www.juventudrebelde.cu

No apto para aficionados

Publicado: Martes 22 mayo 2007 | 12:00:00 am.

Publicado por: Rosa Miriam Elizalde

El 2 de noviembre de 2006 los medios estadounidenses dieron cuenta, con suma discreción, de unas frases protocolares para bendecir, oficialmente, el nacimiento del Comando del Ciberespacio de la Fuerza Aérea Norteamericana.

En la sede del Pentágono en Virginia, el general de tres estrellas Robert J. Elder, experto en tecnología avanzada de la ex Unión Soviética y con más horas de vuelo en el espionaje electrónico que en el aire, fue presentado como el comandante en jefe de esta nueva fuerza que marca un hito en la historia militar.

Por primera vez, se incorpora a las armas ya tradicionales —el aire, el mar y la tierra— un cuarto cuerpo estratégico, que reacomoda las tácticas de guerra en este mundo cada vez más global. Su misión, repetida una y otra vez en ese discurso de iniciación mediática, es: «Alcance mundial, vigilancia mundial, poderío mundial».

En aquella ceremonia ritual, los generales del Pentágono sencillamente levantaron el velo de la aterradora barricada tecnológica que han estado construyendo desde hace diez años para tomar por asalto la Internet, encrucijada en la que se va a dirimir —y ya está ocurriendo— toda la vida económica, social, política y militar del planeta.

«Hasta hoy —dijo el general Elder— hemos estado a la defensiva. El cambio cultural es que pasamos a la ofensiva y vamos a tratar al ciberespacio como un ámbito de combate». También, amenazó: «Vamos a desarrollar, junto con las universidades, guerreros ciberespaciales que sean capaces de reaccionar ante cualquier amenaza las 24 horas del día, durante los siete días de la semana...». Para que no quedara ninguna duda de la gravedad de la orden del Pentágono, el teniente general Elder añadió: «en este ámbito, al igual que en cualquier escenario de guerra, no hay lugar para aficionados».

Quiero llamar la atención sobre esa frase: «no hay lugar para aficionados», que es igual a decir «no hay lugar para nosotros», la mayoría de los usuarios de la Red que apenas tenemos idea de qué procesos tecnológicos

tienen lugar cuando mandamos un correo electrónico o navegamos en la web, y que no somos conscientes de que la Internet está y estará «invisible» pero omnipresente —como la electricidad— en todos los procesos esenciales de nuestras vidas.

Detrás de la reorganización del Ejército norteamericano está la decisión política de mantener no solo el control de este espacio, la supremacía técnica y la vigilancia extrema de todos los que interactúen en él —potenciales terroristas mientras no demuestren lo contrario—, sino la arquitectura global de lo que ellos han decidido que será la sociedad del futuro.

La creación del Ejército para el Ciberespacio no es el comienzo, sino el punto final, la pata de la mesa que faltaba, en esa arquitectura. El Pentágono tiene la función de ser el policía encargado de identificar y asesinar, literal o digitalmente dentro y fuera de los Estados Unidos, las manifestaciones de resistencia o de alternativa política, tecnológica, económica y militar al orden que ellos han diseñado para nosotros. Los Estados Unidos son la primera ciberpotencia. Controlan las innovaciones tecnológicas, las industrias digitales, los proyectos (materiales e inmateriales) de todo tipo. Sus legislaciones al respecto están siendo clonadas de un país a otro. Toda la plataforma para los grandes cambios históricos, asociados a las llamadas tecnologías del acceso y la revolución de la nueva economía, la han ido imponiendo al mundo sin pedirle permiso a nadie, y frente a ese modelo instituido arbitraria y deslealmente solo ha habido tímidas y descoordinadas reacciones de los movimientos sociales.

Desde hace algo más de diez años, mucho antes del 11 de Septiembre que ha servido en bandeja de plata el pretexto para esta ofensiva, los Estados Unidos han venido trabajando para crear dos canales que propicien el ordenamiento de la Red según sus intereses estratégicos.

Uno, el legal, que intenta aprobar normativas nacionales e internacionales que les permitan espiar, intervenir servidores y páginas web y sancionar a los «terroristas» cibernéticos.

Y un segundo canal, en el que ilegalmente operan con avanzadas armas de guerra —las llamadas eufemísticamente de «minería de datos» y de «reconocimiento»—, para someternos a extrema vigilancia y para desactivar sitios web en una operación ofensiva que han denominado «política de eliminación de información virtual que pueda ser útil al enemigo».

