Nos pescan con red: La gran ofensiva del comando ciberespecial del Pentágono está cerca

Autor beu
jueves, 24 de abril de 2008
Modificado el jueves, 24 de abril de 2008

Rosa Miriam Elizalde y Rogelio Polanco, Rebelión/Cubadebate

24-04-2008

"En el pasado, si el Gobierno quería violar la intimidad de los ciudadanos corrientes, tenía que gastar sus recursos en interceptar, abrir al vapor y leer el correo y escuchar, grabar y transcribir las conversaciones telefónicas. Eso era como pescar con caña, de uno en uno. Por el contrario, los mensajes de e-mail son más fáciles de interceptar y se pueden escanear a gran escala, buscando palabras interesantes. Esto es como pescar con red, existiendo una diferencia orwelliana cuantitativa y cualitativa para la salud de la democracia". (Declaración de Phil Zimmermann ante el Subcomité de Política Económica, Comercio y Medio Ambiente de la Cámara de Representantes de los EEUU, el 26 de junio de 1996)

Nuevas evidencias en la prensa norteamericana indican que el Pentágono se está preparando para una ofensiva cibernética a gran escala, con la entrada en funcionamiento en el próximo octubre del Comando del Ciberespacio de la Fuerza Aérea de los Estados Unidos.

El Comandante Robert J. Elder Jr., jefe de esta fuerza especial que ejecutará acciones de guerra en la Internet, dijo al USA Today el pasado 6 de abril que el objetivo fundamental de esta fuerza es desarrollar “estrategias militares que permitan interrumpir el sistema de comunicación enemigo” y que las capacidades ofensivas de ese Comando han mejorado notablemente desde el inicio de la guerra en Iraq, cuando “se emplearon ataques rudimentarios por parte de los Estados Unidos, como saturar los sistemas iraquíes y el uso de ataques por red para evitar la comunicación de las unidades terrestres entre sí”. [1]

Efectivamente, la ciberguerra se inició semanas antes del bombardeo sobre Iraq, después de que el presidente de Estados Unidos, George W. Bush, firmara una directiva secreta en la que aprobaba el ataque a redes “enemigas”, un país que en marzo del 2003 apenas tenía 12 000 computadoras conectadas a la Red y eran muy pocas los que se controlaban desde dependencias militares o manejaban información confidencial.

Este miércoles 23 de abril se anunció la convocatoria al II Simposio Ciberespacial de la Fuerza Aérea, que tendrá lugar del 17 al 19 de junio en Massachussets. Uno de sus objetivos, aventado sin pudor en los medios norteamericanos, “es el control cibernético” y “avanzar en el dominio de este nuevo territorio de guerra, como mismo controlamos el espacio aéreo.” [2]

Y para que no queden dudas de que el Comando Ciberterrorista norteamericano va en serio, la Fuerza Aérea creará 300 nuevos empleos, “como parte del crecimiento previsto en el Comando de Operaciones de la Red, de la Fuerza Aérea, que es la columna vertebral del Comando Ciberespacial -cuya sede principal está provisionalmente en la base de Barksdale, en Luisiana-. Es también la base de nuestra capacidad para luchar contra las nuevas guerras en el ciberespacio". Es decir, contra todos nosotros.

A propósito de esta ofensiva norteamericana y la constitución oficial del Comando Ciberespacial, que se viene articulando desde finales del 2006 como fuerza añadida a los Ejércitos convencionales del Pentágono –el de aire, mar y tierra-, quisiéramos esbozar cuatro aspectos que suelen ser ignorados, subestimados o confundidos por la izquierda, en los debates en torno al uso de la Internet. Asuntos en los que habría que profundizar y que son a nuestro juicio vitales para poder presentar una alternativa a la agresión que ya tenemos encima y que se multiplicará, a más tardar dentro siete meses.

1. Necesidad del conocimiento del entorno tecnológico

Los sociólogos llaman “heterarchies” a la manera en que se unen, como si fueran un mismo cuerpo, las redes sociales y las digitales. Esta articulación dio muestras de sus enormes potencialidades con el Foro Social Mundial, durante las manifestaciones previas a la guerra en Iraq o en la organización de la protesta mundial contra la reunión de la OMC en Seattle.

