Signo y Pensamiento
ISSN: 0120-4823
revistascientificasjaveriana@gmail.com
Pontificia Universidad Javeriana
Colombia

Sierra Caballero, Francisco
Guerra informacional y sociedad-red. La potencia inmaterial de los ejércitos
Signo y Pensamiento, vol. XXI, núm. 40, 2002, pp. 32-41
Pontificia Universidad Javeriana
Bogotá, Colombia

Francisco Sierra Caballero*

Guerra informacional y sociedad-red

La potencia inmaterial de los ejércitos

Ilustraciones de Andrés Borja

Desde una perspectiva genérica del fenómeno de la cibercultura, la guerra informacional representa un replanteamiento de raíz de la acción bélica, la estrategia y sistemas de mando, control e inteligencia, así como de la táctica y la organización militar, cada vez más dependientes del dominio y capacidad de destrucción informativa y del conocimiento de los escenarios de representación del conflicto. Pero qué debemos entender por ciberguerra, cuál es su objeto particular y los rasgos específicos que la identifican como doctrina y acción militar. Por lo general, el uso

* Periodista, escritor y comunicólogo. Profesor-investigador del Departamento de Periodismo y Director del Centro Iberoamericano de Comunicación Digital de la Universidad de Sevilla. Dirección electrónica: **fsierra@us.es** y **fscaballero@yahoo.es**

habitual del término resulta excesivamente vago e impreciso, cuando no contradictorio, aplicado indistintamente junto a nociones equivalentes como infoguerra, guerra de redes, noopolítica o guerra digital. Un serio problema a este respecto es la definición clara y precisa de lo que debemos entender por guerra informativa. Pues, bajo similares denominaciones, se aprecian filosofías bélicas y estrategias y análisis divergentes en la planeación y desarrollo de las políticas de seguridad y control de las comunicaciones. Algunos autores, la mayoría por cierto, definen por ejemplo la guerra informativa como la aplicación militar de la informática y las nuevas tecnologías de la información con fines bélicos, además de recursos de prevención y control de sistemas de seguridad pública.

En esta línea, la noción de ciberguerra comprendería:

- El bloqueo tecnológico de los equipos de transmisión y almacenamiento de información.
- La destrucción interna de los sistemas de información y efectivos de las fuerzas enemigas.
- La manipulación de datos.
- El ataque electrónico a enlaces y sensores de las redes de seguridad.
- Los bombardeos de información y la intoxicación informativa.
- La penetración de los sistemas confidenciales de información.

Bajo la influencia de lecturas como "La tercera ola" de Alvin Toffler, este tipo de planteamientos dominante en el análisis de la ciberguerra relaciona el desarrollo tecnológico con la formulación de estrategias y tácticas adecuadas al nuevo entorno informativo, incorporando el mundo digital a las fuerzas armadas desde una visión determinista y restrictiva de la naturaleza de la actual revolución informacional. Así, por ejemplo, el Departamento de Defensa de EE.UU. define la guerra informativa como la estrategia y operaciones de información, desarrolladas en situaciones de crisis o conflicto para adquirir o promover objetivos específicos sobre adversarios concretos. En palabras de Henry y Peartree:

> IW can be waged in wartime within and beyond the traditional military battlefield. As a subret of IW, command and control warfare (C2W) is an application of IW in military operations that specifically attacks and defends the C2 target set. However, the capabilities and disciplines employed in C2W (psychological operations, deception, operations security, and electronic warfare) as well as other less traditional ones focused on information systems can be employed to achieve IW objectives that are outside the C2 target set"[1].

Este tipo de aproximaciones ha sido refrendada en proyectos como "Army After Next", "Sea Dragon" del Cuerpo de Marines o "New World Vistas" de la Fuerza Aérea de los Estados Unidos, privilegiando los programas tecnológicos como "Tactical Component Network" para el desarrollo del software de defensa o apuestas económicamente arriesgadas como el programa "Land Warrior", hoy de actualidad informativa con motivo de la guerra de Afganistán, y referencia recurrente para quienes piensan que, en efecto, la ciberguerra es una nueva forma de acción bélica de intervención puramente digital, basada solo en ataques remotos sobre vínculos, nodos y bases de datos de las fuerzas enemigas.

