

Cyberwar y netwar

12 de febrero de 2001

La fiambarrera

(RAND Corporation)

SINOPSIS: La revolución de la información así como otras innovaciones organizativas asociadas, están alterando la naturaleza de los conflictos y los tipos de estructuras, doctrinas y estrategias militares necesarias. Este ensayo presenta dos conceptos para pensar sobre estas cuestiones: “cyberguerra” (cyberwar) y “guerra-en-red” (netwar).

Así como la industrialización llevó a guerras de desgaste, con el recurso a ejércitos masivos (así la Primera Guerra Mundial), y la mecanización permitió el predominio de una guerra de maniobras llevada a cabo por los tanques (así en la Segunda Guerra Mundial), la revolución de la información implica el auge de la cyberguerra, en la cual ni la masa de las tropas ni la movilidad servirá como factor decisivo; por el contrario, el contrincante que sepa más, que alcance a ver entre la niebla de la guerra y pueda mantener a su adversario cegado por ella, contará con ventajas decisivas. Las comunicaciones y la inteligencia siempre han sido importantes. Como mínimo la cyberguerra supone que cobrarán mayor importancia aun, hasta convertirse en equiparables e inseparables de la estrategia militar conjunta. En este sentido se parece a las nociones ya existentes de “guerra de información” que enfatizan el C₃I (alusión en inglés al conjunto de command, control, communications and intelligence: dirección, control, comunicaciones e inteligencia, en adelante C₃I). Sin embargo la revolución de la información implica efectos de largo alcance que obligan a sustanciales modificaciones en la organización militar y las distribuciones de fuerzas.

La cyberguerra puede ser para el siglo XX lo que la blitzkrieg fue para el XX. Proporcionará también una vía a los EEUU de incrementar la capacidad de golpear (“punch”) sin tener que inflacionar (“paunch”) los efectivos.

Así como la cyberguerra se refiere a conflictos librados en el campo de la información a un nivel militar, la “guerra-en-red” alude a luchas mayormente asociadas a conflictos de baja intensidad sostenidos por actores no-estatales, tales como terroristas, narcotraficantes, o distribuidores (proliferadores dice) en el mercado negro de armas de destrucción masiva. Ambos conceptos implican que los conflictos futuros se librarán más por “redes” que por “jerarquías”, y que aquel que mejor domine la forma “red” obtendrá mayores ventajas.

“El conocimiento debe transformarse en capacidad”-- Carl von Clausewitz, Sobre la guerra

MODOS EMERGENTES DE CONFLICTO

Supongamos que la guerra funcionara así: Pequeñas cantidades de fuerzas ligeras y de alta movilidad, derrotan y fuerzan a la rendición a grandes masas de fuerzas enemigas, atrincheradas con armamento pesado, con pocas pérdidas humanas por ambas partes. Las fuerzas móviles pueden hacer esto porque están bien preparadas, cuentan con espacio para maniobrar, concentran su fuego rápidamente en lugares inesperados y tienen sistemas superiores de mando, control e información, sistemas descentralizados que permiten iniciativas tácticas y que no obstante permiten a los comandantes centrales contar con una “inteligencia” y una visión de conjunto sin precedentes, a la hora de plantear opciones estratégicas.

La guerra ya no consiste en ver quien invierte más capital, trabajo o tecnología sobre el campo de batalla, sino en dilucidar quien cuenta con la mejor información sobre el campo de batalla. Lo que distingue a los vencedores es su dominio de la información —no sólo desde el punto de vista inmediato de poder localizar al enemigo, manteniéndose a sí mismo oculto, sino también en términos doctrinales y organizativos—.

La analogía es más bien la que se correspondería con un juego de ajedrez en el que uno ve el tablero entero, mientras que el oponente sólo puede ver sus propias piezas; uno puede ganar incluso si sucediera que el adversario empieza el juego con mayores fuerzas.

