ANALES DE DOCUMENTACIÓN

Revista de Biblioteconomía y Documentación.
Servicio de Publicaciones. Universidad de Murcia.
D.L. MU-776-1998. ISSN: 1575 - 2437

Vol. 1, 1998, págs 185-192.

Principal

Sumario

Concepto y fuentes para el estudio de la Information Warfare .

Jesús Tramullas Saz
Facultad de Filosofía y Letras
Universidad de Zaragoza

Resumen: En este trabajo se aborda el concepto de Información Warfare, así como las principales definiciones que se han propuesto para el mismo. Se establecen los diferentes tipos de acciones que se inscriben en este ámbito, y se delinean algunas implicaciones para el especialista en información. Como punto de partida para su estudio, se incluyen una selección de fuentes de información sobre el tema objeto de estudio.

Palabras clave: Information Warfare, seguridad, ataques de información, redes informáticas.

Abstract: This paper broaches the concept of Information Warfare, as well as the main definitions proposed for it. The different types of action included in this field are established, and some implications for the information specialist are outlined. A selection of information sources is included as a starting point for the the study of the subject.

Key words: Information Warfare, Security, information attacks, information networks.

1. Introducción.

La utilización de la información y del conocimiento como arma para obtener y detentar el poder, en su más amplia acepción, es un lugar común en el devenir histórico. Baste para ello recordar los tratados de poliorcética escritos durante los siglos IV y III a.C., o las numerosas anotaciones de las campañas de César en las que se hace referencia a la información que éste obtenía de sus exploradores. Los conflictos bélicos que han tenido lugar durante el siglo XX han puesto de relieve la importancia de las actividades de inteligencia, que comprendían tanto las labores de información propias como las de desinformación al bando contrario. Sin embargo, el reciente conflicto conocido como Guerra del Golfo (1990-1991) ha supuesto un punto de inflexión en el concepto y uso de la información como arma militar. Fruto de ello ha aparecido en la bibliografía especializada toda una teoría sobre lo que se ha dado en llamar Information Warfare [1], que introduciremos seguidamente, así como de las técnicas y tecnologías involucradas. Como puede deducirse, ha sido en el ámbito norteamericano, de la mano de sus fuerzas armadas, de donde han surgido estos estudios, especialmente de la National Defense University y de la Naval War College.

Es necesario remontarse a los conocidos ensayos de A. Toffler para encontrar una formulación teórica sobre el poder que supone en la actualidad la información y el conocimiento, y su papel en las guerras del futuro [2]. Curiosamente, las formulaciones estratégicas y tácticas aplicadas han sido adoptadas, en su mayor parte, del conocido tratado de Sun Tzu *El Arte de la Guerra* , compuesto en la antigua China durante el Período de los Reinos Combatientes (siglos V a III a.C.) [3]. Y es que este estratega daba suma importancia al conocimiento de las circunstancias del combate, a la comunicación de órdenes, a la información sobre el estado de enemigo y a los principios de dominación psicológica sobre el contrario.

El tercer elemento a considerar es la creciente utilización de tecnologías y sistemas de información en todas las actividades humanas, tanto civiles como militares. Por lo tanto, son objeto de formulación teórica en el campo militar, como objetivo tanto ofensivo como defensivo. El enfrentamiento clásico depende ahora de la utilización de tecnologías de la información, y éstas se transforman en un arma de múltiples facetas.

2. Concepto de *Information Warfare*.

Como todo intento de definición, en un campo tan cambiante como el que nos ocupa, no es posible alcanzar una que satisfaga a todos los investigadores. Como punto de partida se puede adoptar la propuesta de Widnall y Fogleman, para los cuales *Information Warfare* (IW) es:

"Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions;

> protecting ourselves against those actions; and exploiting our own military information functions." [4]

Por lo tanto, se ocupa de todas las acciones encaminadas a obtener la superioridad en información sobre un adversario, tanto atacando los sistemas físicos de transferencia y proceso de *información (information systems warfare* , ISW), como el contenido simbólico e informativo de los mismos *(information dominance warfare* , IDW).