Tal concepción idealista, y tecnológicamente limitada, de la guerra informativa prevalece además como concepción dominante entre los investigadores y las autoridades militares estadounidenses, asociada a la suerte de la idea de los nuevos conflictos posmodernos como experiencias levemente trágicas o virtuales, como acciones bélicas —valga el oxímoron— de "no guerra" con escasa o irrelevante incidencia en relación con los

1 Henry, Ryan y Peartree, Edward, "Military Theory and Information Warfare" en *Center for Strategic and International Studies*, Parameters, 1998, p. 7.

eufemísticamente denominados "daños colaterales". Así por ejemplo, en "Information Operations" (FM 100-6), El Pentágono define la ciberguerra como un medio de prevención o eliminación de la necesidad de empleo de tropas de combate como recurso y estrategia auxiliar en la resolución de conflictos, reduciendo considerablemente, en su defecto, el número de bajas y pérdidas humanas y materiales, al reducir de forma significativa el tiempo de confrontación merced a la integración de iniciativas diplomáticas, económicas y militares con el uso inteligente de la información y el conocimiento, en una descripción de la guerra que más responde al imaginario ciberpunk y fantástico de las ensoñaciones digitales, difundidas mundialmente por el universo animado de la industria cultural norteamericana, que al verdadero rostro de las guerras imperiales contemporáneas.

Frente a esta concepción idílica de guerras indoloras y muertos virtuales, en la frontera de la cultura y la sociedad, sin hombres, proyectada por la utopía cibernética del pensamiento científico-técnico decimonónico, otros investigadores coincidimos, por contra, en reconocer con la emergencia de la cibercultura un nuevo modelo de articulación social que modifica radicalmente no solo las formas y medios para la guerra, sino, desde luego, los parámetros de observación y organización de los ejércitos, más allá de las visiones tecnológicamente deterministas al uso y de las fantasías virtuales de la sociedad espectacular.

Desde nuestro punto de vista, el principal reto que plantea la cibercultura es la necesidad de transformar el papel de las fuerzas armadas en la sociedad, a partir del lenguaje de los vínculos y del principio universal de conexión, esencial en toda dialéctica informativa, así como en la concepción de toda nueva experiencia cultural. En otras palabras, Internet más que un instrumento y un espacio para la guerra, es un poderoso sistema de reflexividad que plantea un nuevo horizonte de conocimiento y acción. Por ello, frente a la postura de tratar la complejidad creciente de los conflictos en torno a la información y la comunicación social, desde la simplificación reduccionista o instrumental de modelos lineales, sistemas centralizados jerárquicos y explicaciones monocausales, es necesario pensar respuestas multipolares, desarrollar modelos dialécticos y políticas de defensa orientadas por la descentralización, la apertura y la integración polivalente de espacios, matrices sociales y medios diversos de organización y acción social.

Atendiendo a las nuevas bases fundamentales de la sociocibernética, en el presente artículo se apuntan algunas ideas y críticas estratégicas del pensamiento contemporáneo sobre la ciberguerra señalando los principales problemas y contradicciones de una doctrina bélica —la estadounidense— ajena a las radicales consecuencias del nuevo ecosistema informativo que emerge con la revolución digital.

El lenguaje de los vínculos

Principio de conectividad y nueva topología

En un análisis prospectivo sobre los escenarios de futuro que previsiblemente introducirá Internet, el profesor Francisco Marín advierte que toda política de defensa y estrategia militar pasa, en la actualidad, por la consideración de al menos cuatro problemas fundamentales que alteran significativamente las formas de planeación de la guerra:

a) La presentación en tiempo real de información sobre los conflictos difundida por ciudadanos y observadores sobre el terreno, que limita la acción mediadora del ejército y sus servicios de propaganda, así como la eficacia de los filtros aplicados en guerras como la de Granada o el Golfo Pérsico.

b) La ruptura de los modelos informativos tradicionales, multiplicadora de las fuentes y técnicas de producción de mensajes, que hace más compleja y difícilmente controlable la desinformación.

c) La velocidad del proceso información/decisión/acción, que obliga a las autoridades a planificar las crisis sobre la marcha, previendo estrategias anticipadas a partir de nuevos modelos de gestión.

d) La emergencia de grupos organizados militarmente en la red, bajo el anonimato, cuando no la invisibilidad, para las fuerzas públicas, que pueden desestabilizar y generar situaciones caóticas en perjuicio de los intereses estratégicos de las naciones[2].