Puede parecer que estamos extrapolando la victoria de los EEUU en el Golfo Pérsico contra Irak, pero nuestra concepción está más inspirada por el ejemplo de los Mongoles del siglo XIII. Sus “hordas” fueron casi siempre inferiores en número a sus oponentes, sin embargo conquistaron y mantuvieron durante más de un siglo, el más grande imperio continental jamás visto. La clave para el éxito de los mongoles fue su absoluto dominio de la información sobre el campo de batalla. Atacaban donde y cuando ellos consideraban oportuno, y sus “jinetes flecha” mantenían comunicados diariamente a sus comandantes, a menudo separados cientos de kilómetros.

Incluso el Gran Khan, a veces a miles de millas de distancia, estaba al corriente de lo sucedido en el frente, en cuestión de pocos días.

Una vez diluida la amenaza galvanizante que suponía la Unión Soviética, hemos de contar que EEUU habrá de hacer frente a presiones internas que le obligaran a reducir sus efectivos militares. El tipo de guerra, de capacidad de combate que estamos esbozando, inspirado en el ejemplo mongol, aunque derivado fundamentalmente de nuestro análisis de la revolución de la información, podría permitir a América proteger sus intereses, e incluso los de sus más alejados aliados, con independencia de la talla y la fuerza de nuestros potenciales adversarios futuros.

El avance de la Tecnología y el Know-How

A lo largo de la historia, la doctrina, la organización y la estrategia militar, han sufrido profundos cambios, debido en parte a los avances tecnológicos. La Falange griega, la combinación de cañón y barco, las levas en masa, la “blitzkrieg”, el mando aéreo estratégico: la historia está llena de ejemplos en los cuales las nuevas tecnologías aplicadas a armas, propulsión, comunicaciones y transporte proporcionaron la base para cambios en organización, doctrina y estrategia que per-

mitieron a los innovadores evitar agotadoras batallas de desgaste y llegar en cambio a un orden de combate “decisivo”.

Hoy día una gran variedad de nuevas tecnologías están de nuevo sosteniendo y prometiéndole mayores innovaciones.

Las más interesantes apuntan hacia explosivos de alta carga no nucleares, municiones guiadas con sistemas de precisión, diseños escamoteadores de aviones, tanques y barcos, sistemas de combate radio–electrónicos, etc...

Además se están desarrollando sistemas de realidad virtual para simulación y entrenamiento. Muchos de estos avances se pueden incluir en la noción habitual de “revolución tecnológica militar” (RTM).

El futuro de la guerra —en concreto de la habilidad de los EEUU para anticiparse y resolver las situaciones de conflicto— será formado, en parte, por el modo en que estos avances sean considerados y adoptados.

No obstante, como los historiadores de lo militar han advertido con frecuencia, la tecnología permea la guerra pero no la gobierna. No es la tecnología por sí misma, sino más bien la organización de la tecnología, definida ampliamente, la que realmente importa.

Russel Weigley describe así la situación: “...la tecnología de la guerra no consiste sólo en instrumentos pensados fundamentalmente para el desarrollo de los combates. La habilidad de una sociedad para llevar a cabo una guerra depende de todas y cada una de las facetas de su tecnología: sus carreteras, sus vehículos de transporte, su agricultura, su industria, y sus métodos para organizar la tecnología”. Tal y como dice Van Creveld “detrás del hardware militar se encuentra el hardware general, y detrás de éste se encuentra una tecnología, un cierto know-how, así como un modo de entender el mundo y solventar los problemas que se nos plantean”.

Desde nuestro punto de vista, el giro tecnológico que ajusta con esta amplia definición es la revolución de la información. Dicha revolución es la que nos ha de traer los mayores cambios en la comprensión de la naturaleza de los conflictos y la guerra.

