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)