La naturaleza tramada de tejidos múltiples del ciberespacio, plantea a este respecto la necesidad de nuevas estrategias en situaciones de crisis en función de la cultura de la red, con el consiguiente cambio de estilos y formas de organización del ejército, por fórmulas más flexibles y polivalentes en el desempeño de las funciones de sus miembros y unidades de mando, abriendo incluso la puerta a la gestión colectiva y democrática de las decisiones por la imperiosa necesidad de la integración coordinada de la información con el concurso en la toma de decisiones a altos niveles y en los escalafones inferiores de mando y control. Como veremos, la dialéctica de observación, orientación, decisión y acción, se ha acelerado a tal grado, y expandido de forma tan diversa y compleja, que requiere el protagonismo de múltiples actores e instancias oficiales. Claro que, al mismo tiempo, esta disposición aperturista de Internet es propicia para las intromisiones, delitos y sabotajes de todo tipo.

El espacio de las redes no solo permite la flexibilidad y eficiencia organizativas sino también la invisibilidad y ocultación de las operaciones clandestinas. Ejemplos no faltan a este respecto: desde el primer atentado a las Torres Gemelas de Nueva York, organizado a través de las redes de información cifrada, a la guerra informática de grupos como Aun Shinzikyo o la propagación del terrorismo ultraderechista que prolifera en la red. Y es que Internet es, como antaño la prensa, un potente dispositivo de organización y acción social, además de un medio eficaz para campañas de solidaridad como "Sarajevo vivo, Sarajevo en línea" o de propaganda como la del EZLN.

Podemos decir, en definitiva, que el ciberespacio inaugura una nueva lógica de los conflictos, introduciendo una representación topológica de la guerra, desconocida o más bien ignorada hasta la fecha, en la medida que Internet expande y multiplica las formas de acción del ejército en un espacio sin fronteras, virtual, incierto, continuamente en proceso de cambio, difuso, que no puede, desde luego, ser aprendido a partir de modelos de racionalización cartesianos.

En efecto, el primer principio para observar en la ciberguerra es el de la lógica de organización consustancial a la dialéctica informativa, lógica dispersa, difusa, disipativa que, como el proceso general de globalización, da cuenta de una

.....

2 Marín, Francisco, "Nuevas tecnologías y conflictos en la era multimedia", en Contreras, Fernando y Sierra, Francisco (Ed.), *Culturas de guerra. Medios de información y violencia simbólica*, (en prensa), 2001.

actividad prolífica no reductible a esquemas o cartografías bidimensionales. Antes bien, la dinámica informacional exige modelos de análisis y organización flexibles y complejos. La necesidad de coaliciones y fuerzas conjuntas, la integración operativa de agencias diversas, las nuevas reglas de combate expuestas a la mirada atenta de los medios de comunicación en directo, las labores de inteligencia en un mundo integrado o la reducción del tiempo de información y acción militar justifican, más que de sobra, la idoneidad y exigencia de una cultura militar flexible y descentralizada, capaz de afrontar los complejos conflictos contemporáneos en entornos crecientemente confusos, caóticos y dispersos. No es viable, en otras palabras, un sistema estable y plenamente coherente de organización y control militar. Entre otras razones, porque la lógica de convergencia y conectividad social de la nueva cibercultura introduce procesos sociocibernéticos no lineales, simultáneos, autopoiéticos, solo comprensibles desde la cultura de la adaptación y el aprendizaje permanentes. Pensar un sistema de seguridad estable y totalmente eficaz, solamente es posible suprimiendo Internet, y esta solución no es, lógicamente, una alternativa razonable, pese a excepciones particulares como la de los Emiratos Árabes o Corea del Norte.

Es imprescindible por tanto una nueva política de la información, una nueva cultura informativa. La dinámica transformadora de los sistemas informáticos hace que muchas de las tácticas y estrategias militares resulten inapropiadas, obsoletas, incapaces de abordar la dinámica vertiginosa de la información. La guerra en tiempo real, basada en la gestión de los procesos de explotación informativa a través de redes telemáticas, no solo ha promovido el desarrollo de Internet y mucho antes de las plataformas espaciales de satélites de teledetección y vigilancia geoestratégica, sino más allá aún la conciencia de la necesidad de una cultura bélica basada en medios, políticas de vigilancia, transmisión y control de las comunicaciones civiles global y permanente.