Efectos de la revolución de la información

La revolución de la información refleja el avance de las tecnologías de comunicación y proceso de información así como las innovaciones paralelas en teoría de la organización y la dirección. Enormes cambios se están produciendo en los modos de recoger, almacenar, procesar, comunicar y presentar la información; igualmente sucede en los modos en que las organizaciones son diseñadas para optimizar las ventajas de estos aumentos de información.

La información está convirtiéndose en un recurso estratégico que puede mostrar ser tan valiosos e influyente en la era postindustrial como lo fueron en la era industrial el capital y el trabajo.

Los sistemas de información y comunicación adecuadamente implementados, pueden mejorar la eficiencia de muchos tipos de actividad. Pero esta eficiencia mejorada no es ni el único, ni siquiera el mejor, de los resultados posibles. La nueva tecnología también está teniendo un efecto transformador en la medida en que desmantela viejos modos de pensar y funcionar, capacita para hacer las cosas de modos diferentes y sugiere cómo algunas tareas podrían ser realizadas mejor si se hicieran de un modo diferente. “Las consecuencias de las nuevas tecnologías pueden ser descritas y pensadas en un ‘primer nivel’ de eficiencia, o un ‘segundo nivel’ de efectos en el sistema social”.

La historia de las tecnologías previas demuestra que en los primeros tiempos de cualquier tecnología, se tiende a enfatizarlos efectos de eficiencia e infravalorar o desestimar los potenciales efectos sobre el sistema social. Los avances en las tecnologías relativas al “trabajo en red” permiten pensar en la gente, así como en las bases de datos y los procesadores como recursos de una red de trabajo (network).

“Muchas organizaciones están hoy instalando redes electrónicas por razones de ‘primer nivel’, de eficiencia. Los ejecutivos que están empezando a desplegar el correo electrónico y otras aplicaciones de trabajo en red pueden advertir los beneficios en eficiencia y reducción de tiempos para determinadas transacciones”.

Pero si vemos, más allá de la mera eficiencia, los cambios conductuales y organizativos, veremos el verdadero alcance de los cambios de “segundo nivel”.

Estas tecnologías pueden cambiar los modos en que la gente emplea su tiempo así como aquello sobre lo que saben y se preocupan.

La medida del efecto en que estas tecnologías afectarán a los modos en los que la gente piensa y trabaja conjuntamente —los efectos de “segundo nivel”— (Sproull and Kiesler, 1991: 15–16). La revolución de la información tanto en sus aspectos tecnológicos como no tecnológicos pone en funcionamiento fuerzas que cuestionan el diseño de muchas instituciones. Desbarata y erosiona las jerarquías alrededor de las cuales se estructuran normalmente las instituciones. Difunde y redistribuye el poder, a menudo en beneficio de aquellos que muchos considerarían los actores más pequeños o débiles. Cruza fronteras y replantea los límites de oficios y responsabilidades. Expande los horizontes espacio-temporales que los actores deben considerar. Así por lo general obliga a que sistemas cerrados tengan que abrirse. No obstante aunque todos estos resultados pueden complicar la vida a instituciones demasiado grandes y burocratizadas, de ahí no puede deducirse que la forma institución pero se haya devenido obsoleta.

Todo tipo de instituciones siguen siendo esenciales para la organización de la sociedad. Las instituciones más sensibles y ágiles adaptarán sus estructuras y procesos a la era de la información. Muchas evolucionarán desde las formas jerárquicas tradicionales hacia nuevos modelos de organización más flexibles y con estructura de red.

El éxito dependerá de la capacidad para entrelazar principios de funcionamiento jerárquicos con los propios del trabajo en red.

Mientras tanto los mismos cambios que cuestionan las instituciones, como el debilitamiento de las jerarquías, favorecen el crecimiento de redes de trabajo multi-organizacionales.

De hecho, la revolución de la información esta fortaleciendo la importancia de todo tipo de redes, como las redes sociales o las de trabajo. La forma de trabajo en red es bien diferente de la forma “institucional”.

