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.
Se usó papel propalcote de 280 gramos para la carátula y
papel bond beige de 75 gramos para páginas internas.
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