En esta nueva cultura, el factor tiempo es vital. Si, como decimos, en la empresa postfordista, el valor del *stock* es reducido a la mínima proporción, los ejércitos de la sociedad-red se ven igualmente expuestos a la necesidad de desarrollar una estrategia de máxima comprensión del tiempo, demostrando una capacidad de intervención rápida y flexible plenamente funcional, por otra parte, a la lógica de la producción noticiosa.

El éxito de la guerra depende, a este respecto, de la capacidad de control de la opinión pública y de dominio en la intensidad y orientación temática de las noticias a cargo de la cobertura informativa por los medios, privilegiando el objetivo de mostrar el acontecimiento inmediatamente, con la consiguiente ocultación del proceso de hipermediatización, que hace posible la resolución exitosa de los conflictos. Luego, "la capacidad para controlar la velocidad, especialmente en la informática y los espacios inmateriales se ha hecho primordial [...] Estas opciones diseñan una estrategia que no permite evitar sistemáticamente los enfrentamientos violentos y la gestión del combate, pero que favorece la selección de empresas, la economía en vidas humanas y una gestión más flexible de los conflictos que hay que justificar ante una opinión pública y unos responsables políticos cada vez más informados"[3].

La idea de la guerra en tiempo real es, en este punto, complementaria y plenamente funcional para la narrativa multimedia dominante en la infosfera audiovisual, al mostrar la historia mientras se hace, bajo la retórica espectacularizante y trivial del infoentretenimiento. No obstante, la aplicación, de esta lógica discursiva con fines militares no es en modo alguno sencilla. La complejidad del teatro de operaciones en la sociedad global torna complicada la acción militar, sobre todo si consideramos que el ciberespacio multiplica los actores y fuentes de información involucrados.

La diversidad de satélites y redes Intranet de comunicación, los numerosos tipos de radiotransmisores móviles y canales convencionales de difusión de información, junto a las múltiples formas de comunicación grupal e interpersonal

3 Najman, Maurice, "Estados Unidos prepara las armas del Siglo XXI" en *Le Monde Diplomatique*, Febrero, 1998, p. 4.

autónomas, dispersan y complican los frentes de combate instaurando una lógica de la guerra de flujos invisible y poderosa, pero también incontrolable, que favorece la acción encubierta de las fuerzas enemigas y las formas irregulares de guerra, la contrainformación y la propaganda.

Paradójicamente, por tanto, la guerra informacional, lejos de ser una forma eficaz de control y perfeccionamiento del arte de la guerra, multiplica los riesgos e incrementa el grado de incertidumbre en la sociedad global de la información. Como bien apunta el profesor Gérard Imbert, en una sociedad como la occidental que todo —y tanto— lo ordena y planifica, que se alimenta de previsiones, simulaciones de toda índole (económicas, estadísticas, meteorológicas, políticas y, desde luego, militares), que se esfuerza tanto por reducir el grado de imprevisibilidad de la actualidad (la información como proceso formal es una ordenación del caos imperante) es grande la tentación de desorden. Y mayor, si cabe, en el caso de conflictos y crisis bélicas, la posibilidad de descontrol comunicacional.

Dependencia y vulnerabilidad
El efecto Heisenberg

El paso de las HUMINT (fuentes humanas de inteligencia) a las TECHNIT (inteligencia organizada en torno a los medios tecnológicamente sofisticados) prefigura un nuevo orden político-militar en las sociedades de la información que, al tiempo que organiza y desarrolla las capacidades de mando, control y conocimiento de los ejércitos, asume al mismo tiempo la creciente incertidumbre y la crisis de confianza de los poderes públicos como rasgos más destacados de las denominadas "sociedades de riesgo" (Ulrich Beck), tal y como ha quedado por ejemplo en evidencia tras los atentados del 11 de septiembre.

La noción de red se asocia, a este respecto, informacionalmente, a una visión del sistema mundial como un espacio caótico, amenazado por múltiples desestabilizaciones, conflictos locales, fisuras, desórdenes y terrorismos varios. No es el momento, en esta ocasión, de discutir las consecuencias culturales de este planteamiento en el discurso público, aspecto este que hemos venido analizando en otros trabajos[4]. Centrémonos pues en el problema o limitación esencial de la ciberguerra: la vulnerabilidad de los sistemas de información o, desde una perspectiva más genérica, el problema del efecto Heisenberg.

