# *El teatro informático del Pentágono*

por Eduardo J. Vior

"Los Estados Unidos no están preparados para la guerra cibernética," alarmó el *Washington Post* el pasado lunes 11. "Nueva Guerra Fría en el espacio virtual," anunció el *New York Times* a fin del mes pasado. Ya el mes anterior, en su *Informe sobre el estado de la Unión*, Barack Obama enfatizó que "los enemigos de EE.UU. están buscando cómo sabotear nuestra red eléctrica, nuestras instituciones financieras y nuestros sistemas de control aéreo."

Sin embargo, en paralelo, el *China Daily* del martes 12 informaba que China es una de las mayores víctimas de ataques informáticos. De acuerdo a un informe de la empresa de seguridad Beijing Rising Information Technology Co Ltd. publicado el año pasado, por lo menos el 60 por ciento de los ataques contra grandes compañías chinas e institutos de investigaciones científicas provienen de los Estados Unidos, Corea del Sur, Japón e India.

En tanto, James R. Clapper, Director de Inteligencia Nacional de EE.UU., en su informe al Senado el pasado martes 12, es un poco más objetivo: “Servicios de inteligencia extranjeros han penetrado en numerosas redes gubernamentales, empresarias, académicas y del sector privado. La mayoría de las actividades detectadas apuntaba a redes abiertas conectadas a Internet, pero también a redes encriptadas. Gran parte de los datos sobre patentes norteamericanas está en redes sensibles, pero no clasificadas. La falta de protección de las redes virtuales permite que personas no autorizadas roben en nuestras redes datos importantes para nuestra economía y seguridad nacional.” ¿Se encuentra el mundo realmente al borde de una guerra cibernética entre hiperpotencias que pretenden paralizar la economía de su adversario mediante la masiva destrucción de sus redes virtuales?

Thomas Rid, alemán, lector de “Estudios sobre la Guerra” en el King’s College de Londres y profesor visitante en la Universidad John Hopkins en Washington, advierte contra el mito de la “guerra virtual”. En su reciente libro *Cyber War Will Not Take Place* (*La guerra cibernética no va a ocurrir*) critica la acción conjunta de estrategas, políticos, empresarios, medios y espías para crear un clima de histeria.

En su artículo en *Foreign Policy*, publicado el pasado jueves 14, Rid señala: “muchos participantes en el debate sobre seguridad cibernética reconocen que en él hay mucho inflado. Sin dudas, el maestro de la aparatosidad es el Pentágono, ya aue las primeras que agitan la ameanza cibernética son empresas privadas que lucran con los contratos militares. Por su parte los medios inflan la amenaza para vender más. Finalmente, la comunidad de inteligencia también bate el parche del ataque cibernético, porque todavía está traumatizada por su incapacidad para prever el 11-09-01. Los servicios de inteligencia norteamericanos tienen mucha mejor información, fuentes, conocimientos y analistas que cualquiera de las empresas privadas de seguridad, pero mantienen secretos sus hallazgos. Como los expertos y periodistas se ven entonces compelidos a leer los informes de las empresas privadas, baja el nivel del debate público, sostiene Rid.

Según el experto alemán Obama tiene razón. Es urgente hacer algo, pero la actual campaña publicitaria dificulta hallar una solución racional por cuatro razones: primero, el ruido

mediático impide concentrarse en los reales problemas de ingeniería de las redes. Antiguamente, cada una de las redes que gestionan los servicios esenciales actuaba independientemente. Con el advenimiento de Internet estas redes se interconectaron globalmente y se hicieron muy vulnerables.

Segundo, la campaña actual impide discutir sobre la verdadera inseguridad de las redes. Investigadores de la Universidad Libre de Berlín construyeron un mapa mundial de la vulnerabilidad informática que muestra la debilidad de las redes norteamericanas, europeas y japonesas, pero esta investigación no se discute en los medios.

Tercero, sabotaje y espionaje son dos cosas muy diferentes. Es muy fácil espiar en redes de otro país y robar patentes para competir en el mercado, pero muy difícil sabotear una red más allá de la destrucción de algunos archivos.

Finalmente, el ruido mediático favorece el ataque sobre la defensa. Es mucho más atractivo discutir sobre técnicas de ataque informático –concluye Rid- que sobre la protección de las redes. De este modo las empresas se despreocupan por aumentar su seguridad informática.

Estados Unidos y China (de ellos se trata) no están en guerra cibernética, pero la actual histeria belicista en Washington puede llevar a una peligrosa carrera armamentista en el espacio virtual. Al mismo tiempo se descuida la protección contra peligros reales de redes de gestión de servicios vitales para la mayoría de la población. Por otra parte, la insistencia de las elites de Washington en mejorar las capacidades ofensivas en las redes virtuales puede ser letal para los esfuerzos industrialistas de los países del Sur. Ya hoy las naciones emergentes tienen una participación mínima en el registro de patentes a nivel mundial. Si EE.UU. insiste en robar informes de investigación y sabotear las redes vitales para el buen gobierno político y económico de los países del Sur, el delirio actual destruirá los esfuerzos de cientos de millones de personas para mejorar sus condiciones de vida.