancarias para que sus colaboradores depositaran sus donativos en ellas (Trachtman, 2004).

En última instancia, cuando se parte del escenario de las capacidades adquiridas por los grupos terroristas, no se puede dejar de lado la más importante de todas: los ataques cibernéticos. Además de que estos actores han logrado construir importantes mecanismos a través del ciberespacio con el fin de ajustarse a los parámetros y las características del mundo globalizado, y sopesar la asimetría que poseen frente a las fuerzas militares y de seguridad que los combaten, el elemento determinante del ciberterrorismo radica en su capacidad de realizar ciberataques a los Estados con los que mantienen su lucha (Wolthusen, 2003).

Desde esta perspectiva, ya no se involucran en el análisis prácticas terroristas tradicionales de tipo logísticas o de inteligencia, sino que se atiende a la concepción más pura de terrorismo que se desarrolla en el ciberespacio. Como ha establecido Ghosh (2010), si bien en internet la mayoría del tiempo se está interactuando con información visible, es la información que pasa desapercibida al usuario la que les permite a los ciberterroristas acceder a sistemas informáticos que pueden

contener información que, al ser empleada flagrantemente, puede ocasionar graves daños y pérdidas humanas.

Desde esta concepción pura de terrorismo que actúa en el ciberespacio, se maneja la hipótesis de amenaza, de destrucción o caos masivo del Estado y su ciudadanía. Como lo expresa Berkowitz (1997), el hecho de que las tecnologías informáticas se hayan presentado como *causa y efecto* de la globalización, y como medio de comunicación que unieron al mundo, de igual manera generó que estas tecnologías tuvieran que ser implementadas paulatinamente en todos los procesos llevados a cabo por la sociedad, el Estado y el sector privado (Mills, 2010).

Esto permite que actualmente la mayoría de los procesadores que pertenecen al sector gubernamental, militar, de defensa y seguridad, de la infraestructura crítica y la sociedad de los Estados estén conectados al ciberespacio, canal por el cual alguna de estas instancias puede tener un alto riesgo de ser ciberatacada por alguna organización terrorista. Enviar la información adecuada a través del ciberespacio hasta un objetivo seleccionado puede tener diversas consecuencias; perfectamente, se podrían violar los mecanismos de seguridad que protegen archivos con información estratégica ultrasecreta o dañar páginas gubernamentales para inhabilitar su uso y cambiar información (Berkowitz, 1997).

Al desarrollar un análisis del accionar terrorista, es posible percibir que, bajo las posibilidades que ofrece el ciberespacio y la naturaleza informática del mismo sistema, la teoría que se maneja con mayor fuerza en el momento de generar modelos y políticas de ciberdefensa es aquella en la cual el ciberterrorismo logra atacar directamente los sistemas informáticos de la infraestructura crítica del Estado, por lo cual se produciría, entre otros ejemplos, el recalentamiento de un reactor nuclear, la apertura de compuertas de una hidroeléctrica, el sabotaje del tráfico aéreo y la parálisis de la bolsa de valores (Geers, 2010).

Como lo relatan Bishop y Goldman (2003), ya han sido varios, aunque no demasiados, los casos en los cuales un grupo terrorista está implicado en un ciberataque. El primer ejemplo se registró en 1998, cuando los extintos Tigres Tamiles bombardearon con códigos malignos las páginas gubernamentales de Sri Lanka e imposibilitaron

a los *webmasters* de estos sitios controlarlas y repararlas. De igual manera, también se registró que, durante la guerra de Kosovo, diversos grupos terroristas del conflicto atacaron en varias ocasiones las páginas de la Organización del Tratado del Atlántico Norte (OTAN) en internet.

Para mayor claridad, se puede exponer un grupo de jóvenes provenientes de Israel en 2000 que crearon una herramienta que interfería y no permitía el buen funcionamiento de cualquier sitio que perteneciera a Hizbulá y Hamás, con la cual lograron paralizar el sitio web de la Autoridad Nacional Palestina. En respuesta a lo anterior, se hizo una llamada a una *ciber-yihad*, tras lo cual se atacaron los sitios web del Parlamento Israelí y diferentes ministerios (Allen y Demchak, 2003).

El hecho de que tanto la ciberguerra en cuanto representación de la guerra interestatal o regular en el ciberespacio como el ciberterrorismo en cuanto expresión de la asimetría de los conflictos irregulares hayan adquirido un importante dominio del ciberespacio para llevar a cabo acciones furtivas y hostiles ha puesto de manifiesto la necesidad de consolidar medidas y contramedidas de respuesta a estos fenómenos del siglo XXI, y así extender sobre el ciberespacio el manto de la defensa y seguridad estatal. Tanto para aquellos Estados que desarrollan importantes capacidades para hacer la ciberguerra como para los que se han visto alejados de esta práctica, la necesidad de poner en marcha políticas de ciberdefensa para contrarrestar las amenazas que en este nuevo escenario emergen es un punto de discusión irrestricto en la agenda gubernamental de la mayoría de los países del mundo. Por ello, en la actualidad, países como Israel, Brasil, Singapur, Corea del Sur, Australia, Malasia y Japón, entre muchos otros, ya han institucionalizado políticas, acciones gubernamentales y militares en torno a la ciberdefensa.

Conforme se comienzan a registrar los efectos destructivos de los ataques cibernéticos, los gobiernos toman conciencia de la importancia de consolidar cuerpos de defensa y seguridad frente a estas amenazas. Por tanto, los Estados deben desarrollar la voluntad política para invertir presupuestos en desarrollar capacidades estratégicas en materia de ciberdefensa (Kesan y Hayes, 2010). Lo anterior permite

entender que los nuevos actores actualmente comparten el escenario del ciberespacio y la ciberguerra como estrategia con los participantes tradicionales del sistema internacional, es decir, los Estados, que en esta nueva dimensión generan consecuencias en todos los niveles de la sociedad, desde el nivel más amplio hasta llegar a cada individuo que tenga algún tipo de conexión, cualquiera que esta sea, con el ciberespacio.

Conclusiones

Es imperante concluir que, al reconocer que es un punto de vista subjetivo, y sumado a esto que de manera cultural la ciberguerra todavía sigue estando bajo el imaginario de lo futurista o irreal debido al gran componente tecnológico y virtual informático del que este depende, puede afirmarse que la ciberguerra sí ha logrado demostrar su capacidad para convertirse en elemento de poder para los actores armados regulares e irregulares.

Así como la guerra tradicional, la ciberguerra ve su desarrollo condicionado por las tres características esenciales: el entorno, la tecnología y la doctrina; y probablemente sea influenciada de una forma más directa. La razón de esto es que las tres características son completamente nuevas en comparación con el desarrollo tradicional, esto quiere decir que el entorno es el ciberespacio, creación del hombre, y totalmente desconocido para las guerras anteriores. La tecnología es una necesidad en la ciberguerra, sin los avances tecnológicos no se puede llevar a cabo, por tanto, existe una relación de dependencia. Y en cuanto a la doctrina, se exige una nueva perspectiva por parte de todos quienes tienen injerencia en ella, tratando de comprender el nuevo comportamiento.

La evolución es una variable inseparable del hombre, los cambios en su comportamiento son medidos por ella. Por tanto, podría ser

apenas lógico pensar que siempre se está en una constante búsqueda por cambiar y mejorar las condiciones de todos los fenómenos que rodean al ser humano, entre ellos, por supuesto, la guerra; de modo que es el enfrentamiento con características cibernéticas un acontecimiento novedoso, que requiere toda la dedicación por parte de los actores del sistema internacional para lograr su comprensión y conseguir actuar frente a ella.

La cibernética como proceso comportamental de comunicación y control es una asociación natural en el hombre, por tanto, los fenómenos que se generan a partir de ella tienen la misma característica. Desde el hombre como individuo, hasta las creaciones sociales de este, como los Estados, todos construyen una relación directa con la cibernética, y ahora con el ciberespacio y la ciberguerra. Los lazos sociales y políticos con el entorno y la guerra en el ciberespacio son innegables y actualmente inseparables de la humanidad, lo que obliga a construir nuevos marcos desde el sector gubernamental y social tratando de hacer frente a los cambios y a las consecuencias negativas y positivas de la creciente dependencia de todos los aspectos de la sociedad al ciberespacio.

Con los casos y ejemplos analizados tanto desde la perspectiva de los actores regulares con los que se configuran bajo la égida del Estado como de los actores irregulares o armados de manera ilegal, fue posible constatar que, al emplear computadoras, redes de comunicación, internet y otro tipo de dispositivos que se fundamentan en la informática y la comunicación, estos actores pueden alcanzar de manera eficiente sus intereses políticos o militares.