Parece claro, por lo expuesto hasta ahora, que la creciente dependencia tecnocomunicacional de los ejércitos da lugar a graves problemas de inseguridad que atañen no solo a la política militar y de defensa, sino incluso a la estabilidad social y económica. El peligro de un "Pearl Harbor" electrónico que informes como "Strategic Information Warfare : A New Face of War" de The Rand Corporation vienen analizando desde hace años, apunta precisamente en dirección al potencial peligro de la anulación e interferencias de los puntos de interconexión electrónica que gobiernan el desarrollo y organización de las sociedades

4 Sierra, Francisco, *Los profesionales del silencio. La información y la guerra en la doctrina de EE.UU.*, Editorial Iru, Guipúzcoa, 2002.

posmodernas, expuestos como están los sistemas de seguridad digitales a todo tipo de amenazas, derivadas de la creciente apertura sistémica de las sociedades de comando informacional, cuyo desarrollo depende de la creciente diferenciación, del cambio acelerado y continuo y la inevitable flexibilidad organizativa, exigencias éstas paradójicamente más que propicias para las turbulencias y violencias múltiples.

Tal y como advierte James Adams :

> "Si el nuevo mundo es tan distinto y amenazante, eso se debe a la destrucción de las antiguas fronteras. A medida que éstas desaparecen en el ciberespacio, el concepto mismo de la seguridad económica se vuelve más esquivo. La Era de la Información presenta una serie de desafíos nuevos a los gobiernos habituados a defender una estructura como la nacional. Para afrontarlos se necesitarán nuevas defensas, lo cual requerirá a su vez una mayor capacidad ofensiva"[5].

Esto es, al sufrir múltiples amenazas no tradicionales por la extensión a través de las fronteras y del tiempo de las formas de guerra y las organizaciones criminales, las fuerzas armadas se ven impelidas a incrementar su potencia de fuego y capacidad de gestión y prevención de los conflictos. De ahí la insistencia de la doctrina de la ciberguerra en la superioridad informativa.

El objetivo común de las políticas militares hoy es la dominación informativa antes y durante el desarrollo de maniobras en el teatro de operaciones. La nueva estrategia bélica de seguridad nacional comprende, por ello, como una prioridad el desarrollo de un proceso de apertura *(free flow information)* y de control continuado y flexible frente a la habitual doctrina de contención activa de la guerra fría. El objetivo político-militar, en suma, es el dominio de las redes de información y la implantación de un sistema de vigilancia total y permanente en el control de las fuentes de información, la identificación del enemigo y las acciones encubiertas, la supervisión de las comunicaciones públicas y privadas y el conocimiento tecnológico. Esta política hace necesaria la integración de la estrategia y las operaciones militares con la industria electrónica en el diseño de la arquitectura mundial de las telecomunicaciones, impulsando una cooperación estrecha con los "señores del aire", pues, por más que se desarrollen los sistemas de comunicación militares, la vigilancia del espacio depende de plataformas, satélites y sistemas de información públicos y privados que no están sujetos al control y uso militar. Un elemento crucial para controlar los riesgos de gestión y desarrollo de la política de seguridad en la era de la información consiste por tanto en vincular en plataformas comunes con el sector privado los sistemas de protección y control informacional, atendiendo los puntos vulnerables que las redes e infraestructuras de información de la administración del Estado y de los operadores privados comparten por igual. Se trata, en definitiva, de hacer efectiva la superioridad informativa en la capacidad de colectar, procesar y difundir un flujo continuo de información, controlando por anticipado la capacidad de inteligencia y conocimiento del enemigo sobre las fuentes, las operaciones y los actores involucrados en el conflicto.

Así, al menos, se viene planteando por parte de Estados Unidos que, desde un análisis global de la guerra y las políticas de defensa, ha desplegado un poderoso sistema de vigilancia y control planetario de la información en torno a centros como Fort Meade, tejiendo mundialmente dispositivos de espionaje y gestión de información y conocimiento en función de sus intereses estratégicos mediante un amplio y nutrido cuerpo de funcionarios (informáticos, lingüistas, relaciones públicas, analistas de sistemas, comunicólogos, psicólogos, ingenieros...) que hoy cubren todas las áreas y formas de comando, control, comunicaciones e inteligencia imaginables.