En un artículo publicado el 28 de marzo pasado por el USA Today con el alarmante título de Comando prepara ataques a sitios web terroristas, se afirma que «los documentos contractuales del Pentágono muestran que el Ejército solicitó a las compañías (comerciales) desarrollar un espectro completo de técnicas para atacar redes informáticas. Según muestran los documentos, este programa, dirigido por el Laboratorio de Investigación de la Fuerza Aérea, prevé gastar 40 millones de dólares en cuatro años».

Tanto el Pentágono como las agencias de seguridad norteamericana parten del presupuesto de que todos somos sospechosos de ejercer el terrorismo, incluso si demostramos lo contrario. Y digo esto con premeditación. El Washington Post publicó el pasado 25 de marzo que la famosa Base de Datos de Identidad de los Terroristas (TIDE por sus siglas en inglés), creada a partir del 11 de Septiembre con la integración de todas las agencias de Inteligencia del país, incorpora diariamente un promedio de 1 200 nombres de ciudadanos nacionales y extranjeros. Ahí van a parar todos los registros inimaginables, desde itinerarios de vuelos hasta cuentas de restaurantes, resultados académicos e identificaciones personales en los chats de Internet. El TIDE tiene un solo defecto: después que ingresa el nombre allí es prácticamente imposible borrarlo del sistema, por la compleja maraña de permisos que se necesitan para eliminar un expediente ya iniciado. «La Oficina de Rendición de Cuentas del Gobierno (GAO, por sus siglas en inglés)—dice la autora del artículo del Washington Post, Karen

de Young— reportó que en el 2005, por ejemplo, solo fueron borrados 31 nombres».

Gracias a este segundo canal ilícito operan las variantes mejoradas del sistema Carnivore para el espionaje telemático —la versión europea se conoce como OSEMINTI y la han producido Francia, Italia y España a un costo de 2 000 millones de dólares.

Y también, navegan las nuevas terminologías y etiquetas que criminalizan los movimientos sociales y facilitan el terreno a la intervención legal e ilegal. La caricatura del nuevo terrorista tiene ahora un AKM en la mano derecha y una laptop, en la izquierda, y se dedica con especial ahínco a la «Guerra Santa Tecnológica» tal como la definió el Observador del Terrorismo de la Fundación Jamestown. En esa guerra, afirman los expertos del Pentágono, se enfrentan los «guerreros ciberespaciales» del general Elder contra «piratas», «cibervigilantes», «terroristas», «estados hostiles» e «individuos moderados radicalizados».

No faltan, incluso, los expertos que vaticinan terroríficos escenarios controlados por los «enemigos cibernéticos». En una especie de Harry Potter para adultos, el Ministerio de la Defensa de Gran Bretaña publicó un informe de su Centro de Desarrollo, Conceptos y Doctrinas en el que augura que los ciberterroristas serán capaces de crear chips que podrían implantarse en el cerebro humano, bombas de impulso electromagnéticas y otros diabólicos artefactos.

«En el 2035 —afirma el almirante Chris Parry, jefe del Centro— estarán disponibles armas de pulso electromagnético, capaces de destruir los sistemas de comunicación de una zona o de inutilizar centros neurológicos de comunicación o negocios». Se utilizarán armas de neutrones que matan sin destruir infraestructuras, que podrían ser usadas en limpiezas étnicas. Armas que permitirán ver a través de las paredes, y otras biológicas, radiológicas y nucleares altamente letales.

Lo que no suelen admitir estos expertos es que los únicos que tienen la capacidad para crear ese tipo de artilugio de guerra y dirigir ataques en gran escala en la red, son los dueños de las tecnologías y los que controlan las investigaciones en las universidades y en los laboratorios militares. Como reconoció Ahmed Mücahid Ören, el coordinador del debate sobre ciberseguridad de la Conferencia Mundial sobre Seguridad, convocada por la Unión Europea a fines de febrero de este año: «Un gran ataque electrónico requiere mucho tiempo, mucha información y muchísimo dinero».

Fragmento de la intervención en las Jornadas Internacionales de Telesur sobre el Derecho ciudadano a informar y estar informado, que concluyó el pasado domingo.

http://www.juventudrebelde.cu/opinion/2007-05-22/no-apto-para-aficionados