De manera significativa, cabe recalcar, tomando uno de los ejemplos en materia de ciberguerra desde los actores regulares que es uno de los parangones para la explicación de este fenómeno, que es posible constatar que países como los Estados Unidos o Israel no dependen de la movilización de sus recursos militares o de seguridad y defensa para evitar, desde su perspectiva, que Irán consiga armas nucleares. Ahora, simplemente tienen que utilizar y valerse de sus recursos de ciberguerra para obtener un objetivo geopolítico militar o de seguridad.

Si se tiene en cuenta que, si bien las organizaciones terroristas o subversivas presentan grados de sofisticación menos avanzados que

los Estados y sus Fuerzas Armadas debido a los recursos con los que cuentan, estos actores irregulares están obteniendo réditos políticos y aumentando su poder a partir del uso de tecnologías informáticas, no solo porque pueden perjudicar las representaciones de los gobiernos contra los que luchan en internet, al afectar sus páginas web, sino que, desde otro punto de vista, en la realidad este tipo de agrupaciones han conseguido la constitución de unos tentáculos virtuales que les han permitido adoctrinar, reclutar y entrenar a miembros o nuevos miembros en otros territorios; es decir, esto ha funcionado muy bien para estos grupos desde el punto de vista del poder y de la capacidad de desterritorialización de sus procesos bélicos, estratégicos y tácticos.

También se deja sobre la mesa el debate que determina la cultura de la cibernética en todos los fenómenos abordados que de manera semántica o cultural se ha bautizado con el prefijo *ciber*. Es importante este tema, porque parte del proceso de concienciación e invitación a otros académicos a que analicen la ciberguerra es dejar claro de antemano que todo aquello denominado con el prefijo *ciber* no depende del hecho de que sean procesos o actividades que se llevan a cabo en el ciberespacio, sino que son actividades que se derivan de la lógica del control, como se explicó en uno de los capítulos del libro.

Las intenciones de los actores armados que emplean la ciberguerra se deben llevar a un punto de análisis mucho más estratégico y profundo, y no solo llegar al "cómo" y "qué tipo" de información se afectó, sino de qué manera los procesos y los elementos vitales que se definían por la información afectada tengan que hacerlo bajo los principios de la corrupción, el reemplazo o el robo de esta. Eso es lo que verdaderamente debería importar sobre el ejercicio de la ciberguerra: no tanto el medio y cómo se afecta este, la información, sino qué es lo que verdaderamente está pasando con los procesos humanos, y lo que es más importante como sociedad y como Estado, qué es indispensable proteger.

Es preciso recalcar y profundizar en este punto como una conclusión adicional. Las capacidades que la ciberguerra ofrece a los actores armados han alcanzado instancias que, en los contextos del Estado como ente regulador que garantiza la seguridad, son vitales y debería tener en cuenta. Por ejemplo, y aunque fue la primera doctrina que se

constituyó a partir de la inclusión de las tecnologías informáticas en la guerra, parte de lo que se debe tener en cuenta como elemento amenazado dentro de los Estados es la mente o el comportamiento de los ciudadanos o las fuerzas militares.

También se tiene la creencia, gracias a las noticias, de que la ciberguerra afecta cosas como servidores, sistemas informáticos de bancos de grandes corporaciones, páginas web, pero, en últimas, no se está comprendiendo cuál es el efecto posterior de estas acciones, qué pasa con el comportamiento de las personas que ven afectados sus procesos porque hay un actor amenazante que está jugando con información vital. De la misma manera, y con toda la revolución tecnológica que se está dando en el contexto cíborg, es importante también reconocer que en algún momento la propia existencia o salud va a depender de la capacidad para defenderse de la ciberguerra.

Cada vez se fomenta más la idea de la posibilidad de integrar en los sistemas que rodean el desarrollo de la realidad global dispositivos informáticos que pueden potenciar el actuar natural como seres humanos, es decir, poner chips informáticos en los cerebros o adaptar a los cuerpos, en aquellos miembros faltantes, prótesis robóticas que se encuentran vinculados a un ambiente interconectado de información. Así que cabría preguntarse qué pasaría, y como ya se han preguntado diversos analistas en medios periodísticos, si alguien tuviera la capacidad de hackear los sistemas informáticos que controlan muchos de los marcapasos que utilizan actualmente millones de personas en el mundo, y de los cuales sus propios fabricadores ya han establecido que, debido a la evolución que han tenido, pueden conectarse a través de ondas informáticas a otro tipo de dispositivos para poderlos monitorear o controlar; pero, de la misma manera, así como se abre una puerta de comunicación para este tipo de procesos, también esta comunicación puede ser alterada por un actor que quiera hacer daño sobre la población de un país.

Se pone en consideración que, por más de que la ciberguerra se enmarque, valga la redundancia, en el campo de la guerra, esta como fenómeno social o humano ha sobrepasado las dimensiones propias de la guerra. Es importante tener en cuenta que, si bien este espacio bélico llegó a sufrir grandes transformaciones como lo fue aceptar e

incluir actores no estatales que se habían armado de manera ilegal, con la ciberguerra la inclusión de actores es un proceso prácticamente sin control, sin registro y sin la capacidad de determinar quién se podría convertir en un soldado en este nuevo contexto. Aunque no fue propósito de este libro la inclusión de toda la gama de actores que podrían utilizar las tecnologías informáticas en un sentido de poder, se formularía como una gran conclusión de este que utilizar las tecnologías informáticas como armas o como mecanismo de presión política se convirtió en un fenómeno sumamente democrático.

Y, claramente, no se usa el término democrático desde el sentido del sistema de gobierno, sino en el sentido de que todos pueden llegar a ser parte de la ciberguerra. Valga la pena aclarar que, cuando se alude a este concepto holístico o incluyente como puede ser la democracia, no se hace referencia como tal a un escenario en el cual verdaderamente cada ser humano del planeta pueda convertirse en un cibersoldado; tiene que ver más con el sentido de las herramientas que dan acceso a la práctica de la ciberguerra y, como el lector notará, más allá de tener que recurrir a mercados negros o ilegales para poder adquirir un arma en sinónimo de poder, la ciberguerra pone a disposición los dispositivos por los cuales se lleva a cabo en los mercados cotidianos de todas las ciudades y los pueblos del mundo. Por tanto, es posible encontrar en diversas tiendas computadoras, tabletas, celulares y, al mismo tiempo, aquellos prestadores de servicios que permiten conectar dos dispositivos a internet para que la información que se maneja en estos tenga un alcance global y se rompa el concepto de la frontera estatal.

Las conclusiones que respondan específicamente a los objetivos del proyecto son indispensables, dando alcance a las metas propuestas al dar inicio. En cuanto a la generalidad, queda claro que, por supuesto, el ciberespacio se ha convertido en una dimensión de acción humana para reproducir la práctica de la guerra interestatal propia de las relaciones internacionales. La ciberguerra es un fenómeno que ha permitido traslapar el entorno real donde se habían llevado a cabo tradicionalmente los procesos humanos y el ciberespacio, donde ciertas características como la inmediatez, el anonimato, los bajos costos, el alcance global, entre otras, han facilitado los enfrentamientos bélicos entre los actores del sistema internacional.

En cuanto a los específicos, con una intención aclaratoria, se demostró cómo se ha puesto en práctica de la guerra y los elementos perennes que este fenómeno contiene, para entender su relación con la tecnología, componente esencial del ciberespacio, lo que permite comprender que la guerra, como el comportamiento humano, se han visto determinados por los avances tecnológicos que se adaptan a ellos para aprovechar los beneficios que estos generen.

El ciberespacio a su vez es descrito como un entorno creado exclusivamente por las manos del hombre, que ha visto el nacimiento de una dependencia, donde, debido a características ya mencionadas, se han anclado casi todos los procesos posibles, desde la actuación individual y personal, hasta los Estados más grandes con sus infraestructuras enlazadas a este, dejando al descubierto vulnerabilidades que abren caminos para ser aprovechadas y entrar en conflicto.

La ciberguerra, con sus cuatro teatros —psicológico, centros de gravedad, robótico y cíborg—, refleja que este fenómeno no tiene una sola cara, que se puede llevar a cabo por infinidad de caminos, los mismos que tiene el ciberespacio. Desde la influencia sobre los individuos, pasando por afectar las infraestructuras críticas para debilitar tanto física como moralmente a los gobiernos o comandantes, la construcción de herramientas que ya no dependan del hombre y se manejen por cuenta propia, llegando a la modificación misma del cuerpo humano para hacerlo más fuerte y menos vulnerable a las falencias propias de este, la ciberguerra se convierte en un fenómeno que sobrepasa los límites conocidos y requiere la comprensión a múltiples niveles.