Mientras que las instituciones (las más grandes, en particular) se construyen tradicionalmente en torno a jerarquías y tratan de actuar por cuenta propia, las redes de muchas organizaciones consisten en organizaciones, casi siempre pequeñas, o de partes de instituciones que se han interconectado para actuar conjuntamente. La revolución de la información favorece el crecimiento de tales redes al hacer posible que actores diversos y dispersos se comuniquen, se consulten, se coordinen y trabajen juntos incluso en medio de grandes distancias, y esto sobre la base de disponer de más y mejor información que la que nunca se había conseguido reunir. Estas cuestiones afectan directamente sobre la condición futura de lo militar, así como sobre la naturaleza de la guerra y el conflicto más en general.

Tanto la Cyberguerra como la Guerra–en–red son verosímiles

La tesis de este ensayo es que la revolución de la información provocará cambios tanto en los modos en los que las sociedades generan conflictos como en aquellos con los que las fuerzas armadas desarrollan una guerra.

Proponemos una distinción entre lo que llamamos “guerra–en–red” —conflictos de nivel social e ideológico (ideacional) sostenidos en parte mediante modos de comunicación propios de Internet— y la “cyberguerra” a nivel militar.

Admitimos la novedad de estos términos, quizá estén por llegar otros más ajustados. Pero, por ahora, ayudan a iluminar una distinción útil e identifican la amplitud de modos en los que la revolución de la información puede alterar la naturaleza del conflicto, así como el contexto y la conducción de la guerra.

Mientras que tanto la cyberguerra como la “guerra–en–red” pueden plantearse en torno a cuestiones de información y comunicaciones, en un nivel más profundo, ambas son formas de guerra sobre el “conocimiento”, sobre quien sabe qué, cuando, dónde y porqué, formas de guerra sobre cuan segura es una sociedad o un dispositivo militar en función de su conocimiento sobre sí misma y sus adversarios.

EXPLICAR LA GUERRA–EN–RED

La guerra–en–red consiste en un conflicto relacionado con la información a gran nivel, entre naciones o sociedades.

Implica intentar dañar o modificar aquello que un grupo de población, tomado como objetivo, sabe o cree saber sobre sí mismo y el mundo. Una guerra–en–red puede centrarse sobre la

opinión pública general o sobre la opinión de una elite, o sobre ambas. Puede implicar medidas de diplomacia públicas, de propaganda o campañas psicológicas, subversión política o cultural, sabotaje o interferencias sobre los media locales, infiltración en bases de datos y redes informáticas, así como esfuerzos que alienten movimientos disidentes o de oposición a través de dichas redes.

De modo que diseñar una estrategia para a guerra-en-red implica agrupar, desde una nueva perspectiva, una serie de medidas a las que quizá se había recurrido previamente, pero a las que no se había considerado en conjunto.

En otras palabras, la guerra-en-red representa un nuevo elemento en el espectro de conflictos que miden lo económico, lo político y lo social también como formas militares (militarizables) de “guerra”.

En contraste con las guerras económicas que atacan la producción y distribución de mercancías, o las guerras políticas que apuntan a las instituciones de gobierno y los dirigentes, las guerras-en-red se distinguirían por tener como objetivo la información y las comunicaciones.

Como otras formas de este espectro, las guerras-en-red serían principalmente no-militares, pero acaso podrían tener dimensiones que las hicieran deslizarse en el terreno de la guerra militar. Por ejemplo, una guerra económica puede implicar restricciones al comercio, “dumping” de precios, penetraciones ilícitas y subversiones de negocios y mercados en el país tomado como objetivo, el robo de tecnología... y nada de ello tendría porqué suponer la intervención de las fuerzas armadas. Sin embargo, una guerra económica también puede llegar a necesitar un bloqueo armado, un bombardeo estratégico de objetivos económicos y por tanto deslizarse hacia una guerra militar.

De igual manera, una guerra-en-red que pretende perjudicar las funciones de C₃I del enemigo, deviene, al menos en parte, lo que hemos llamado una cyberguerra.