A partir especialmente del Plan Nacional para proteger el Ciberespacio de la administración Clinton, el proyecto de Dominación Global de la Información se ha traducido así en un eficaz

5 Adams, James, *La próxima guerra mundial. Los ordenadores son las armas y el frente está en todas partes*, Granika, Buenos Aires, 1999, p. 417.

control panóptico de comunicación e inteligencia peligrosamente centralizado por el ejército estadounidense y agencias como el Centro de Protección de la Infraestructura Nacional o la *National Imagery and Mapping Agency* dependientes de Estados Unidos, hoy además reforzado con la "Combating Terrorism Act" (2001) o proyectos como "Cyberspace Electronic Security Act". Tales iniciativas se justifican, por lo general, por la multiplicación de accesos y puntos de interconexión, la diversificación de usuarios y amenazas potenciales y la apertura liberalizada de los servicios y operadores en las redes de telecomunicaciones. Así, "la proliferación de fuentes de información elaborada es acompañada por la reducción del número de fuentes que la brindan en bruto. La proliferación de los métodos para controlar el flujo es compensada con creces por el desarrollo de sistemas que permiten a los recolectores de información comunicarse (y dominar la comunicación mundial) a voluntad"[6].

La retórica de la ciberguerra despliega, en definitiva, un discurso tecnológicamente reduccionista que pretende equiparar la acción bélica a un problema de control y organización de los procesos informativos, esto es, a un problema básicamente de superioridad infotécnica. Se piensa, y con fe se cree, que existe una relación lineal entre superioridad informativa y éxito de las operaciones militares. A diferencia de la guerra de maniobras, el dominio de la información sobre la estrategia, recursos, maniobras y operaciones del adversario garantizaría, según esto, un eficaz despliegue de la fuerza y la consiguiente realización de los objetivos básicos del mando militar. Y esto solo es posible con la "posesión" de un conocimiento preciso del teatro de operaciones y un dominio tecnológicamente superior del arte de la guerra, basada en la información y la inteligencia.

Ahora bien, el problema de la actual doctrina de seguridad pública es que participa de una filosofía del control informativo ajena a la dialéctica contemporánea de la sociedad digital, por su empeño en preservar un control total y permanente sobre los flujos y sistemas de información y conocimiento de las nuevas redes mundiales de poder, ignorando la lógica ambivalente del proceso informativo que por principio impide o limita toda estrategia de control unilateral.

Si, como sabemos, la información es antes que un producto un proceso transitivo y dialógico de interacción, la superioridad informativa sólo puede ser relativa, nunca absoluta, y está sujeta además a amplios márgenes de error, incertidumbre o azar. Entre otras razones porque quien quiere disfrazar sus comunicaciones a través de Internet puede hacerlo con bastante facilidad sin riesgo de ser sorprendido. Las técnicas de cifrado de información pueden ser tanto utilizadas por grupos terroristas como por el gobierno y las fuentes regulares del ejército. "Esta es precisamente una de las paradojas peligrosas de la Guerra Informativa. Cuanto más eficiente se es en el ataque, más vulnerable se vuelve uno al ataque"[7].

Hoy por ejemplo, los nuevos guerreros de la infosfera pueden, en cualquier momento, poner en peligro los dispositivos de defensa cibernética por acciones y efectos virales. En respuesta, los gobiernos y agencias de inteligencia tratan de desarrollar sofisticados medios de captación y re-

6 Ibíd., p. 438.
7 Ibíd., p. 236.

gistro de datos que no dejan de multiplicar las incertidumbres y riesgos de intervención. Pues una de las leyes universales de la información es precisamente su carácter indeterminado y ambivalente.

La información es tanto entrópica como neguentrópica: es un recurso para la acción y organización social, pero también (información es la diferencia que crea una nueva diferencia) un medio de transformación sistémica: es condición de todo orden tanto como cambio y motivo de alteraciones imprevisibles en el interior de todo sistema. La paradoja de la información es, en este sentido, la paradoja entrópica del universo en el que vivimos : a medida que los canales y flujos de información incrementan su capacidad de difusión y procesamiento de información, el nivel de incertidumbre, la capacidad de inteligencia y control militar resultan más difusas y a la vez limitadas.