Por último, se identificaron actores distintos de los Estados que participan en la ciberguerra. Casos como los hacktivistas y terroristas reflejan que los individuos pueden usar herramientas tecnológicas para cumplir sus objetivos; que si bien no se puede hablar de la participación de cada ciudadano en el mundo en la ciberguerra como se mencionó, queda en evidencia que aquellos con intereses, conocimientos y recursos pueden aprovecharse del ciberespacio.

Para finalizar, se ha detectado como un elemento recurrente el incremento del interés por los temas relacionados con el ciberespacio, en especial, aquellos donde podría existir un alto riesgo de hacerse realidad las peores catástrofes pensadas por la humanidad. No obstante,

y por más que las noticias a nivel mundial presentan constantemente la perpetración de actos amenazantes a través de internet, aún queda bastante curiosidad por sembrar en la cultura pública los alcances que las acciones humanas tienen hoy gracias a lo *ciber*.

Por esto, al igual que muchos colegas en Colombia y el mundo entero, el autor considera que, a partir de pequeños pasos y de ofrecer semillas de interés a las personas acerca de la ciberguerra, y en general de todas las ciberamenazas, es el camino para iniciar un proceso de sensibilización en comunidades académicas y en la sociedad en general. Si bien es importante ver y explotar todos los elementos positivos de las tecnologías informáticas, también lo es que en esferas gubernamentales, económicas, industriales-empresariales, instituciones prestadoras de servicios, instancias públicas o sociales, y claro está, la vida privada se encuentra en peligro por una gran cantidad de acciones maliciosas que buscan alterar el buen funcionamiento de la tecnología en la que hemos depositado la confianza de controlar el mundo.

Este no es un libro que abarca todas las aristas que se podrían trabajar acerca de la temática, y tampoco se trata de uno que viene a plantear verdades absolutas. Desde la perspectiva del autor, se trata de un libro que busca formular cuestionamientos en el intento de generar curiosidad, necesaria para que otros académicos se adhieran a la labor investigativa y propositiva respecto de lo ciberespacial y su relación con aspectos políticos vitales como la seguridad y defensa nacional. A lo largo de este, el lector vislumbrará una realidad ineludible que hará que vea con mayor seriedad las cuestiones relacionadas con temas como internet y sus propios equipos; no obstante, se espera que también se motive un grado de concienciación mayor, uno que, tal vez, desde el nivel social, empiece a generar discursos y debates de cómo el Estado tiene una nueva responsabilidad con sus ciudadanos en el siglo xxi.

Bibliografía

Abbate, J. E. (1994). *From ARPANET to Internet: A history of ARPA-sponsored computer networks, 1966-1988*. Pennsylvania: University of Pennsylvania.

Adams, J. (2001). Virtual defense. *Foreign Affairs*, *80*(3), 98-112.

Ajami, S. y Rajabzadeh, A. (2013). Radio Frequency Identification (RFID) technology and patient safety. *Journal of Research in Medical Sciences*, 18(9), 809-813.

Alcaraz, C. y Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, 53-66.

Allen, D. M. y Allen, J. H. (2012, enero). *How to become a cyber warrior* [Podcast de audio]. Recuperado de https://www.cert.org/podcasts/podcast_episode.cfm?episodeid=34730

Allen, P. y Demchak, C. (2003). La guerra cibernética palestina-israelí. *Military Review*, 2, 52-59.

Anding, D. E. (2007). *Center of gravity and the range of military operations: Can an old dog apply to new tricks?* Massachusetts: Naval War College.

Arquilla, J. y Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141-165.

Arquilla, J. y Ronfeldt, D. (1997a). A *new epoch and espectrum of conflicts*. En J. Arquilla y D. Ronfeldt (eds.), *In Athena's camp: Preparing for conflict in the information age* (pp. 1-22). Santa Mónica, CA: RAND.

Arquilla, J. y Ronfeldt, D. (1997b). Cyberwar is coming! En J. Arquilla y D. Ronfeldt (eds.), *In Athena's camp: Preparing for conflict in the information age* (pp. 23-60). Santa Mónica, CA: RAND.

Arquilla, J. y Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy.* Santa Mónica, CA: RAND.

Arquilla, J., Ronfeldt, D. y Zanini, M. (2000). *Networks, netwar, and information-age terrorism.* En Z. Khalilzad y J. White (eds.), *Strategic appraisal: The changing role of information in warfare* (pp. 75-111). Santa Mónica, CA: RAND.

Asaolu, O. S. (2006). On the emergence of new computer technologies. *Educational Technology & Society*, *9*(1), 335-343.

Asaro, P. M. (2012). How just could a robot war be? En P. Tamara y E. Gaston (eds.), *Ethics of 21st century military conflict* (pp. 257-269). Nueva York: International Debate Education Association.

ASCE Critical Infrastructure Guidance Task Committee (2009). *Guiding principles for the nation's critical infrastructure.* Virginia: American Society of Civil Engineers.

Ashmore, W. C. (2009). Impact of alleged russian cyber attacks. *Baltic Security & Defence Review*, 11, 4-40.

Ballén Molina, R. (2010). Las razones que motivan la guerra. *Diálogos de saberes: investigaciones y ciencias sociales*, 32, 103-120.

Ballina Talento, G. (2008). *La evolución de la internet como medio de comunicación masivo* (Tesis de grado, Universidad de San Carlos de Guatemala, Guatemala).

Barfield, W. y Williams, A. (2017). Cyborgs and enhancement technology. *Philosophies*, *2*(1).

Bazyan, S. (2012). *Environmental impact of war technology and prohibition processes* (Tesis de maestría, Mittuniversitetet, Östersund, Suecia).

Bejarano, P. (2014, febrero 6). Código Enigma, descifrado: el papel de Turing en la Segunda Guerra Mundial. *Eldiario.es*. Recuperado de http://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_0_226078042.html

Bellamy, C. (2015). *The evolution of modern land warfare: Theory and practice.* Londres: Routledge.

Bendrath, R. (2001). The ciberwar perceptions and politics in U.S. critical infrastructure protection. *Information & Security: An International Journal*, 7, 80-103.

Berkowitz, B. D. (1997). Warfare in the information age. En J. Arquilla y D. Ronfeldt (eds.), *In Athena's camp: Preparing for conflict in the information age* (pp. 175-190). Santa Mónica, CA: RAND.

Bessani, A. N., Sousa, P., Correia, M., Neves, N. F. y Veríssimo, P. (2008). The CRUTIAL way of critical infrastructure protection. IEEE *Security & Privacy*, 6, 44-51.

Bhattacharjee, S. (2009). The strategic dimensions of cyber security in the indian context. *Strategic Analysis*, *33*(2), 196-201.

Bieber, F. (2000). Cyberwar or sideshow? The Internet and the Balkan wars. *Current History*, *99*(635), 124-128.

Bishop, M. y Goldman, E. (2003). The strategy and tactics of information warfare. *Contemporary Security Policy*, *24*(1), 113-139.

Black, J. (2009). The revolution in military affairs: The historian's perspective. *The RUSI Journal*, *154*(2), 98-102.

Boaru, G. y Badita, G. I. (2008). Critical infrastructure interdependencies. En I. Bujoreanu y D. Sora (coords.), *Defense resources management in the 21st century* (pp. 130-146). Bucarest: National Defense University Carol I Publishing House.

Boot, M. (2003). The new American way of war. *Foreign Affairs*, *82*(4), 41-58. Recuperado de https://www.foreignaffairs.com/articles/united-states/2003-07-01/new-american-way-war

Boot, M. (2006). The paradox of military technology. *The New Atlantis*, 14, 13-31.

Boyd Jara, C. (2009, agosto 5). Internet: el refugio de grupos terroristas [Entrada blog]. Recuperado de http://intelligenceservicechile.blogspot.com/2009/08/internet-el-refugio-de-grupos.html

Bradley, A. (2003). *Anatomy of cyberterrorism is America vulnerable?* (Tesis de grado, Air University, Alabama, Estados Unidos).

Brenner, S. W. (2009). *Cyberthreats: The emerging fault lines of the nation state*. Oxford: Oxford University Press.

Brey, P. A. y Mitcham, C. (2005). Prosthetics. En *MacMillan Encyclopedia of Science, Technology and Ethics* (pp. 1527-1532). Basingstoke: MacMillan Press.

Brooks, S. G. y Wohlforth, W. C. (2007). Power, globalization, and the end of the cold war: Reevaluating a landmark case for ideas. En J. Levy y

G. Goertz (eds.), *Explaining war and peace: Case studies and necessary condition counterfactuals* (pp. 195-236). Abingdon: Routledge.