Martin Libicki [5], uno de los mayores expertos sobre la *Information Warfare* , ha expuesto la dificultad que supone formular una definición de ésta. Libicki ha señalado la existencia de siete tipos principales de Information Warfare, cada uno de ellos con sus propias características, conformando un mosaico variable:

1. Command and Control Warfare, C2W: acciones contra y en defensa de las actividades de organización y mando de las fuerzas combatientes. Se trata de operaciones integradas para la destrucción de la capacidad de acción de las fuerzas, basadas en la destrucción o inhabilitación de su mando y de la cadena correspondiente.
2. Intelligence-based Warfare, IBW: forma de combate basada en la rápida y efectiva adquisición de información inteligente, y en su uso efectivo inmediato.
3. Electronic Warfare, EW: acciones encaminadas al control del espectro electromagnético del enemigo o a su destrucción, mediante la utilización de energía propia.
4. Psychological Warfare, PSYW: uso de propaganda y otras acciones psicológicas para influenciar la moral y la percepción del enemigo, y fortalecer las propias.
5. Hacker Warfare: ataques a sistemas informáticos civiles con la finalidad de copiar, destruir, impedir el acceso o alterar la información contenida en ellos.
6. Economic Information Warfare, EIW: la aplicación de las tácticas y técnicas de la IW al campo de los intereses económicos.
7. Cyberwarfare: combate entre contendientes en un campo de batalla virtual, también se utiliza para designar futuras guerras robóticas. Se encuentra influenciado por la literatura “ciberpunk”.

Para este autor, las diferencias dificultan la redacción de una definición. Por contra, Schwartau reduce el uso de *Information Warfare* exclusivamente (también Libicki acepta la posible futura preponderancia de la *Cyberwarfare*) a los enfrentamientos que pueden librarse en campos de batalla electrónicos, que otros autores han llamado también *netwars*[6]. En este contexto es en el cual Schwartau ha definido la existencia de tres clases de *Information Warfare* :

1. Clase I, *Personal Information Warfare* : área relacionada con las cuestiones y la seguridad personal, así como la privacidad de los datos y del acceso a las redes de información.
2. Clase II, *Corporate/Organizational Level Information Warfare* : área del espionaje clásico entre organizaciones de diferente nivel (de la empresa al Estado).
3. Clase III, *Open/Global Scope Information Warfare* : área relacionado con las cuestiones de “ciberterrorismo”, a todos los niveles.

Diferente aproximación es la adoptada por Whitaker, para el cual las aproximaciones a *la Information Warfare* pueden incluirse en tres grandes categorías [7]:

1. *Third-Wave Warform* : según este enfoque, se trataría de una nueva forma de enfrentamiento, pero dentro del enfoque tradicional de geopolítica y estrategia, cuyo objeto son los sistemas de información.
2. *Samurai Semiotics* : es una expresión de un cambio profundo en la forma de pensar y de actuar, en la que importa más la manipulación de la información simbólica, sobrepasando el contexto de los sistemas de información.
3. *Free-Form Hype-Pretext* : se utiliza como una excusa tecnológica para promover la producción y venta de soluciones comerciales de alto coste, financiado por complejos e intereses militares.

Las tendencias más avanzadas ponen el énfasis en los niveles psicológicos, de creencias y de conocimiento del adversario. Szafranski ha señalado como los ataques tecnológicos a los sistemas de información son la herramienta para destruir el sistema de conocimiento del enemigo:

> “Information warfare is a form of conflict that attacks information systems directly as a means to attack adversary knowledge or beliefs... is hostile activity directed against any part of the knowledge and belief systems of an adversary.” [8]

En esto coincidirían los tipos 1 y 7 de Libicki, en el marco del tipo 4, y en la categoría *de Samurai Semiotics* de Whitaker. Desde esta perspectiva es desde la cual se están aportando los estudios teóricos más novedosos, centrados en el diseño de armas de información, tanto ofensivas como defensivas. Por ejemplo, la C2W utiliza medios tecnológicos para anular la capacidad de organización y mando del contrario, pero su objetivo final es destruir la confianza en el mando, crear confusión, y consecuentemente romper el soporte moral del enemigo.