Sin embargo, estas experiencias, desgraciadamente, parecen haberse esfumado con la misma relampagueante rapidez con que aparecieron. Una causa que nos atreveríamos a esbozar tiene que ver con el desencuentro que existe en las redes sociales y las redes tecnológicas. Suele haber claridad sobre las muy concretas reivindicaciones políticas que nos

mueven, pero no de la manera en que se han de interrelacionar los grupos que intervienen en ellas. Dicho de otra forma, tenemos conciencia de la importancia de la sangre para la vida de un organismo, pero esta parece flotar en el vacío, como si no necesitara del concertado laberinto de venas o como si estas fueran secundarias. No es un defecto particular de las sociedades con menos desarrollo de la Red, sino la expresión del uso tardío y generalmente empírico de la Internet en las organizaciones de izquierda, cuya participación de las llamadas nuevas tecnologías generalmente se ha reducido a un letargo de tendederas digitales y al uso del correo electrónico con volátiles acciones de resistencia.

No se puede hablar de Red en la era de la globalización –que Ignacio Ramonet ha sintetizado en la fórmula “neoliberalismo más Internet” -, si no se tiene en cuenta el medio a través del cual se expresa. Al hablar del medio no nos referimos exclusivamente a la web, al correo electrónico, al teléfono celular y otros sucedáneos, en los que parece concretarse y que están sufriendo tan formidable transformación que quizás más temprano que tarde todas estas formas conocidas nos serán tan extrañas como inútiles.

El término Red de Redes en sí mismo alude, seamos conscientes de ello o no, a la base tecnológica de la forma organizativa que caracteriza a la era de la información: la red. Pero alude también a una manera de estructurar el pensamiento y de organizar las relaciones de comunicación con el soporte de unos medios muy especiales, en los que la innovación intensiva se produce en ámbitos de inteligencia más que en soportes materiales. Es tecnología y método al mismo tiempo. Como ha dicho el general del Cuerpo de Marina Alfred M. Gray, “comunicación sin ‘inteligencia’ es ruido; ‘inteligencia’ sin comunicación es irrelevante.” [3] (Por supuesto, en boca de un militar yanqui ha de esperarse que la palabra inteligencia esté siendo utilizada en doble sentido, pero en su justo significado sintetiza perfectamente lo que queremos decir.)

“Este movimiento actúa, como en anteriores contextos históricos, de manera contradictoria. Internet no es un instrumento de libertad ni tampoco es un arma para ejercer la dominación unilateral. Internet –afirma el teórico Manuel Castells- no es una utopía ni una distopía; es el medio en que nosotros nos expresamos –mediante un código de comunicación específico- que debemos comprender si pretendemos cambiar nuestra realidad”. [4]

En la coevolución paralela de Internet y la sociedad, la dimensión política de nuestras vidas esta siendo profundamente transformada. Quedar al margen de estas redes es la forma más grave de exclusión que se puede sufrir en nuestra cultura, y en este sentido son más proféticas que nunca las palabras de Marshall McLuhan:

… las sociedades siempre han sido moldeadas más por la índole de los medios con que se comunican los hombres que por el contenido mismo de la comunicación. El alfabeto es una tecnología que el niño muy pequeño absorbe de un modo totalmente inconsciente. La tecnología eléctrica promueve y estimula la unificación y el movimiento que lleva a un auténtico envolvimiento. Es imposible comprender los cambios sociales y culturales si no se conoce el funcionamiento de los medios. [5] 2. La organización en Red asociada a un pensamiento estratégico.

Asomémonos brevemente a la esfera que más rápidamente está siendo transformada por las redes de información. En Estados Unidos la innovación tecnológica ha estado asociada en un lugar especialísimo con la guerra: el esfuerzo científico de la ingeniería generado en torno a la Segunda Guerra Mundial fue el ámbito tecnológico que permitió la revolución de la microelectrónica, mientras que la carrera armamentista durante la Guerra Fría favoreció su desarrollo. De modo que el nacimiento de la Internet no es un hecho aislado, ni un experimento fortuito en un laboratorio, sino el resultado de la política tecnológica más innovadora del mundo.