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

Carrillo Payá, P. (2006). *Terrorismo y ciberespacio*. Recuperado de http://www.assessorit.com/web/images/stories/prensa/pcarrillo-paper.pdf

Casey, G. (2009). *Future Soldier 2030 Initiative*. RDECOM. Recuperado de https://www.wired.com/images_blogs/dangerroom/2009/05/dplus2009_11641-1.pdf

Castells, M. (1997). An introduction to the information age. *City*, *2*(7), 6-16.

Castells, M. (1999). *La era de la información: economía, sociedad y cultura* (vol. 1). México: Siglo XXI.

Castells, M. (2000). *La sociedad red*. Madrid: Alianza Editorial.

Castells, M. (2001). *Galaxia Internet*. Barcelona: Plaza & Janés.

Castells, M. (2004). *The network society: A cross-cultural perspective*. Cheltenham, MA: Edward Elgar Publishing.

Castro, C. y Filippi, L. (2010). Modelos matemáticos de información y comunicación cibernética (Wiener, Shannon y Weaver): mejorar la comunicación es el desafío de nuestro destino cultural. *Revista RE-Presentaciones Periodismo, Comunicación y Sociedad, 3*(6), 145-161.

Cebrowski, A. K. y Garstka, J. J. (1998). Network-centric warfare: Its origin and future. *U.S. Naval Institute Proceedings*, *124*(1), 28-35.

Chandler, W. W. (1983). The installation and maintenance of Colossus. *Annals of the History of Computing, 5*(3), 260-262.

Chilton, K. P. (2009). Cyberspace leadership: Towards new culture, conduct, and capabilities. *Air & Space Power Journal*, *23*(3), 5-11. Recuperado de http://go.galegroup.com/ps/anonymous?id=GALE%7CA212767728&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=1555385X&p=AONE&sw=w

Clark, A. (2003). *Natural-born cyborgs: Minds, technologies, and the future of human intelligence*. Nueva York: Oxford University Press.

Clark, T. (2015). *Autonomous robotics for military usage*. Recuperado de http://www.pitt.edu/~trc50/writing_assignment_3.pdf

Clark, R. A. y Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. Nueva York: ECCO.

Clarke, B. (2015, septiembre 1). The 30 most important airplanes of all time the planes that defined the aerospace age. *Popular Mechanics*. Recuperado de http://www.popularmechanics.com/flight/g2142/the-30-most-important-airplanes-of-all-time/

Clarke, R. (2009). War from cyberspace. *The National Interest*, 104, 31-36.

Clausewitz, C. (1942). *Principles of war*. Pensilvania: Stackpole Books.

Clemente, D. (2013). *Cyber security and global interdependence: What is critical?* Londres: Chatham House, Royal Institute of International Affairs.

Coeckelbergh, M. (2013). Drones, information technology, and distance: Mapping the moral epistemology of remote fighting. *Ethics and Information Technology*, *15*(2), 87-98.

Cohen-Almagor, R. (2000). The terrorists' best ally: The Quebec media coverage of the FLQ crisis in october 1970. *Canadian Journal of Communication*, *25*(2), 251-284.

Cohen, J. (2013). Memory implants: A maverick neuroscientist believes he has deciphered the code by which the brain forms long-term memories. *MIT Technology Review*. Recuperado de https://www.technologyreview.com/s/513681/memory-implants/

Cohnen, F. (2010). Las ciberguerras del siglo XXI. *Antena de Telecomunicación*, 179, 16-21.

Colesniuc, D. (2013). Cyberspace and critical information infrastructures. *Informatica Economica*, *17*(4), 123-132.

Cooper, J. R. (1997). Another view of the revolution in military affairs. En J. Arquilla y D. Ronfeldt (eds.), *In Athena's camp: Preparing for conflict in the information age* (pp. 99-140). Santa Mónica, CA: RAND.

Conway, M. (2002). Reality bytes: Cyberterrorism and terrorist 'use' of the Internet. *First Monday*, *7*(11). Recuperado de http://doras.dcu.ie/498/1/first_mon_7_11_2002.pdf

Cordesman, A. H. y Wagner, A. R. (1990). *The lessons of modern war*. Boulder: Westview Press.

Counter-Terrorism Committee Executive Directorate (2017). *Physical protection of critical infrastructure against terrorist attacks*. Nueva York: Counter-Terrorism Committee Executive Directorate.

Criado Grande, J. I., Ramilo Araujo, M. C. y Serna, M. S. (2002). *La necesidad de teoría(s) sobre gobierno electrónico: una propuesta integradora*. Ponencia presentada en XVI Concurso de Ensayos y Monografías del

CLAD sobre Reforma del Estado y Modernización de la Administración Pública "Gobierno Electrónico". Caracas, Venezuela. Recuperado de https://www.urbe.edu/info-consultas/web-profesor/12697883/articulos/Comercio%20Electronico/la-necesidad-de-teoria(s)sobre-gobierno-electronico-una-propuesta-integradora.pdf

Cronin, B. y Crawford, H. (1999). Information warfare: Its application in military and civilian contexts. *The Information Society*, *15*(4), 257-263.

Crowell, R. M. (2017). *Some principles of cyber warfare using corbett to understand war in the early twenty: First century*. Londres: The Corbett Centre for Maritime Policy Studies.

Danet, D. y Hanon, J. P. (2014). Digitization and robotization of the battlefield: Evolution or robolution? En R. Doaré, D. Danet, J. P. Hanon y G. de Boisboissel, *Robots on the battlefield: Contemporary perspectives and implications for the future* (pp. XIII-XXXV). Kansas: Combat Studies Institute Press.

Danish Institute For International Studies (2017). *The UN discusses lethal autonomous weapons Killer Robots: The future of war?* Recuperado de http://pure.diis.dk/ws/files/817702/Killer_robots_WEB.pdf

Davis, N. C. (1997). An information-based revolution in military affairs. En J. Arquilla y D. Ronfeldt (eds.), *In Athena's camp: Preparing for conflict in the information age* (pp. 79-98). Santa Mónica, CA: RAND.

De Boisboissel, G. (2014). The use of robots on the Battlefield: Benefits, constraints, and limitations for soldiers. En R. Doaré, D. Danet, J. P. Hanon y G. de Boisboissel, *Robots on the battlefield: Contemporary perspectives and implications for the future* (pp. 203-216). Kansas: Combat Studies Institute Press.

Delibasis, D. (2007). *The right to national self-defense: In information warfare operations*. Tennessee: Arena books.

Department of Defense (1997). *C4ISR architecture framework version 2.0*. Washington D. C.: C4ISR Architecture Working Group.

DoD *Dictionary of Military and Associated Terms* (2018). Recuperado de http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-07-25-091749-087

Douhet, G. (2009). *The command of the air.* Alabama: University of Alabama Press.

Doyle, D. J. (2014). Robots, androids, and cyborgs in warfare: Ethical and philosophical issues. *Ethics in Biology, Engineering and Medicine: An International Journal*, *5*(1), 13-23.

Droznes, L. (2005). *El arte de la guerra: guía de aplicación de los principios básicos de la guerra a las realidades de los mercados competitivos contemporáneos*. Buenos Aires: Autodesarrollo.

Dunlap Jr, C. J. (2006). Neo-strategicon: Modernized principles of war for the 21st century. *Military Review*, 42-48.

Dunn Cavelty, M. (2010). Cyberwar: Concept, status quo, and limitations. *CSS Analysis in Security Policy*, 71, 1-3.

Dunn, M. A. (2001). The cyberspace dimension in armed conflict: Approaching a complex issue with assistance of the morphological method. *Information & Security,* 7, 145-158.

Echevarría, A. (2003). Clausewitz's Center of Gravity: It's not what we thought. *Naval War College Review,* 108-123.

Echavarría Jesús, C. (2009, diciembre 23). La innovación yihadista: propaganda, ciberterrorismo, armas y tácticas. *Grupo de Estudios Estratégicos*. Recuperado de http://www.gees.org/articulos/la-innovacion-yihadista-propaganda-ciberterrorismo-armas-y-tacticas

El Mundo (2002, febrero 23). Musharraf ordena la detención de todos los miembros del grupo que degolló al periodista Daniel Pearl. Recuperado de http://www.elmundo.es/elmundo/2002/02/21/internacional/1014327615.html

Eikmeier, D. C. (2004). Center of gravity analysis. *Military Review*, *84*(4), 2-5.

Enders, W. y Sandler, T. (2000). Is transnational terrorism becoming more threatening? A time-series investigation. *Journal of Conflict Resolution*, *44*(3), 307-332.