3. *Cyberwar* y *netwar*.

Según algunas fuentes, fue W. Gibson (aunque no se puede olvidar tampoco a B. Sterling) el responsable del término y del concepto actual de "ciberespacio", a través de sus relatos de ciencia ficción. En este contexto cabe situar *cyberwar* y *netwar* (algunos autores hacen a éste segundo sinónimo del primero). En un trabajo clásico, Arquilla y Ronfeldt sostienen que *cyberwar* es el conflicto relacionado con el conocimiento, a nivel militar, limitado a actividades de información, entre oponentes dotados de alta tecnología. *Netwar* sería el mismo enfrentamiento, pero no de tipo militar [9]. En la situación actual, el espacio de batalla y de dominación para este enfrentamiento serían las redes de interconexión de ordenadores a nivel mundial, como Internet y sus sucesores. En este entorno, la principal táctica es el ataque de información, que busca corromper la información del adversario de forma directa, sin cambios visibles en la entidad real en la que se encuentra y/o almacena. La red de interconexión se configura como un espacio virtual, en el que se disponen las herramientas y los recursos de información, reflejando en ciertas formas el mundo real, y que consecuentemente puede ser objeto de actividad de enfrentamiento, dominación y superioridad.

Con este planteamiento, en la *cyberwar* se busca atacar el nivel psicológico y de conocimiento del adversario. Stein [10] ha argumentado que el objetivo de la *netwar* es el pensamiento y el comportamiento humanos, y que la primera y fundamental expresión es la propaganda de los medios de comunicación de corte "clásico" (baste pensar en el papel de la CNN en la Guerra del Golfo). Las nuevas posibilidades electrónicas permite actuar ya no como propaganda, sino creando por simulación situaciones que parecen reales, y que inducen a error al objetivo de las mismas. El sembrar la duda en el criterio de verdad es el primer objetivo de la aplicación de la táctica. Sin embargo, este mismo principio de duda hace que el factor irracional o de acción inesperada tome especial relevancia, ya que no pueden valorarse las situaciones creadas de forma metódica, al introducir gran parte de caos. En otras palabras, es posible establecer el inicio, pero muy difícil preveer las consecuencias y reacciones. Las posibles respuestas pueden llevar a una escalada similar a las estudiadas durante la Guerra Fría, en la que ningún bando obtenía una posición ganadora.

4. Repercusiones para los especialistas en información.

Los especialistas en información implicados en el desarrollo y mantenimiento de recursos de información en soporte electrónico e interconectados en redes se encuentran especialmente afectados por las cuestiones planteadas. Cualquier organización se puede ver afectada por un ataque de estas características, por lo que la primera actividad a desarrollar es formar a los interesados en los riesgos y las medidas básicas de seguridad. Existen numerosos manuales y publicaciones sobre seguridad informática que pueden ofrecer los conocimientos básicos necesarios.

El objetivo de los ataques es la información, tanto para su copia no autorizada, como para su modificación de forma inadvertida. El cambio de contenidos afectará la compresión y el conocimiento de la realidad de la organización afectada, con las consecuencias materiales y económicas que pueda tener (se puede imaginar, por ejemplo, la modificación de los datos de un balance final que vaya a ser utilizado en una negociación bancaria). Por lo tanto, la utilización de copias de respaldo y de sistemas de replicación y comparación de bases de datos son otros de los métodos de trabajo a implantar de forma paulatina. No debe olvidarse que la *cyberwar/netwar* tiene su campo de batalla en el ataque a la información por parte de otros grupos de interés (desde terroristas a grupos económicos). Desde un enfoque tradicional, podríamos decir que vuelve el papel de custodio de la integridad de la información que preside la ética del profesional, y que se remonta a los *scriptoria* medievales. Desde una perspectiva futurista, podríamos decir que el especialista en información debe añadir, a sus cada vez más variados conocimientos, los de "ciberguerrero" o "infowarrior". En cualquiera caso, este campo de actividad demandará cada vez mayor importancia y necesidad de formación en un futuro cercano.