ARPANET, fuente principal de lo que acabaría siendo Internet, fue ideada, deliberadamente diseñada y posteriormente gestionada por un grupo de militares y académicos que sin el apoyo del Departamento de Defensa jamás habrían sido capaces de sumar los recursos necesarios para construir una red de computación. Fue fundamental la participación de brillantes informáticos de algunas de las más prestigiosas universidades norteamericanas, a quienes no les importó en lo absoluto trabajar bajo el financiamiento del Pentágono en medio de la guerra en Viet Nam.

Como explicara recientemente el Comandante en Jefe Fidel Castro en una de sus Reflexiones, la feroz carrera armamentista y la conciencia de la inferioridad tecnológica de ese país, fueron dos de los principales desencadenantes de la desintegración de la Unión Soviética. De entonces acá tres han sido los desafíos fácilmente identificables de la hegemonía militar norteamericana, que han estado acompañados por el esfuerzo para desarrollar y controlar la Red:
- El primero es el tipo de competencia entre iguales que representaba la Unión Soviética. El principal candidato a esta designación ahora es China.
- El segundo desafío es el que representan los llamados estados-canalla (oscuros rincones del mundo), designación que se aplica a cualquier tipo de estado en vías de desarrollo que represente un obstáculo a la hegemonía norteamericana.
- Y el tercero, por supuesto, es el que ocupó el primer plano con los ataques del 11 de Septiembre: el enemigo no-estatal, que criminaliza a todos los que se oponen al poder hegemónico norteamericano.

A partir de estos escenarios se ha estructurado una poderosísima “Red de redes contra la humanidad”, en el que la guerra altamente tecnificada tiene el papel protagónico. La transformación del consorcio militar industrial norteamericano, que parece ir derivando hacia un consorcio militar-cultural gracias a las tecnologías de la información, descansa en dos líneas estratégicas: la tecnológica y la puramente doctrinaria.

En el ámbito tecnológico, se están desarrollando a niveles jamás vistos las comunicaciones electrónicas, los sistemas de vigilancia, los aviones no tripulados, los proyectiles dirigidos por satélites y un arsenal de aplicaciones de híbridos de la nanotecnología, la microelectrónica y la Inteligencia Artificial, que permiten reducir la presencia física de los soldados en los escenarios bélicos. Las invenciones del tipo The Matrix, con su célebre cita filosófica “bienvenido al desierto de lo real”, están cada vez más próximas a la realidad. The New York Times, por ejemplo, ha publicado en el 2005:

El Pentágono predice que los robots serán una importante fuerza de combate en el ejército americano en menos de una década, y que perseguirán y eliminaran a nuestros enemigos en el campo de batalla. Los robots son una parte crucial del esfuerzo en el que está empeñado el Ejército para reformarse y convertirse en una verdadera fuerza de combate para el siglo XXI, y el contrato firmado para desarrollar un proyecto valorado en 127 mil millones de dólares y conocido como Sistemas de Combate del Futuro, es el contrato militar más importante de la historia americana. Los militares planean invertir decenas de miles de millones de dólares en unas fuerzas armadas completamente automatizadas. Los costos de esta transformación contribuirán a elevar el presupuesto del Departamento de Defensa casi un 20 por ciento más. [6]

El segundo ámbito de la doctrina militar norteamericana en Red es tan importante como el anterior. Un nuevo estilo de pensamiento está imponiéndose en los think-tanks militares de Estados Unidos y la OTAN. Se le conoce con el término de swarming [7] o enjambre y representa un cambio radical frente a las concepciones militares basadas en despliegues masivos de capacidad artillera, armamento blindado y grandes concentraciones de tropas. El enjambre es una estrategia militar en la cual una tropa ataca a un enemigo desde múltiples direcciones diferentes para después reagruparse.

Este tipo de guerra “no-lineal” elimina la noción del frente y representa una versión de alta tecnología de la guerra de guerrillas. La guerra “basada en redes”, según la terminología del Pentágono, depende totalmente de un sistema de comunicaciones sólido y seguro, capaz de mantener una conexión constante entre todos los nodos de la red.