Emol.com (2007, noviembre 15). En marcha computadora de la Segunda Guerra Mundial. Recuperado de http://www.emol.com/noticias/tecnologia/2007/11/15/281942/en-marcha-computadora-de-la-segunda-guerra-mundial.html

Estupiñán Bethencour, F. (2001). Mitos sobre la globalización y las nuevas tecnologías de la comunicación. *Revista Latina de Comunicación Social, 4*(38), 1-2.

Fabricio, A. (s. f.). *Concepto de doctrina*. Recuperado de https://es.scribd.com/doc/57143024/CONCEPTO-DE-DOCTRINA

Fadok, D. S. (1995). *John Boyd and John Warden: Air power's quest for strategic paralysis*. Alabama: School of Advanced Airpower Studies.

Fazio Vengoa, H. (2003). Globalización y guerra: una compleja relación. *Revista de Estudios Sociales*, 16, 42-56.

Fitzgerald, F. (2001). *Way out there in the blue: Reagan, star wars and the end of the cold war*. Nueva York: Simon and Schuster.

Fleming, J. L. (1993). *Capital ships: A historical perspective*. Rhode Island: Naval War College.

Fojón, J. E. (2006). *Vigencia y limitaciones de la guerra de cuarta generación*. Real Instituto Alcano de Estudios Internacionales y Estratégicos. Recuperado de http://documentostics.com/component/option,com_docman/task,doc_view/gid,864/Itemid,5/

Foster, Jr , J. S., Gjelde, E., Graham, W. R., Hermann, R. J., Kluepfel, H. M., Lawson, R. L. … Woodard, J. B. (2008). *Report of the Commission to Assess the Threat to the United States from EMP Attack: Critical national infrastructures*. Washington D. C.: Congressional EMP Commission.

Fredericks, B. (1997). Information warfare: The organizational dimension. En R. E. Neilson (ed.), *Sun Tzu and information warfare: A collection of winning papers from the Sun Tzu art of war in information warfare competition* (pp. 79-102). Washington D. C.: National Defense University Press Publications.

Fulp, J. D. (2003). Training the cyber warrior. En C. Irvine y H. Armstrong (eds.), *Security education and critical infrastructures* (pp. 261-273). Boston, MA: Springer.

Gaddis, J. L. (1997). History, theory, and common ground. *International Security*, *22*(1), 75-85.

Gamero-Garrido, A. (2014). *Cyber conflicts in international relations: Framework and case studies*. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427993

Gates, B. (1995). *Camino al futuro*. Bogotá: McGraw-Hill.

Geers, K. (2008). *Cyberspace and the changing nature of warfare*. Recuperado de https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/RTO-MP-IST-076/$MP-IST-076-KN.pdf

Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. *Information Security Journal*: *A Global Perspective, 18*(1), 1-7.

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, *26*(3), 298-303.

Gibbs, S. y Hern, A. (2017, mayo 12). What is WannaCry ransomware and why is it attacking global computers? *The Guardian*. Recuperado de https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20

Gibson, W. (1984). *Neuromancer.* Nueva York: Ace Books.

Glavanakova, A. (2006). *Cyborg body politics. Bulgarian Journal of American and Transatlantic Studies*, 1. Recuperado de https://research.uni-sofia.bg/handle/123456789/1245

Glebocki, J. (2008). DOD *Computer Network Operations: Time to hit the send button.* Carlisle Barracks, PA: U.S. Army War College. Recuperado de http://www.dtic.mil/dtic/tr/fulltext/u2/a478337.pdf

Ghosh, S. (2004). The nature of cyber-attacks in the future: A position paper. *Information Systems Security, 13*(1), 18-33.

Gorman, S. P. (2005). *Networks, Security and Complexity: The role of public policy in critical infrastructure protection*. Cheltenham: Edward Elgar Publishing.

Granada, S. y Sánchez Meertens, C. (2009). Correlación de fuerzas en disputas de guerras civiles: una aplicación al caso colombiano. En J. A. Restrepo y D. Aponte (eds.), *Guerra y violencias en Colombia: herramientas e interpretaciones* (pp. 233-272). Bogotá: Pontificia Universidad Javeriana.

Grauer, R. (2013). Old wine in new bottles: The nature of conflict in the 21st century. *The Whitehead Journal of Diplomacy and International Relations, 14*(9), 9-23.

Green, J. (2002). The myth of cyberterrorism. *Washington Monthly*, *34*(11), 8-13.

Grinter, L. E. y Schneider, B. R. (1998). *Battlefield of the future: 21st century warfare issues*. Alabama: Air University Press.

Gros Salvat, B. (2001). De la cibernética clásica a la cibercultura: herramientas conceptuales desde donde mirar el mundo cambiante. *Education in the Knowledge Society* (EKS), 2. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=1243527

Guarín, R. (2009). *Medios de comunicación, terrorismo y antiterrorismo*. Bogotá: Escuela de Inteligencia y Contra Inteligencia Brigadier General Ricardo Charry.

Gutiérrez Díez, L. A. (1995). Evolución de la tecnología militar y "su impacto" en España. *Cuadernos de Estrategia*, *75*, 83-114.

Gutiérrez, M. F. (2010). Virus y cibervirus: virus biológicos y virus informáticos llaman la tensión de los virólogos. *Innovación y Ciencia*, *17*(1), 50-56.

Hables Gray, C. (1997). *Postmodern war: The new politics of conflict*. Nueva York: Guilford Publications.

Haeni, R. E. (1997). *Information warfare: An introduction*. Washington D. C.: The George Washington University.

Harshberger, E. y Ochmanek, D. (1999). Information and warfare: New opportunities for U.S. military forces. En Z. Khalilzad y J. White (eds.), *Strategic appraisal: The changing role of informatin in warfare* (pp. 157-178). Santa Mónica, CA: RAND.

Haulman, D. (2003). *One hundred years of flight USAF chronology of significant air and space events 1903-2002*. Alabama: Air University Press.

Henry, R. y Peartree, C. E. (1998). Military theory and information warfare. *Parameters*, 28, 121-135.

Herr, H., Whiteley, G. P. y Childress, D. (2003). Cyborg technology: Biomimetic orthotic and prosthetic technology. En Y. Bar-Cohen y C. Breazeal, *Biologically inspired intelligent robots* (pp. 103-143). Washington D. C.: SPIE Press.

Heylighen, F. y Joslyn, C. (2001). Cybernetics and second-order cybernetics. En R. A. Meyers (ed.), *Encyclopedia of physical science & technology* (3.ª ed., pp. 155-170). Nueva York: Academic Press.

Hollis, D. (2011). Cyberwar case study: Georgia 2008. *Small Wars Journal*, *6*(1), 1-10.

Holmes, R. (ed.) (2007). *Campos de batalla: las guerras que han marcado la historia*. Barcelona: Ariel.

Hosek, J. R. (2003). The soldier of the 21st century. En S. E. Johnson, M. C. Libicki y G. F. Treverton (eds.), *New challenges, new tools for defense decisionmaking* (pp. 181-209). Santa Mónica, CA: RAND.

Hosmer, S. T. (1999). The information revolution and psychological effects. En Z. Khalilazad y J. White (eds.), *The changing role of information in warfare* (pp. 217-252). Santa Mónica, CA: rand.

Internet Society (2014, junio 3). *Global internet report 2014: Open and sustainable acces for all*. Ginebra: Internet Society.

Jablonsky, D. (1994). U.S. Military Doctrine and the Revolution in Military Affairs. *Parameters*, *24*(3), 18-36.

Jackson, G. M. (2000). *Warden's five-ring system theory: Legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?* (Tesis de grado, Maxwell Air Force Base, Alabama, Estados Unidos).

Jain, G. (2005). Cyber terrorism: A clear and present danger to civilized society? *Information Systems Education Journal*, *3*(44), 1-8.

Jiménez Cruz, J. (2008). Cibernética, inteligencia artificial y robótica. *Casa del Tiempo, 5*(13), 52-56.

Joshi, A. (2000). The scourge of cyber-terrorism. *Strategic Analysis*, *24*(4), 827-831.

Joyner, C. C. y Lotrionte, C. (2001). Information warfare as international coercion: Elements of a legal framework. *European Journal of International Law*, *12*(5), 825-865.

Kaldor, M. (1998). *New and old wars: Organized violence in a global era.* Lincolnshire: Stanford University Press.

Kellermann, T., Martinez, P., Contreras, B. y Marchiori, B. (2015). *Report on cybersecurity and critical infrastructure in the Americas.* Washington D. C.: OAS Secretariat for Multidimensional Security.