En la visión tradicional de las fuerzas militares, la información es sin embargo considerada un simple producto, un mensaje codificado para la transmisión y organización de la actividad de defensa, anulando la dimensión dinámica, transitiva y dialéctica consustancial a todo proceso informativo. La información, según esta concepción militar, es solo un elemento complementario de transmisión e instrucción por las líneas de mando y comunicaciones que, de manera auxiliar, ayuda a librar eficazmente las guerras no convencionales. Más que una nueva dimensión o paradigma de la doctrina militar, se trataría por tanto de hacer la guerra según el modo convencional con nuevos medios, no a partir de nuevas bases. Es habitual, en consecuencia, una lectura de la noción de ciberguerra restringida, basada en la comprensión instrumental de la tecnología de la información, cuando la centralidad de los procesos informativos y las redes telemáticas aconsejaría, según hemos tratado de explicar, una filosofía de organización y desarrollo de la cultura y planeación militar de los ejércitos diametralmente distinta, máxime considerando el grado de coordinación y complejidad de las variables involucradas en toda política de seguridad.

En un tiempo en el que la crisis de las organizaciones, la cultura de la seguridad en torno a los sistemas de información y control social, necesitan ser reformulados ante la inminencia de la vulnerabilidad cibernética que amenaza con minar las bases de confianza que rigen nuestras sociedades, parece cuando menos lógico pensar en la pertinencia de otra mirada distinta a la paranoica asunción de la cultura del dominio informacional en las redes telemáticas.

La cuestión, a nuestro entender, es si seguimos pensando en la información como un problema más de organización de las políticas de defensa o, como dice Hayden, como una nueva topología, un nuevo lugar y paradigma de la cultura de seguridad. Esta última interpretación se nos antoja, por las razones antes expuestas, el punto de partida más adecuado para acometer los retos militares de la ciberguerra.

Bibliografía

Adams, James, *La próxima guerra mundial. Los ordenadores son las armas y el frente está en todas partes*, Granika, Buenos Aires, 1999.

Aguirre, Mariano y Mathews, Robert, *Guerras de Baja Intensidad*, Fundamentos, Madrid, 1989.

Aldrich, Richard W., *Cyberterrorism and computer crimes: issues surrounding the establishment of an international legal regime*, USAF, Institute for National Security Studies, Colorado, 2000.

Brown, M.C., *The Revolution in Military Affairs: The Information Dimension*, UA, AFCEA, 1996.

Bunker, Robert J., "Epocal Change: War Over Social and Political Organization", *Parameters*, US Army War College Quaterly, 1997.

Caldera, Louis y Shinseki, Eric, "La visión de un ejército transformado" en *Military Review*, Septiembre-Octubre, 2000.

Campen, Alan D. et al (Comp.), *The First Information War*, AFCEA International Press, Fairfax, 1992.

Contreras, Fernando, *El Cibermundo. Dialéctica del discurso informático*, Alfar, Sevilla, 1998.

Friedman, George y Meredith, *The Future of War*, Crown, Nueva York, 1996.

Guisnel, J., *Guerres dans le Cyberespace*, La Decouverte, París, 1997.

Libicki, Martin, *Defending Cyberspace and Other Metaphors*, National Defense University, Washington, 1997.

Harris, Phil, "Communication and Global Security: The Challenge for the Next Millenium", en Golding, Peter y Harris, Phil (Ed.), *Beyond Cultural Imperialism. Globalization, Communication and the New International Order*, Sage, Londres, 1999.

Henry, Ryan y Peartree, Edward, "Military Theory and Information Warfare" en *Center for Strategic and International Studies*, Parameters, 1998.

Howard, Michael, *The Invention of Peace: Reflections on War and International Order*, Profile Books, Londres, 1999.

Kaldor, Mary, "Comprender el mensaje del 11 de septiembre", en El País, jueves 27 de septiembre de 2001, p.25.

Kaplan, Robert D., *La anarquía que viene. La destrucción de los sueños de la posguerra fría*, Ediciones B, Barcelona, 2000.

Klare, Michael, "Washington veut pouvoir sur tous les fronts" en *Le Monde Diplomatique, Manière de Voir*, número 53, Septiembre-Octubre, 2000.