Estación del Comando del Ciberespacio, de la Fuerza Aérea norteamericana, en Luisiana. Esta fuerza, un nuevo Ejército que se incorpora a los ámbitos tradicionales de la guerra –la tierra, el aire y el mar-, “se apoyará en estrategias militares que permitan interrumpir el sistema de comunicación enemigo, con mayor precisión que en Iraq en el 2003, donde logramos intervenir todas las comunicaciones terrestres del Ejército de Saddam Hussein”, aseguró el General Robert Elder, jefe del Comando Ciberespacial.

Las implicaciones que esto está teniendo para las fuerzas armadas son enormes. Se ha ido desmontando paulatinamente la organización tradicional del ejército en cuerpos, divisiones, regimientos y batallones de gran envergadura. En esta lógica surge el Comando Ciberespacial para el despliegue a través de las redes, que debe ser el responsable del incremento desmesurado de las agresiones contra sitios chinos y venezolanos en los últimos meses [8] . Lo mismo ha ocurrido con la división funcional entre diversas especialidades: infantería, unidades blindadas, comunicación, artillería, ingeniería. Las unidades han pasado a ser básicamente multifuncionales y dependen de su capacidad de conexión en red para conseguir apoyo mutuo.

Como señala la RAND Corporation [9] , “este proyecto doctrinal no puede ponerse en práctica sin un sistema de comunicación y vigilancia plenamente integrado. Esta nueva perspectiva requiere que las fuerzas armadas se transformen en una ‘organización sensorial’, en la que el sistema resultará fundamental para lograr mantener a las unidades operativas conectadas a la red. El sistema de mando, control, comunicaciones, ordenadores, inteligencia, vigilancia y reconocimiento (C4ISR) puede llegar a generar tanta información que será imprescindible... para mantener el topsight -una visión general de todo lo que esté ocurriendo-.”

Por supuesto, sabemos que toda esta doctrina tiene una falla de origen: la subestimación del ser humano. Al final, toda guerra se decide en enfrentamientos cuerpo a cuerpo. No se puede ocupar el territorio, ni desarmar al enemigo, es decir, aniquilar su voluntad de lucha, sin vencerlo en el campo de batalla. Como dice Howard Zinn, “cuando Estados Unidos luchó en Vietnam, fue una confrontación entre tecnología moderna organizada y seres humanos organizados. Y vencieron los seres humanos.” [10] Pero que tengamos esta convicción no significa que no haya que estar muy atentos a los planes del enemigo. 3. Movimientos sociales: pasar a la articulación horizontal

El Foro Social Mundial y las manifestaciones previas a la guerra de Iraq en el 2003, que incorporaron a millones de personas en todo el mundo, son ejemplos esperanzadores de las posibilidades de la conjunción de las redes técnicas con las redes sociales, desde el punto de vista que aquí analizamos. Pero habría que admitir que desde entonces no hemos vuelto a ver expresiones semejantes de resistencia política articulada.

Hasta el 2003, la falta de canales comunicativos estructurados resultó ser una fuerza y no una debilidad para las

acciones de las redes contrahegemónicas, porque todos los movimientos podían ser inmediatamente eficaces y no esperaban ninguna clase de ayuda externa o extensión para garantizar su efectividad. Uno de los modelos más exitosos fue el de las movilizaciones contra la reunión de la OMC en Seattle, a finales de 1999.

Gracias a que todavía no estaban organizados los sistemas de vigilancia a través de la Red, desde múltiples puntos de Internet se articuló la movilización, incluida una complicada logística –por ejemplo, la mayoría de los miles de participantes que llegaron a la ciudad no se alojó en hoteles para no llamar la atención de las autoridades, sino en la casa de otros activistas. Cuando el gobierno estadounidense se dio cuenta, la acción era ya un hecho. La célula matriz de las protestas, los grupos de afinidad, eran unidades de 15 a 20 personas que funcionaban discrecionalmente y que tenían capacidad de tomar sus propias decisiones estratégicas. Algunos hicieron teatro callejero, otros se encadenaron, otros llevaban marionetas gigantes, algunos simplemente se agarraron de los brazos para impedir de manera no violenta el paso de los delegados. En cada grupo había gente dispuesta a ir a la cárcel, otros que serían el apoyo una vez que estuvieran en prisión y una persona calificada en primeros auxilios. La "descentralización coordinada", con el apoyo inestimable de Internet, hizo posible que se cumplieran los objetivos de la mayoría de los activistas, movilizados por todo el mundo.