Kemp, S. (2017, enero 24). Digital in 2017: Global overview. *We Are Social*. Recuperado de https://wearesocial.com/special-reports/digital-in-2017-global-overview

Kerr, P. K., Rollins, J. y Theohary, C. A. (2010). The Stuxnet computer worm: Harbinger of an emerging warfare capability. *CRS Report for Congress*. Recuperado de http://www.fas.org/sgp/crs/natsec/R41524.pdf

Kerr, P. K., Rollins, J. y Theohary, C. A. (2012). The Stuxnet computer worm: Harbinger of an emerging warfare capability. *CRS Report for Congress*.

Kesan, J. P. y Hayes, C. M. (2010). Thinking through active defense in cyberspace. En *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (pp. 327-341). Washington D. C.: The National Academies Press.

Khan, K. (2013). Understanding information warfare and its relevance to Pakistan. *Strategic Studies*, *32*(4), 138-159.

Khan, Z. (2015, diciembre 2). *5 technologies that transformed warfare*. *TechoMag*. Recuperado de http://www.techomag.com/5-technologies-that-transformed-warfare/

Khiabany, G. (2003). Globalization and the internet: Myths and realities. *Trends in Communication*, *11*(2), 137-153.

Korns, S. W. y Kastenberg, J. E. (2009). Georgia's cyber left hook. *Parameters*, 60-76.

Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal*, 3, 237-245.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Efining the problem. En F. D. Kramer, S. H. Starr y L. K. Wentz (eds.), *Cyberpower and national security* (pp. 26-43). Virginia: Potomac Books.

Kushner, H. W. (2003). *Encyclopedia of terrorism*. Londres: Sage.

Laqueur, W. (1987). *The age of terrorism*. Boston: Little Brown.

Lee, R. M., Assante, M. J. y Conway, T. (2014). *German steel mill cyber attack*. Recuperado de https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Lemley, M. A., Menell, P. S., Merges, R. P. y Samuelson, P. (2000). *Software and internet law.* (3.ª ed.). Cambridge, MA: Aspen Law & Business.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Recuperado de https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Leveringhaus, A. y Giacca, G. (2014). *Robo-Wars: The regulation of robotic weapons*. Oxford: University of Oxford.

Li, J. y Daugherty, L. (2015). *Training cyber warriors: What can be learned from defense language training?* Santa Mónica, CA: RAND.

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

Libicki, M. C. (1998). Information war, information peace. *Journal of International Affairs*, *51*(2), 411-428.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Mónica: RAND.

Liddell Hart, B. (1967). *Strategy: The indirect approach*. Los Ángeles: University of California.

Liivoja, R. (2015). Technological change and the evolution of the law of war. *International Review of the Red Cross*, *97*(900), 1157-1177.

Lin, H. y Kerr, J. (2017). *On cyber-enabled information/influence warfare and manipulation*. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680

Lin, P., Bekey, G. y Abney, K. (2008). *Autonomous military robotics: Risk, ethics, and design*. California Polytechnic State University, San Luis Obispo.

Lind, W. S. (2004, marzo 2). *Fifth generation warfare*. Recuperado de http://www.dnipogo.org/lind/lind_2_03_04.htm

Lind, W. S. (2004). Understanding fourth generation war. *Military Review*, *84*(5), 12-16.

Lind, W. S., Nightengale, C. K., Schmitt, J. F., Sutton, J. W. y Wilson, G. I. (1989). *The changing face of war: Into the fourth generation*. Recuperado de http://www.lesc.net/system/files/4GW+Original+Article+1989.pdf

López, C. (2007). La guerra informática. *Boletín del Centro Naval*, 817, 219-224.

López de Turizo y Sánchez, J. (2012). La evolución del conflicto hacia un nuevo escenario bélico. *El ciberespacio: nuevo escenario de confrontación*, 126, 117-167.

Lorents, P. y Ottis, R. (2010). Knowledge based framework for cyber weapons and conflict. En C. Czosseck y K. Podins (eds.), *Conference on Cyber Conflict Proceedings* (pp. 129-142). Tallin: CCD COE Publications.

Maggio González, G. (2013). *El sun tzu aplicado a la competencia por el mercado*. Madrid: Habilitas.

Mallick, P. K. (2009). *Principles of war: Time for relook*. Nueva Delhi: Center for Land Warfare Studies.

Manthorpe, W. H. (1996). The emerging joint system of systems: A systems engineering challenge and opportunity for APL. *Johns Hopkins apl Technical Digest*, *17*(3), 305-307.

Martí Sempere, C. (2006). *Tecnología de la defensa: análisis de la situación española*. Madrid: Instituto Universitario General Gutiérrez Mellado.

Masters, C. (2010, mayo 20). Cyborg soldiers and militarised masculinities. *Euozine*. Recuperado de http://www.eurozine.com/cíborg-soldiers-and-militarised-masculinities/

Matusitz, J. (2005). Cyberterrorism: How can American foreign policy be strengthened in the information age? *American Foreign Policy Interests*, *27*(2), 137-147.

Mayntz, R. (2004). *Organizational forms of terrorism: Hierarchy, network, or a type sui generis?* Recuperado de https://www.econstor.eu/handle/10419/19906

McKitrick, J., Blackwell, J., Littlepage, F., Kraus, G., Blanchfield, R. y Hill, D. (2001). The revolutions in military affairs. En B. R. Scheneider y L. E. Grinter (eds.), *Battlefield of the future: 21st century warfare issues* (pp. 65-98). Alabama: Air University Press.

Mehan, J. (2014). *Cyberwar, cyberterror, cybercrime and cyberactivism*. Cambridge: IT Gobernance.

Mestres, F. y Vives-Rego, J. (2016). Reflexiones sobre los cyborgs y los robots: evolución humana y aumentación. *Ludus Vitalis*, *20*(37), 225-252.

Metz, S. y Kievit, J. (1995). *Strategy and the revolution in military affairs: From theory to policy*. DIANE Publishing. Recuperado de http://ssi.armywarcollege.edu/pdffiles/00229.pdf

Millán Barbany, G. (2000). La conquista del espacio. En *Horizontes culturales: las fronteras de la ciencia: 1998* (pp. 207-220). Madrid: Espasa-Calpe.

Miller, J. H. (1997). Information warfare: Issues and perspectives. En R. E. Neilson (ed.), *Sun Tzu and information warfare: A collection of winning papers from the Sun Tzu art of war in information warfare competition* (pp. 145-167). Washington D. C.: National Defense University Press Publications.

Miller, R. A. y Kuehl, D. T. (2009). Cyberspace and the "First Battle" in 21st-century war. *Defense Horizons*, 68, 1-6.

Mills, E. (2010, febrero 23). Experts warn of catastrophe from cyberattacks. *CNET*. Recuperado de https://www.cnet.com/news/experts-warn-of-catastrophe-from-cyberattacks/

MIT Media Lab People (s. f.). *Hugh Her Biomechatronics*. Recuperado de https://www.media.mit.edu/people/hherr/overview/

Molander, R. C., Riddile, A., Wilson, P. A. y Williamson, S. (1998). *Strategic information warfare: A new face of war.* Santa Mónica: RAND.

Molano Rojas, A. (2009). *El nombre y la cosa: aportes al debate definicional sobre el terrorismo*. Bogotá: Escuela de Inteligencia y Contrainteligencia BG. Ricardo Charry Solano.

Montanari, L. y Querzoni, L. (eds.) (2014). *Critical infrastructure protection: Threats, attacks and countermeasures*. Tenace. Recuperado de http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf

Moteff, J., Copeland, C. y Fischer, J. (2003). Critical infrastructures: *What makes an infrastructure critical?* Washington D. C.: The Library of Congress.

Motoike, I. y Yoshikawa, K. (1999). Information operations with an excitable field. *Physical Review* E, *59*(5), 5354.

Münkler, H. (2005). *The new wars*. Cambridge: Polity Press.

Nagpal, R. (2002). *Cyber terrorism in the context of globalization*. Ponencia presentada en II World Congress on Informatics and Law, Madrid, España.

National Aeronautics and Space Administration (s. f.). *A pictorial history of rockets*. Recuperado de https://www.nasa.gov/pdf/153410main_Rockets_History.pdf

National Cyber Security Center (2014). *International case report on cyber security incidents: Reflections on three cyber incidents in the Netherlands, Germany and Sweden*. Estocolmo: National Cyber Security Center.

National Institute of Standards and Technology (2014). *Framework for improving critical infrastructure cybersecurity.* Maryland: National Institute of Standards and Technology.

National Institute of Standards and Technology (2017). *Framework for improving critical infrastructure cybersecurity*. Maryland: National Institute of Standards and Technology.