Las guerras-en-red tomarán varias formas, en función de sus actores. Alguna puede darse entre los gobiernos de naciones-Estado rivales. De alguna forma los gobiernos de Cuba y los EEUU están ya metidos en una suerte de guerra-en-red, manifiesta en las actividades de Radio y TV Martí, por parte de los EEUU, y en las actividades de las redes y grupos de apoyo a Cuba en todo el mundo.

Otros tipos de guerra-en-red pueden surgir entre gobiernos y actores no-estatales, por ejemplo una guerra-en-red puede desatarse por los gobiernos contra grupos ilegales y organizaciones implicadas en terrorismo, proliferación de armas de destrucción masiva o trafico de drogas.

O por el contrario, la guerra-en-red puede ser librada contra las políticas de gobiernos específicos por parte de grupos reivindicativos y movimientos sociales implicados en cuestiones, por ejemplo, de medio ambiente, derechos humanos o cuestiones religiosas. Los actores no-estatales pueden o no estar asociados con otras naciones, y en algún caso pueden estar asociados vastas redes y coaliciones transnacionales.

Otro tipo de guerra-en-red puede darse entre actores no-estatales, rivales entre sí, acaso con gobiernos maniobrando desde los márgenes del conflicto para evitar que los daños colaterales afecten al interés nacional o quizá para apoyar a uno de los contendientes. Esta es el tipo más

improbable de guerra–en–red, pero los elementos para que se dé ya han aparecido, especialmente entre los grupos reivindicativos de todo el mundo.

Algunos movimientos se están organizando cada vez más en redes y coaliciones que desbordan las fronteras, identificándose más con el desarrollo de la sociedad civil (incluso de la sociedad civil global) que con sus naciones–Estado, y están usando tecnologías de información y comunicaciones muy avanzadas para reforzar sus actividades.

Este puede muy bien ser el territorio para los conflictos ideológicos futuros, y la guerra–en–red quizá la característica central.

La mayoría de las guerras–en–red probablemente serán no–violentas, pero hay que pensar que en los peores casos podrían darse escenarios de conflicto de baja–intensidad. Martin Van Creveld (1991: 197) considera esta opción cuando se preocupa porque “en el futuro, la guerra no se librará entre ejércitos, sino entre grupos que hoy llamamos terroristas, guerrillas, bandidos y ladrones, pero que sin duda reclamarán títulos más formales para describirse a si mismos”. Desde su punto de vista, la guerra entre estados disminuirá y el Estado, de hecho, se convertirá en una forma obsoleta de organización social. Nuestras opiniones coinciden en gran medida con las de Van Creveld, aunque no creemos que el Estado sea, siquiera potencialmente, una forma obsoleta. Más bien apostamos a que será transformado por estos desarrollos.

Algunas guerras–en–red implicarán opciones militares. Posiblemente estas vengan dadas en contextos relacionados con la proliferación nuclear, el tráfico de drogas y el anti–terrorismo, en función de las potenciales amenazas que estos suponen para el orden internacional y la seguridad nacional.

Por lo demás, tendencias sociales más amplias (por ejemplo, la redefinición de los conceptos de seguridad, los nuevos roles de los grupos reivindicativos, la confusión de los límites tradicionales entre lo militar y lo no–militar, lo público y lo privado, lo estatal y lo social) pueden hacer que se vean afectados los intereses de al menos algunas oficinas militares, por lo que éstas tendrían que implicarse en actividades de guerra–en–red.

Las guerras–en–red no son guerras reales, en su definición tradicional. Pero la guerra–en–red puede ser desarrollada como instrumento para evitar que una guerra real se desate.

La disuasión en un mundo caótico puede ser función de la presencia y la postura que adoptemos tanto en lo relativo a la fuerza como a lo cibernético.