Ya esto no se puede hacer sin desatar las alarmas. Se acabó el mito de que Internet era un espacio inmune a la regulación y como afirma Mike Davis, experto en ecología urbana y autor del libro Planet of Slums (Planeta de suburbios), “las mejores cabezas del Pentágono han aprendido la lección… Ahora tienen por blanco las ciudades salvajes, fracasadas del Tercer Mundo –especialmente sus suburbios marginados–, que serán el campo de batalla característico del siglo XXI. La doctrina bélica del Pentágono está siendo reformulada para apoyar una guerra mundial de baja intensidad de duración ilimitada contra segmentos criminalizados de los pobres urbanos.” [11]

Desde mucho antes del 11 de Septiembre, la maniobra estadounidense sigue la pauta de adelantarse a cualquier otro gobierno o emporio global para ordenar la Red y proveerla de la arquitectura tecnológica, legal y represiva que mejor convenga a Estados Unidos. Cuenta con una circunstancia altamente beneficiosa para sus objetivos: la influencia de las políticas neoliberales, que fragmentan y atomizan las sociedades, e impiden que los grupos que enfrentan estas políticas reconozcan al enemigo principal. Al proyecto neoliberal le interesa que los grupos permanezcan aislados, enfrentados entre sí, sin capacidad de encontrar objetivos y estrategias comunes. Esta primera dificultad ha puesto en jaque la creación de redes de solidaridad y de comunicación antagónicas a la globalización neoliberal, porque choca con sus principios y con sus lógicas de funcionamiento.

La prueba es que un movimiento de extraordinaria importancia para la soberanía en la Red como el de la lucha por mantener la neutralidad en Internet [12] , involucra casi exclusivamente a grupos por los derechos civiles en Estados Unidos. La ausencia de redes internacionales de solidaridad en torno a este tema y el desconocimiento de la ofensiva militar estadounidense en Internet, indican que las transnacionales de telecomunicaciones estadounidenses podrían alzarse con la victoria e imponer a todos más y más barreras para la libertad en Red. Sin ir demasiado lejos, en el discurso del 28 de enero último sobre el Estado de la Nación, el presidente Bush prácticamente amenazó a los legisladores para que aprobaran de inmediato un nuevo proyecto de ley de vigilancia que le otorgaría inmunidad a las empresas de telecomunicaciones que colaboraron con el espionaje sin órdenes judiciales. Literalmente dijo: “Eso significa que si no toman medidas para el viernes, nuestra capacidad de permanecer al tanto de las amenazas terroristas se debilitaría y nuestros ciudadanos estarían en mayor peligro. El Congreso debe asegurarse de que no se interrumpa el flujo de inteligencia vital. El Congreso debe aprobar protecciones de responsabilidad legal a favor de las empresas que se considera que contribuyeron a los esfuerzos por defender a Estados Unidos. Tuvimos suficiente tiempo para debatir. Es hora de actuar.” [13] Poco después la Ley se aprobó sin más dilación.

El otro gran desafío de nuestros movimientos es trascender los modelos organizativos que dificultan la participación de sus miembros y la creación de redes con otros grupos. Seguimos aferrados a un modelo que se caracteriza por sistemas de difusión, al estilo de la televisión y de la radio, con un punto de emisión y muchos receptores que generalmente no son tenidos en cuenta. Estamos muy retrasados en el uso del modelo que propicia Internet, horizontal y desterritorializado.
4. El futuro: fuera de la red, no existe

El futuro, al margen de la Red, no existe. Jeremy Rifkin, autor de un libro paradigmático, La era del acceso [14] , asegura que la brecha entre conectados y desconectados será aún mayor que la existente hoy entre ricos y pobres, hasta el punto de que quien no esté enlazado en red no existirá ni política, ni social, ni económicamente. Él, como otros investigadores de este tema, coinciden abrumadoramente en que, a medida que Internet se va convirtiendo en la infraestructura dominante en nuestras vidas, la propiedad y el control del acceso a estas tecnologías se convierten también en el principal caballo de batalla político de la sociedad contemporánea.

