Comando del ciberespacio de la fuerza aérea de Estados Unidos

ROSA MIRIAM ELIZALDE :: 15/06/2007

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 del régimen norteamericano.

Intervención en las Jornadas Internacionales "El derecho ciudadano a informar y estar informados". Caracas 18 al 20 de mayo de 2007

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."

TODOS SOMOS TERRORISTAS

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 sólo 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.

En este ámbito, el obsesivo interés del gobierno de los Estados Unidos, agenciero de las grandes multinacionales de las telecomunicaciones, va mucho más allá del control de nuestras mentes, aunque, por supuesto, es un objetivo de primer orden convertir en una "tubería" privada que fluya en un solo sentido el espacio de comunicación más participativo que jamás haya tenido la humanidad.

Pero no es esta la única preocupación que tienen. Ignacio Ramonet ha dicho con razón que el dueño de la flota digital será quien controle el comercio y el dinero del mundo, como sucedía durante los siglos XVII al XVIII con la Flota de Indias. Y quien controle estas tecnologías, también conservará la supremacía militar. Pero el superpoderoso sistema de guerra norteamericano, que se sostiene en las técnicas de la comunicación y de la información, puede ser sensible a las acciones de guerra asimétrica, una lección que aprendieron en Vietnam y que les está dando infinitos dolores de cabeza en Iraq. Los misiles, los aviones, los helicópteros, las bombas "inteligentes" se desplazan simultáneamente por pistas digitales y aéreas, y el espacio cibernético puede ser tan o más vulnerable a las emboscadas que los caminos tangibles. "No hay lugar para aficionados", esa frase soberbia del General Elder, tiene un significado añadido: la decisión de los Estados Unidos de convertir en asunto de seguridad nacional el desarrollo y uso de las tecnologías digitales más avanzadas.

¿Cuál es la táctica inmediata que ha seguido el complejo militar-industrial norteamericano para impedir que la Internet sea un tesoro público y se convierta en una autopista privada, anclada a sus intereses hegemónicos? Los propios militares nos lo dicen. En un artículo publicado por la revista Military Review en el número de septiembre-octubre de 2003, dos oficiales que estudiaron a fondo la guerra cibernética palestino-israelí, develan un fragmento de un documento elaborado por el Pentágono sobre Seguridad Nacional e Internet[3]. Allí se definen las "cuatro necesidades en la política nacional e internacional de los Estados Unidos", en torno a este tema:

- Decidir quién proporcionará la seguridad en la Red -es decir, quién es el dueño.

-Proporcionar respuestas legales al rápido crecimiento horizontal de la Red -es decir, una

Ley Patriota universal.

- Poner en vigencia responsabilidades legales para quienes creen incidentes no deseados -es decir, la represión.

-Detener la proliferación de armas y tecnologías cibernéticas no deseadas - es decir, códigos cerrados a la mirada ajena y autopistas exclusivas para la poderosa elite norteamericana.

La argumentación que ofrece el Pentágono a estas "cuatro necesidades" es un manual de ciberterrorismo mundial ilustrado, en el que no podemos detenernos en este análisis por falta de tiempo. Quiero llamar atención al menos en un aspecto: 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. (Si están al tanto de las noticias habrán visto los acuerdos entre Estados Unidos y la Unión Europea para la retención de datos y el impulso a legislaciones sobre un tipo de sociedad de la información.)

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 4 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[6], 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 1200 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 Ã–ren, el coordinador del debate sobre ciberseguiridad 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."

OBSERVATORIO REGIONAL DE LA INTERNET

Desgraciadamente, estamos totalmente indefensos y enajenados de la guerra que ya nos hacen. Existe abundante información útil, pero está fragmentada y dispersa, mientras la izquierda sigue gravitando en dos corrientes igualmente engañosas y en cierto modo suicidas.

La primera corriente cree que la Internet es una panacea en la que se disiparán sus históricos problemas de expresión y articulación internacional. La segunda tendencia, absolutamente paranoica, suele mirar a la Red a distancia y con terror, y está convencida de que es un ámbito poblado de abismos y monstruos de siete cabezas como en el Gran Océano de las crónicas precolombinas.

Ambas corrientes nos dejan a merced de las decisiones y los zafarranchos de combate del Pentágono y sus filiales en Europa, y hay que reconocer que han logrado avanzar en sus estrategias de dominación en la web. No es casual que desde el 2003 no ha habido otras reacciones de la magnitud que vimos en los días previos al inicio de la intervención militar

en Iraq, protesta que se hizo sentir de manera simultánea y organizada en cientos de ciudades del mundo con la ayuda indiscutible de la Internet.

Como mismo no podemos existir sin la tierra, sin el aire y sin el mar por más que otros nos hagan la guerra para arrebatarnos esos ámbitos de vida, es un asunto de elemental sobrevivencia defender el espacio cibernético sin el que no hay manera de construir el futuro de nuestra especie.

La ciberguerra terrorista que han declarado los Estados Unidos da por sentado dos miedos: uno al terrorismo en sí mismo y otro, a las tecnologías. Por tanto hay que apropiarse de estas técnicas; hay que diseñar nuestras propias estrategias; tenemos que monitorear también 24 horas al día si es posible la Red y sugerir alternativas frente a las agresiones del Comando Ciberespacial; urge identificar todos los resquicios legales que nos permitan hacerle frente a sus arremetidas, y sobre todo, debemos ayudar a construir, de un modo menos empírico, nuestras comunidades virtuales.

Asociado al Observatorio Global de los Medios, a la Red de Redes En Defensa de la Humanidad u otra institución que pueda apoyarlo, creo que debemos pensar seriamente y con urgencia en la posibilidad de tener un Observatorio Regional de la Internet que sistematice la recopilación de datos, que filtre la información y profundice en el conocimiento de la evolución y las tendencias de la Internet con una intencionalidad política, y por supuesto, que enlace a los movimientos, instituciones de gobierno e investigadores que directa o indirectamente evalúan los sistemas digitales, la comunicación y los movimientos sociales y políticos que se articulan a través de la Internet. Necesitamos información para dar la batalla legal frente a las ilegalidades y a las normas supuestamente legales que nos imponen. Y para denunciar, permanentemente, las violaciones y los atropellos.

Ignorar esta guerra no detendrá a los profesionales que comanda el general Elder. Todo lo contrario. Ahora mismo, en este mismo instante, nos están apuntando al cerebro y al corazón. Aceptemos el reto. Meditemos cómo organizarnos y qué legítimos instrumentos están a nuestro alcance para defender a toda costa la Internet solidaria, que es el único modo de impedir que las fantasías de Orwell se instalen entre nosotros, definitivamente, como realidad.

CubaDebate

---

https://www.lahaine.org/mundo.php/comando_del_ciberespacio_de_la_fuerza_ae