Explicar la Cyberguerra

Con el término cyberguerra nos referimos a llevar a cabo, o prepararse para llevar a cabo, operaciones militares de acuerdo con principios relacionados con la información. Esto supone desbaratar, cuando no destruir, los sistemas de información y comunicaciones, entendidos ampliamente abarcando incluso la cultura militar, sobre la que depende el adversario para saber sobre sí mismo: quien es, donde está, qué puede hacer por tanto, por qué está luchando, qué amenazas debe enfrentar en primer lugar, etc... Significa intentar saberlo todo sobre el adversario, al tiempo que

se evita que éste averigüe cualquier cosa sobre uno mismo. Significa desequilibrar “la balanza de información y conocimiento” a favor propio, especialmente si el balance de fuerzas no está tan a nuestro favor. Significa usar el conocimiento de modo que menos capital y trabajo tengan que ser invertidos. Esta forma de guerrear puede implicar diferentes tecnologías, especialmente para el C₃I, para la recopilación, procesamiento y distribución de inteligencia, para las comunicaciones tácticas, para logística e “identificación amigo-enemigo” (IFF: identification friend or foe), así como para sistemas de armas “smart” inteligentes, etc...

Puede suceder que implique también intrusión, sobrecarga, engaño, saturación o cegamiento electrónico de los circuitos de comunicación e informaciones del adversario. No obstante la cyberguerra no se limita a ser simplemente un conjunto de medidas basadas en la tecnología. Y no debería ser confundida con significados ya pasados anclados en nociones de guerra electrónica, robotizada, automatizada o computerizada.

La Cyberguerra puede tener importantes consecuencias para la organización y la doctrina militar. Como se ha hecho notar, la literatura sobre la revolución de la información pone en relieve innovaciones “organizacionales”, haciendo que diferentes partes de una institución funcionen más bien como redes interconectadas que como jerarquías separadas. Así la Cyberguerra puede tener que implicar una suerte de “rediseño” institucional tanto en dentro de cada una de las áreas como en las relaciones entre diversas de ellas.

Adaptarse a un funcionamiento de estructuras en red puede requerir algún tipo de descentralización del mando y el control, al que se podrían poner objeciones desde comprensiones más anticuadas que estipulaban que el avance de las nuevas tecnologías proporcionaría un mayor grado de control centralizado de las operaciones militares.

Pero la centralización es sólo una cara de la moneda: efectivamente, las nuevas tecnologías pueden también proveer una mejor “visión de conjunto”, una comprensión central del escenario que refuerza la dirección en una situación compleja.

Muchos tratamientos de rediseño “organizacional” defienden la descentralización, sin embargo la descentralización por sí misma no es el punto clave. Es la conjunción de la descentralización con la visión de conjunto la que aporta las verdaderas ventajas.

La Cyberguerra puede implicar a su vez el desarrollo de nuevas doctrinas sobre el tipo de fuerzas que se necesitan, sobre dónde y cómo desplegarlas, qué y cómo atacar al enemigo.

Cómo y dónde situar qué tipo de ordenadores con sus correspondientes sensores, redes, bases de datos y demás, puede ser tan importante como en su tiempo fue la cuestión relativa al despliegue de bombarderos y de sus funciones de apoyo. La Cyberguerra puede también tener implicaciones para integrar los aspectos políticos y psicológicos de la guerra con los netamente militares. En suma, la Cyberguerra trae a colación vastas cuestiones de organización y doctrina militar, así como de estrategia, táctica y diseño de armas. Puede ser aplicable tanto en conflictos de baja como de alta intensidad, en medios convencionales o no, para propósitos defensivos u ofensivos. Como innovación en el campo de la guerra, anticipamos que la Cyberguerra puede resultar para el siglo XXI lo que la “blitzkrieg” fue para el siglo XX.

No obstante, pensamos que aun hoy el concepto es demasiado especulativo para alcanzar una definición precisa.

Tomado de http://www.rebellion.org/cultura/cyberwar_netwar080201.htm