Klare, Michael y Kornbluch, Peter (Coord.), *Contrainsurgencia, proinsurgencia y antiterrorismo en los 80. El arte de la guerra de baja intensidad*, CNCA/Grijalbo, México, 1999.

Marín, Francisco, "Nuevas tecnologías y conflictos en la era multimedia", en Contreras, Fernando y Sierra, Francisco (Ed.), *Culturas de guerra. Medios de información y violencia simbólica*, (en prensa), 2001.

Metz, Steven, "Previendo el futuro: el Ejército y los conflictos en países anárquicos", en *Military Review*, Septiembre-Octubre, 1994.

Milcom 97, "Space as an Area of Vital National Interest", Milcom 97, Hyatt Regency Hotel, Monterrey, CA, 3 de Noviembre de 1997.

Molander, Roger C. et al, *Strategic Information Warfare: A New Face of War*, Rand Corporation, Santa Mónica, 1996.

Najman, Maurice, "Estados Unidos prepara las armas del Siglo XXI" en *Le Monde Diplomatique*, Febrero, 1998.

O'Neill, Bard, *Insurgency and Terrorism. Inside Modern Revolutionary Warfare*, Brassay's, Washington, 1990.

Quirós, Fernando y Sierra, Francisco (Dir.), *Comunicación, globalización y democracia. Crítica de la economía política de la comunicación y la cultura*, Comunicación Social Ediciones y Publicaciones, Sevilla, 2001.

Romm, Joseph, *Defining National Security: The Nonmilitary Aspects*, Council on Foreign Relations Press, Nueva York, 1993.

Russett, Bruce, *Controlling the Sword: The Democratic Governance of National Security*, Harvard University Press, Cambridge, 1990.

Schiller, Herbert I., "El dominio de las redes electrónicas mundiales", en *Le Monde Diplomatique*, Agosto/Septiembre, 1998.

Schwartzstein, Stuart, *The Information Revolution and National Security*, Center for Strategic and International Studies, Washington, 1996.

Shaker, S. y Wise, A.R., *War Without Man*, Pergamon Press, Washington, 1988.

Sierra, Francisco (Coord.), *Comunicación e insurgencia. La información y la propaganda en la guerra de Chiapas*, Editorial Iru, Guipúzcoa, 1997.

Sierra, Francisco, "Propaganda y Nuevo Orden Mundial" en *Historia y Comunicación Social*, número 4, Universidad Complutense de Madrid, 1999.

Sierra, Francisco, "El discurso de la nueva doctrina de seguridad pública. Guerra informativa y sociedad televigilada" en *Voces y Culturas*, número 15-I Semestre, Barcelona, 2000.

Sierra, Francisco, *Los profesionales del silencio. La información y la guerra en la doctrina de EE.UU.*, Editorial Iru, Guipúzcoa, 2002.

Snow, Donald M., *Peacekeeping. Peacemaking and Peace-Enforcement: The US Role in the New International Order*, Carlisle Barracks, Pennsylvania, 1993.

Snyder, Alvin, *Warriors of Disinformation*, Arcade, Nueva York, 1995.

Sullivan, G. y Dubik, J., *Land Warfare in the 21st. Century*, Carlisle Barracks, Pennsylvania, 1993.

Sullivan, G. y Dubik, J., "Cómo se librará la guerra en la Era de la Información" *Military Review*, Mayo-Junio, 1995.

Tello, Angel, *Conflictos y comunicación en la globalización*, Ediciones de Comunicación, La Plata, 1999.

Toffler, A. y H., *Las guerras del futuro*, Plaza y Janés, Madrid, 1994.

Van Creveld, Martin, *The transformation of War*, The Free Press, Nueva York, 1991.

Van Creveld, Martin, *Technology and War*, Pergamon Press, Oxford, 1991.

Virilio, Paul, "La proliferación televisual", en *Le Monde Diplomatique*, Marzo, 1998.

Weinberger, Caspar y Schweizer, P., *The Next War*, Regnery Publishing, Nueva York, 1997.

Whitaker, Reg, *El fin de la privacidad. Cómo la vigilancia total se está convirtiendo en realidad*, Ediciones Piados, Barcelona, 1999.

Young, Peter (Ed.), *Defence and the Media in Time of Limited War*, Fran Cass, Portland, 1992.