Nichiporuk, B. (1999). U.S. Military Opportunities: Information-warfare concepts of operation. En Z. Khalilazad y J. White (eds.), *The changing role of information in warfare* (pp. 179-216). Santa Mónica, CA: RAND.

Norman, D. (1997). An information-based revolution in military affairs. En J. Arquilla y D. Ronfeldt (eds.), *In Athena's camp: Preparing for conflict in the information age* (pp. 79-98). Santa Mónica, CA: RAND.

Novikov, D. A. (2016). *Cybernetics: From past to future*. Moscú: Springer.

Nye, Jr., J. S. y Owens, W. A. (1996). America's information edge. *Foreign Affairs*. Recuperado de https://www.foreignaffairs.com/articles/united-states/1996-03-01/americas-information-edge

Organisation for Economic Co-operation and Development (2008). *Protection of 'Critical Infrastructure' and the role of investment policies*

relating to national security. París: Organisation for Economic Co-operation and Development.

Ortega, L. F. (2012). La ciberseguridad y la ciberdefensa. En *El ciberespacio: nuevo escenario de confrontación* (pp. 35-70). Madrid: Ministerio de Defensa.

Ortiz, R. D. (1996). *Amenazas transnacionales a la seguridad, tecnología e ingobernabilidad: Colombia*. Ponencia presentada en IV Congreso Español de Ciencia Política y de la Administración, Granada, España.

Ottis, R. (2010). From pitchforks to laptops: Volunteers in cyber conflicts. En C. Czosseck y K. Podins (eds.), *Conference on Cyber Conflict Proceedings* (pp. 97-109). Tallin: CCD COE Publications.

Paul, C., Porche III, I. R. y Axelband, E. (2014). *The other quiet professionals: Lessons for future cyber forces from the evolution of special forces*. Santa Mónica, CA: RAND.

Páez, E. P. (2014). *La guerra cibernética en el nivel operacional* (Trabajo final integrador, Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Madrid, Colombia).

Peña Galbán, L. Y., Casas Rodríguez, L. y Mena Fernández, M. (2009). La guerra psicológica contemporánea: conceptos esenciales y características. *Revista Humnidades Médicas*, *9*(2). Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1727-81202009000200012

Perešin, A. (2007). Mass media and terrorism. *Medijska istraživanja*, *13*(1), 5-22.

Pollitt, M. M. (1998). Cyberterrorism: Fact or fancy? *Computer Fraud & Security*, *1998*(2), 8-10.

Porteus, H. (2010, octubre 7). *The stuxnet worm: Just another computer attack or a game changer?* Recuperado de https://lop.parl.ca/Content/LOP/ResearchPublications/2010-81-e.pdf

Press, G. (2015, enero 2). A very short history of the internet and the web. *Forbes*. Recuperado de https://www.forbes.com/sites/gilpress/2015/01/02/a-very-short-history-of-the-internet-and-the-web-2/#663ccb907a4e

Randell, B. (1980). The Colossus. En N. Metropolis, J. Howlett y G.-C. Rota (eds.), *A history of computing in the twentieth century: A collection of essays*. Massachusetts: Academic Press.

Richardson, D. (2001). *Stealth warplanes*. Minnesota: Zenith Press.

Rinaldi, S. M., Peerenboom, J. P. y Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, *21*(6), 11-25.

Rogers, J. D. (1998). Internetworking and the politics of science: NSFNET in Internet history. *The Information Society*, *14*(3), 213-228.

Rosenfield, D. K. (2009). Rethinking cyber war. *Critical Review*, *21*(1), 77-90.

Sampaio, F. (2001). *Ciberguerra: guerra eletrônica e informacional, um novo desafio estratégico*. Porto Alegra: Escola Superior de Geopolítica e Estratégia.

Sánchez, J. (2017). Restoring active memory (RAM). *Defense Advanced Research Projects Agency.* Recuperado de https://www.darpa.mil/program/restoring-active-memory

Sánchez Medero, G. (2008). Ciberterrorismo: la guerra del siglo XXI. *El Viejo Topo*, 242, 14-23.

Sánchez Medero, G. (2009a). Ciberguerra y ciberterrorismo: ¿realidad o ficción? Una nueva forma de guerra asimétrica. En F. A. Cuervo-Arango y J. d. Peñaranda Algar (coords.), *Dos décadas de posguerra fría: Actas de las I Jornadas de Estudios de Seguridad de la Comunidad de Estudios de Seguridad General Gutiérrez Mellado* (pp. 215-242). Madrid: Comunidad de Estudios de Seguridad General Gutiérrez Mellado.

Sánchez Medero, G. (2009b). Internet: una herramienta para las guerras en el siglo XXI. *Revista Política y Estrategia*, 114, 224-242.

Sánchez Medero, G. (2010). Los Estados y la ciberguerra. *Boletín de Información*, 317, 63-76.

Sánchez Medero, G. (2012). La ciberguerra: los casos de Stuxnet y Anonymous. *Derecom*, 11, 124-133.

Schneier, B. (2017, mayo 23). Who are the shadow brokers? *The Atlantic*. Recuperado de https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/

Schreier, F. (2015). *On cyberwarfare*. Ginebra: Centre for the Democratic Control of Armed Forces.

Shakarian, P. (2011). Stuxnet: Cyberwar revolution in military affairs. *Air & Space Power Journal*, 50-59.

Shakarian, P., Shakarian, J. y Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach*. Massachusetts: Chris Katsaropoulos y Benjamin Rearick.

Shea, D. A. (2003). *Critical infrastructure*: *Control systems and the terrorist threat*. Congressional Research Service. Recuperado de https://fas.org/irp/crs/RL31534.pdf

Shelton, H. H. (1998). Operationalizing Joint Vision 2010. *Military Review*, *78*(3).

Sierra Caballero, F. (2002). Guerra informacional y sociedad-red: la potencia inmaterial de los ejércitos. *Signo y Pensamiento*, *21*(40), 32-41.

Sierra Caballero, F. (2003). La guerra en la era de la información: propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicaciones. *Sphera Pública*, 3, 253-268.

Silberstein, G. E. (1992). Seizing the enigma: The race to break the German U-boat codes, 1939-1943. *History: Reviews of New Books*, *20*(4).

Siles González, I. (2007). Cibernética y sociedad de la información: el retorno de un sueño eterno. *Signo y Pensamiento, 26*(50), 84-99.

Simon, T. (2017). *Critical infrastructure and the internet of things.* Ontario: Centre for International Governance Innovation and Chatham House.

Simonetti, B. (2008). *Guerra cibernética*. Santa Maria: Universidade Federal de Santa Maria.

Singer, P. W. y Friedman, A. (2014). *Cybersecurity: What everyone needs to know.* Oxford: Oxford University Press.

Smith, G. S. (2004). Recognizing and preparing loss estimates from cyber-attacks. *Information Systems Security*, *12*(6), 46-57.

Steering Committee for Foundations for Innovation in Cyber-Physical Systems (2012). *Strategic R&D opportunities for 21st century, cyber-physical systems, connecting computer and information systems with the physical world*. Illinois: Foundation for Innovation in Cyber-Physical Systems.

Stein, G. J. (2001). Information war, cyberwar, netwar. En L. Grinter y B. Scheneider, *Battlefield of the future: 21st century warfare issues* (pp. 153-170). Alabama: Air University Press.

Stel, E. (2014). *Seguridad y defensa del ciberespacio*. Buenos Aires: Dunken.

Strange, J. (2005). *Centers of gravity & critical vulnerabilities: Building on the Clausewitzian foundation so that we can all speak the same language*. Virginia: Defense Automated Printing Service Center.

Sulaiman, R. (2005). Information warfare. *Global Information Assurance Certification Paper.* Recuperado de https://www.giac.org/paper/gsec/1870/information-warfare/103284

Taddeo, M. (2012a). An analysis for a just cyber warfare. En C. Czosseck, R. Ottis y K. Ziolkowski (eds.), *2012 4th International Conference on Cyber Conflict* (pp. 209-218). Tallin: NATO CCD COE Publications.

Taddeo, M. (2012b). Information warfare: A philosophical perspective. *Philosophy & Technology, 25*(1), 105-120.

Talking Exoskeletons with suitX Founder Dr. Homayoon Kazerooni (2016, febrero 12). Recuperado de https://www.roboticsbusinessreview.com/rbr/talking_exoskeletons_with_suitx_founder_dr_homayoon_kazerooni/

Téllez Acuña, F. R. (2016). Prefijo CIBER: arqueología de su presencia en la sociedad del conocimiento. *Investigación y Desarrollo*, *24*(1), 142-162.