Debemos tener muy claro que la resistencia y la denuncia no serán suficientes. Las leyes, los tribunales, la opinión publica, los medios de comunicación, los organismos políticos y gobiernos progresistas son instancias fundamentales que deben contribuir a decidir otro futuro para la Red de Redes que no sea el diseñado por Washington. Es imposible controlar la Internet global, pero sí es posible controlar a la gente que la utiliza y, de hecho, estará cada vez más controlada, a no ser que se imponga un modelo que opte por la defensa de patrones solidarios y de transparencia de las

instituciones, actuando desde las barricadas de los que exigen la libertad en el uso de Internet, pero yendo más allá de ellas en la confrontación con los mecanismos del poder político.

El otro gran reto que se nos avecina es vencer el miedo más antiguo de la humanidad: el miedo a los monstruos tecnológicos que podamos engendrar. Tal es el caso, especialmente, de la ingeniería genética, aunque dada la convergencia entre la microelectrónica y la biología, y el desarrollo potencial de sensores ubicuos y la nanotecnología, este temor biológico primario se extiende a todo el ámbito de los descubrimientos tecnológicos.

Las futuras sinergias entre las tecnologías informáticas, la nanotecnología, la biotecnología y las ciencias del conocimiento podrían mejorar drásticamente la condición humana por el crecimiento de la disponibilidad de alimentos, energía y agua, y por el mayor intercambio de información e interconexión entre las personas en todas partes. Sin embargo, las abismales diferencias entre los números que acompañan el presupuesto de guerra y el de los servicios elementales para garantizar la vida de la mayoría de los habitantes del planeta, indican que esos propósitos están lejos de hacerse realidad.

Como ha dicho Fidel, no puede llamarse ni medianamente humana una sociedad donde “se perpetúa el poder económico y el disfrute de las nuevas tecnologías en unas pocas manos. Resolver este dilema es tan trascendente para el destino de la humanidad como enfrentar la crisis del cambio climático en el planeta, problemas que están absolutamente interrelacionados.” [15]

No se vislumbra aún cuánto de la sabiduría, la buena voluntad y la inteligencia social serán empleados para el mejoramiento humano. A juzgar por el modelo imperial en franca ventaja, parece que estos esfuerzos viajan en sentido opuesto. Los gastos militares anuales en el mundo han alcanzado una cifra récord 1,2 millones de millones de dólares, mientras que el ingreso del crimen organizado sumó casi el doble. La sociedad de la vigilancia altamente tecnificada se lanza a la conquista de aún más sofisticadas computadoras, cada una con una inteligencia que eventualmente nos sobrepasará.

Kevin Warwick, profesor de Cibernética de la Universidad de Reading, en Inglaterra, cree que lo que realmente ocurrirá hacia el año 2030 es que “nos habremos convertido en víctimas de las máquinas. Su vigilancia nos controlará totalmente. Quizás habremos evitado un holocausto nuclear, porque no apareció alguien lo suficientemente loco para apretar el botón, pero para el año 2030 nos habremos puesto a nosotros mismos en el infierno. Las máquinas de inteligencia artificial nos observarán. Hacia el año 2030 aún estaremos tratando de razonar y negociar con las máquinas. ¿Por qué ellas deben atendernos cuando son mucho más inteligentes de lo que nosotros somos? Lo que deberíamos esperar es que nosotros, los humanos, seamos tratados por las máquinas de la misma manera que nosotros tratamos a los animales, como trabajadores esclavos y productores de energía”. [16]

Un visionario de las nuevas tecnologías y el desarrollo de las máquinas inteligentes como Ray Kurzweil presupone que “cuando tengamos software ejecutándose en nuestros cerebros y nuestros cuerpos, que controlen el sistema inmunológico de los nanobots, el impacto en el mundo será infinitamente mayor” [17] . Y adelanta que “los intentos por controlar estas tecnologías por la vía de programas gubernamentales secretos, conjuntamente con su desarrollo clandestino inevitable, fortalecería la naturaleza inestable en que sus aplicaciones peligrosas podrían convertirse en dominantes”. [18]

La realidad es que la evolución futura de la Red de Redes está sometida a las dinámicas contradictorias que oponen la dominación imperial a nuestros proyectos de justicia social y a nuestras esperanzas. El universo virtual es el espejo del universo tangible. Debemos situar nuestra acción en el contexto específico de dominación y liberación donde vivimos: en la sociedad red, construida en torno a las redes, y no al margen de ellas o creyendo ingenuamente que es el paraíso o el infierno, de acuerdo al prisma con que se mire.