5. Fuentes para el estudio de la Information Warfare.

ALBERTS, D.S, *Defensive information warfare* . Washington: National Defense University, 1996. ANTHES, G.H, *Net Attacks Up, Defenses Down* . Computerworld , January, 1996, p. 71-72.

ARQUILLA, J. y RONFELDT, D., "Cyberwar is coming!" *Comparative Strategy* , 2, 1993, p. 141-165.

ARQUILLA, J. y RONFELDT, D., *The advent of netwar* . Santa Monica: RAND Corp., 1996. BAUMARD, P., *From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift* . URL: http://www.indigo-

net.com/annexes/289/baumard.htm

CAMPEN, A.D., DEARTH, D.H. y GOODEN, R.T. (eds.), *Cyberwar: security, strategy, and conflict in the information age* . Fairfax: AFCEA International Press, 1996.

DOD Dictionary of Military and Associated Terms . Joint Doctrine Division, J-7, Joint Staff. URL: http://www.dtic.mil/doctrine/jel/doddict/

GARIGUE, R., *Information Warfare - Theory and Concepts* . Ottawa: Office of the Assistant Deputy Minister - Defence Information Services, DND, Goverment of Canada Report, 1995.

GOODMAN, S.E., "War, Information Technologies, and International Asymmetries." *Communications of the ACM* , 39, 12, 1996, p. 11-15.

GREENBERG, L.T., *Information warfare and international law* . Washington: National Defense University, 1997.

HALL, L.P., *National military strategy: information warfare* . Carlisle Barracks: U.S. Army War College, 1997.

HARLEY, J.A, *Information, technology, and the center of gravity* . Newport: Advanced Research Dept., Naval War College, 1996.

HAYES, R.E., *Information warfare and deterrence* . Washington: National Defense University, Institute for National Strategic Studies, 1997.

HILL, C. y HUDSON, J., *Bibliography for information warfare* . Newport: Naval War College, 1995. *Information Warfare* . Washington: Air Force Doctrine Division, 1996. *Information warfare: a strategy for peace, the decisive edge in war* . Washington: Joint Chiefs of Staff, 1996. J

UDY, D.R, *After recognition comes implementation: the challenges for the information age revolution in military affairs* . Carlisle Barracks: U.S. Army War College, 1997.

KABAY, M.E., *Prepare yourself for information warfare* . ComputerWorld, March 1995. URL: http://www.computerworld.com/search/AT-html/9503/950301SL9503lead.asc.html

KILLAM, T.B., *Weapons of mass disruption for the operational info-warrior* . Newport: Joint Military Operations Dept., Naval War College, 1996.

KUEHL, D., *Defining information* . Washington: National Defense University, Institute for National Strategic Studies, 1997.

LEVIDOW, L. y ROBINS. K. (eds.), *The Cyborg Worlds: the military information society* . Free Assn Books, 1990.

LIBICKI, M.C., *What is information warfare?* Washington: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense, 1995.

LIBICKI, M.C., *Defending cyberspace, and other metaphors* . Washington: National Defense University, 1997.

MOLANDER. R.C, RIDDILE, A.S. y WILSON, P.A., *Strategic information warfare: a new face of war* . Santa Monica: RAND Corp., 1996.

NEILSON, R.E. (ed.), *Sun Tzu and information warfare: a collection of winning papers from the Sun Tzu Art of War in Information Warfare Competition* . Washington: National Defense University Press, 1997.

PASTORETT, T.N. (comp.), *Information warfare: selected references* . Maxwell: Air University Library, 1996. POWER, R., "CSI Special Report on Information Warfare". *Computer Security Journal* , 11, 2, 1995.

SCHWARTAU, W. (ed.), *Information Warfare: chaos on the electronic superhighway* . New York: Thunder's Mouth, 1996.

SINGER, A. y ROWELL, S., *Information Warfare: An Old Operational Concept With New Applications* . National Defense University Strategic Forum Number 99, 1996. URL:

http://198.80.36.91/ndu/inss/strforum/forum99.html

SOO HOO, K.J. GREENBERG, L. y ELLIOT, D., *Strategic information warfare: a new arena for arms control?.* Stanford: Center for International Security and Arms Control, Institute for International Studies, Stanford University, 1997.