Thayer Mahan, A. (1911). *Naval strategy*. Pensilvania: U.S. Marine Corps.

The Economist (2007, mayo 10). Estonia and Russia A cyber-riot. Recuperado de http://www.economist.com/node/9163598

The Economist (2010, julio 1). War in the fifth domain. Recuperado de http://www.economist.com/node/16478792

The U.S.-China Economic and Security Review Commission (2009). *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. The U.S.-China Economic. Virginia: Northrop Grumman Corporation.

The White House (2003). *The National Strategy to Secure Cyberspace*. Washington D. C.: The White House.

Thomas, T. L. (2003). Al Qaeda and the Internet: The Danger of "Cyberplanning". *Parameters*, 33, 112-123.

Thomas, T. L. (2007). Hizbulá, Israel, and Cyber PSYOP. *Isphere*, 30-35.

Thong, M. C. S. S., Howe, M. T. C. y Lee, M. N. W. J. (2012). Unmanned technology: The holy grail for militaries? POINTER, *Journal of the Singapore Armed Forces, 38*(4), 16-25.

Tibbetts, P. S. (2002). *Terrorist use of the internet and related information technologies* (Tesis de grado, School of Advanced Military Studies, Kansas, Estados Unidos).

Tisseron, A. (2014). Robotic and future wars: When land forces facetechnological developments. En R. Doaré, D. Danet, J. P. Hanon y G. de Boisboissel, *Robots on the battlefield: Contemporary perspectives and implications for the future* (pp. 3-18). Kansas: Combat Studies Institute Press.

Toffler, A. y Toffler, H. (1994). *Las guerras del futuro: la supervivencia en el alba del siglo XXI*. Barcelona: Plaza & Janés.

Toffler, A., Toffler, H. y Solana, G. (1994). *Las guerras del futuro: la supervivencia en el alba del siglo XXI*. Barcelona: Plaza & Janés.

Torres Sorian, M. (2009). *Terrorismo yihadista y nuevos usos de internet: la distribución de propaganda (ARI)*. Real Instituto El Cano. Recuperado de http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/ari110-2009

Trachtman, J. P. (2004). *Global cyberterrorism, jurisdiction, and international organization*. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=566361

Trafton, A. (2013, julio 25). *Neuroscientists plant false memories in the brain*. Recuperado de http://news.mit.edu/2013/neuroscientists-plant-false-memories-in-the-brain-0725

Trias, E. D. y Bell, B. M. (2010). Ciber esto, ciber aquello… ¿Y qué? *Air and Space Power Journal*, *22*(3), 77-87.

Tzu, S. (1999). *El arte de la guerra*. Bogotá: Panamericana.

Tzu, S., Von Clausewitz, K. y Musashi, M. (2016). *Genios de la estrategia militar* (vol. 1). Nueva York: Luis Alberto Villamarín Pulido.

Unión Internacional de Telecomunicaciones (2014). *La UIT publica las cifras de TIC de 2014*. Recuperado de http://www.itu.int/net/pressoffice/press_releases/2014/23-es.aspx#.WpauM0xFzIU

U.K. Office of Cyber Security (2009). *Cyber security strategy of the United Kingdom: Safety, security and resilience in cyber space*. Londres: Crown Copyright.

U.S. Army Cyber Command (2016a). *The facts: Cyber enlisted soldier careers*. Recuperado de http://www.arcyber.army.mil/Style20Library/ARCYBER%20Custom%20Assets/factsheets/ARCYBER%20fact%20sheet%20-%20Cyber%20Enlisted%20Careers%20%282March2016%29.pdf

U.S. Army Cyber Command (2016b). *The facts: Training for cyber soldiers*. Recuperado de http://arcyber.army.mil/Style%20Library/ARCYBER%20Custom%20Assets/factsheets/ARCYBER%20fact%20sheet%20-%20Cyber%20Training%20at%20CCOE%20(15March2016).pdf

U.S. Department of Defense (1996). *Joint Vision 2010*. Recuperado de http://webapp1.dlib.indiana.edu/virtual_disk_library/index.cgi/4240529/FID378/pdfdocs/2010/Jv2010.pdf

U.S. Department of Defense (2010). *Joint Publication 3.0*. Wahington D.C., Estados Unidos: Estado Mayor Conjunto.

USAF College of Aerospace Doctrine, Research and Education (1997). Three levels of war. En *Air and space power mentoring guide* (vol. 1). Maxwell AFB, AL: Air University Press.

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

Vargas Vargas, E. M. (2014). *Ciberseguridad y ciberdefensa: ¿qué implicaciones tienen para la seguridad nacional?* (Tesis de grado, Universidad Militar Nueva Granada, Bogotá, Colombia).

Vázquez Liñán, M. (2000). La propaganda de guerra en la internet. *Historia y Comunicación Social*, *5*, 53-74.

Velandia Mora, M. A. (2006). *Estrategias para construir la convivencia solidaria en el aula universitaria: trabajo en equipo y comunicación generadora de mundos*. Bogotá: Universidad Cooperativa de Colombia.

Verising (2009). Cyber Threats and Trends. IDEFENSE Topical Research Report, Estados Unidos.

Verton, D. (2004). *La amenaza invisible del ciberterrorismo*. Nueva York: McGraw Hill.

Warden, J. A. (1995). *The air campaign: Planning for combat*. Pensilvania: DIANE Publishing.

Wander Nascimento, J. (2003). *Ciberwar uma proposta gen érica de ações defensivas para a MB*. Mharina do Brasil. Escola de Guerra Naval.

Weimann, G. (2004). *Cyberterrorism: How real is the threat?* Washington D. C.: United States Institute of Peace.

Wilson, C. (2004). Information warfare and cyberwar: Capabilities and related policy issues. *CRS Report for Congress*. Recuperado de https://fas.org/irp/crs/RL31787.pdf

Wilson, C. (2005). *Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress*. Washington D. C.: Congressional Research Service.

Wilson, C. (2007). *Information operations, electronic warfare, and cyberwar: Capabilities and related policy issues*. Washington D. C.: Congressional Research Service.

Wisskirchen, G., Biacabe, B. T., Bormann, U., Muntz, A., Niehaus, G., Soler, G. J. y Von Brauchitsch, B. (2017). *Artificial intelligence and robotics and their impact on the workplace*. Londres: IBA Global Employment Institute.

Wittes, B. y Chong, J. (2014). *Our cyborg future: Law and policy implications*. Washington D. C.: Center for Technology Innovation at Brookings.

Wolthusen, S. D. (2003). *Asymmetric information warfare: Cyberterrorism critical infrastructures*. Ponencia presentada en Proceedings of the XV International Amaldi Conference of Academies of Science and National Scientific Societies on Problems of Global Security, Helsinki, Finlandia.

Work, R. O. y Brimley, S. (2014, enero 22). 20YY: *Preparing for war in the robotic age*. Recuperado de https://www.cnas.org/publications/reports/20yy-preparing-for-war-in-the-robotic-age

Zeng, D. y Wu, Z. (2014). From artificial intelligence to cyborg intelligence. *IEEE Intelligent Systems*, *29*(5), 2-4.

Zanini, M. (1999). Middle Eastern terrorism and netwar. *Studies in Conflict and Terrorism*, *22*(3), 247-256.

Zanini, M. y Edwards, S. J. (2001). The networking of terror in the information age. En J. Arquilla y D. Ronfeldt, *Networks and netwars the future of terror, crime, and militancy* (pp. 29-60). Santa Mónica: RAND.

Esta obra se editó en Ediciones USTA,
Departamento Editorial de la Universidad Santo Tomás.
Tipografía de la familia Sabón.
2018

El autor de esta obra sostiene que el ciberespacio puede considerarse como una nueva dimensión de acción humana para reproducir la guerra interestatal propia de las relaciones internacionales. Para su argumentación propone tres objetivos: primero, analizar la práctica de la guerra, sus elementos perennes y entender su relación con la tecnología; segundo, presentar las cualidades y los elementos que hacen del ciberespacio una nueva dimensión de acción humana óptima para reproducir la práctica de la guerra, y tercero, describir la naturaleza de la ciberguerra y las formas en las que se ha materializado en la vida real. Por último, el autor también evidencia la existencia de nuevos actores que buscan aprovechar las características de los enfrentamientos bélicos en el ciberespacio.

Este libro es un impulso a la labor investigativa y propositiva de otros académicos en lo ciberespacial y su relación con aspectos políticos vitales —como la seguridad y defensa nacional—, y una referencia necesaria para generar un debate sobre las nuevas responsabilidades del Estado con sus ciudadanos en el siglo XXI.

UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
FACULTAD DE GOBIERNO Y RELACIONES INTERNACIONALES