Manuel Castells reproducía un diálogo, en el que lo desafían del siguiente modo: “‘¿Por qué no me deja usted en paz? ¡Yo no quiero saber nada de su Internet, de su civilización tecnológica, de su sociedad red! ¡Lo único que quiero es vivir mi vida!’ Muy bien –respondió Castells-, pues si ese fuera su caso tengo malas noticias: si usted no se relaciona con las redes, las redes sí se relacionan con usted. Mientras quiera seguir viviendo en sociedad, en este tiempo y en este lugar, tendremos que tratar con la sociedad red.”

La gran ofensiva del Comando Ciberespacial está cerca y no podremos construir una alternativa de futuro al margen de la red o desconociendo su lógica conceptual. Navegantes solidarios o peces en brasero ajeno: ese es el dilema.

[1] Anick Jesdanun: "US Cyberwarfare Prep Includes Offense". Agencia AP, 6 de abril de 2008. Se puede descargar en: http://ap.google.com/article/ALeqM5h93IdWAX5NRBlmIyQJ76eSzufiTgD8VSGL700

[2] AF, DOD leaders on tap for June Cyber Symposium. Air Force Link, 23 de abril de 2008. http://www.af.mil/news/story.asp?id=123095656

[3] Citado en: Viegas Nunes, Paulo Fernando, “El impacto de las nuevas tecnologías en el medio militar. La

Guerra de Información (IW)”. Air & Space Power Journal - Español Segundo Trimestre 2001.

[4] Todas las referencias en este trabajo a Manuel Castells han sido tomadas de: Castells, Manuel. La Galaxia Internet: Reflexiones sobre Internet, empresa y sociedad. Random House Mondadori, Barcelona, 2001.

[5] McLuhan, Marshall: The Global Village: Transformations in World Life and Media in the 21st Century, Oxford University Press, USA, 1992.

[6] The New York Times, 16 de febrero de 2005.

[7] Literalmente, enjambre. El término procede del sustantivo swarm (enjambre), por tanto swarming sería un tipo de combate o ataque concentrado y ágil como de un enjambre de abejas.

[8] De acuerdo con los registros de la empresa norteamericana Akamai Technologies, líder en análisis del comportamiento del tráfico en Internet, estos dos países fueron los más atacados por “piratas” informáticos en el 2007. Para que se tenga una idea de lo que estamos diciendo: en julio de 2007 se implantó un récord. Venezuela, que posee 4 millones de usuarios de Internet, tuvo 764 ataques en 64 horas, 500 más que China, el país que seguía en la lista y que posee 100 millones de usuarios. En: http://www.akamai.com/html/technology/dataviz1.html

[9] Arquilla, John, y Ronfeldt, David, “Swarming and the future of conflict”, RAND National Defense Research Institute, Santa Mónica, CA, 2000.

[10] Zinn, Howard: La otra historia de los Estados Unidos. Editorial de Ciencias Sociales, La Habana, 2004. p.343.

[11] Davis, Mike: Planet of Slums. Verso, Londres, marzo de 2006.

[12] La neutralidad de la Red era un principio que establecía que todos los sitios deben ser tratados de igual manera por los proveedores de servicio de Internet. Se encontraba recogida en la Ley de Comunicaciones estadounidense (Communications Opportunity, Promotion and Enhancement Act). Los movimientos sociales norteamericanos han ido perdiendo, una tras otras, las batallas legales y políticas por la defensa de este principio que convertiría a la Red en una autopista de doble estándar: una para los ricos que puedan pagar servicios exclusivos de banda ancha, y otra para los pobres, con prestaciones lentas y precarias.

[13] Bush, George W., "Discurso del Presidente Sobre el Estado de la Nación 28-01-2008"

[14] ¿?

[15] ¿?

[16] ¿?

[17] ¿?

[18] ¿?