STEIN, G.J., *Information Warfare* . 1995. URL: http://www.cdsar.af.mil/apj/stein.html

STEIN, G.J., "Information War - Cyberwar -Netwar ." *Battlefield of the Future. 21st Century Warfare Issues.* URL: http://www.cdsar.af.mil/battle/chp6.html

STEWART. M.J ., *Information operations, information warfare: policy perspectives and implications for the force* . Carlisle Barracks: U.S. Army War College, 1997.

SZAFRANSKI, R., *A Theory of Information Warfare. Preparing for 2020* . 1995. URL: http://www.cdsar.af.mil/apj/szfran.html

UNITED STATES AIR FORCE, *Information Warfare, Fact Sheet 95-20* . URL: http://www.dtic.dla.mil/airforcelink/pa/factsheets/Information_Warfare.html

UNITED STATES AIR FORCE, *Rome Laboratory: information systems for the warfighter* . Rome: Rome Laboratory, 1997.

U.S. Information Warfare Jane's Special 1997-1998 . Jane's Information Group, 1998.

HEATLEY, G.F. y HAYES, R.E., *Information warfare and deterrence* . Washington: Institute for National Strategic Studies, 1996. URL: http://www.ndu.edu/ndu/inss/books/iwd/index.html

WIDNALL, S.E., y FOGLEMAN, R.R., *Cornerstones of information warfare* . Washington: Dept. of the Air Force, 1995. URL: http://www.dtic.mil/airforcelink/pubs/corner.html

6. Servicios de información en Internet.

Guide to Information Warfare.
URL: http://www.uta.fi/~ptmakul/infowar/index.html

*I-War Research Group.*URL: http://www.i-war.com/ *Information War and Cyberspace Security. RAND Research Review 1995.*
URL: http://www.rand.org/publications/RRR/RRR.fall95.cyber/

Information Warfare on the Net
URL: http://www.fas.org/irp/wwwinfo.html

Information Warfare Tutorial.
URL: http://carlisle-www.army.mil/usacsl/iw/tutorial/intro.htm

InfoWar.com
URL: http://www.infowar.com/

Institute for the Advanced Study of Information Warfare (IASIW)
URL: http://www.psycom.net/iwar.1.html

Journal of Electronic Defense
URL: http://www.jedefense.com/jed.html/

---

[1] La primera anotación que debe realizarse es que el término *warfare* no refleja un estado de guerra, sino un conjunto de medidas y acciones hostiles que pueden tomarse en un momento dado para asegurar un estado o interés.

[2] TOFFLER, A. y TOFFLER, H., *War and AntiWar: Survival at the Dawn of the 21 st Century* . Boston: Little, Brown and Co., 1993.

[3] Puede utilizarse la traducción española de F. Montes: SUN TZU, *El arte de la guerra* . Madrid: Ed. Fundamentos, 1990.

[4] WIDNALL, S.E. y FOGLEMAN, R.R., *Cornerstones of Information Warfare* , 1995. URL: http://www.af.mil:80/lib/corner.html

[5] LIBICKI, M., *What is Information Warfare?* August 1995. URL: http://www.ndu.edu/ndu/inss/actpubs/act003/a003cont.html

[6] SCHWARTAU, W. (ed.), *Information Warfare: chaos on the electronic superhighway* . New York: New York: Thunder's Mouth, 1996.

[7] WHITAKER, R., "The Three Categories of IW Foci to Date." WHITAKER, R *., Information Warfare: Questioning Power Via Cyberspace* , 1995. URL: http://www.informatik.umu.se/~Erwhit/IW.html

[8] SZAFRANSKI, *A Theory of Information Warfare. Preparing for 2020* . 1995. URL: http://www.cdsar.af.mil/apj/szfran.html

[9] ARQUILLA, J. y RONFELDT, D., "Cyberwar is coming!" *Comparative Strategy* , 2, 1993, p. 141-165.

[10] STEIN, G.J., "Information War - Cyberwar -Netwar ." *Battlefield of the Future. 21st Century Warfare Issues* URL: http://www.cdsar.af.mil/battle/chp6.html