CIBERCOMANDO. EL PENTÁGONO NORTEAMERICANO YA CREÓ UNA UNIDAD MILITAR PARA BLINDARSE DE LOS ATAQUES INFORMÁTICOS.

La guerra fría en el ciberespacio

DIEGO M. VIDAL
internacional@miradasalsur.com

La hiperconectividad mundial ha convertido el espacio virtual en escenarios bélicos intangibles, donde las armas pesadas se mueven a la velocidad de la luz y pueden almacenarse en la más diminuta memoria flash. Estos campos de batalla virtuales no son bañados de sangre ni quemados por la pólvora, pero comparten los mismos objetivos que las guerras de antaño y los daños llegan a ser incalculablemente mayores.

El término "ciberespacio", acuñado por el inglés William Gibson en su novela *Neuromante* (1984), tiene ocupadas a las grandes potencias y demás países del mundo en millonarias inversiones para garantizar sus defensas ante un ciberataque enemigo y evitar que "la comunidad afectada puede experimentar una regresión tecnológica a la Edad de Piedra", como señala el periodista Misha Glenny, compatriota de Gibson, en *El lado oscuro de la red*. "La guerra cibernética se caracteriza por la transnacionalidad, la multiplicidad de blancos, la inmediatez y la volatilidad de los ataques, y utiliza como técnicas la infiltración en redes enemigas, la recolección de datos sensibles, la interferencia de señales inalámbricas, la producción de programas de software con 'puertas traseras' para el acceso exterior y envío de virus", explica a *Miradas al Sur* el licenciado Gustavo Raúl Sain, autor de *Delito y nuevas tecnologías. Fraude, narcotráfico y lavado de dinero por Internet* y docente de la Universidad Nacional de Quilmes.

Aunque las naciones involucradas tratan de mantener en secreto estas investigaciones en el desarrollo de nuevo "armamento de software", cada vez es más evidente la preocupación de los gobiernos por cómo adelantarse a posibles incursiones hostiles. Estados Unidos ha construido un gigantesco centro de operaciones o cibercomando (Uscybercom) en el desierto de Utah, y la República Popular China tiene el suyo en Shanghai. También la Organización del Atlántico Norte (Otan) suma su preocupación y luego de la "ciberagresión" sufrida por Estonia en el 2007 (cuando un masivo asalto de hackers rusos paralizó por dos semanas desde bancos, servicios de saneamientos, webs de gobierno y hasta los semáforos de la capital estonia), a pedido del Centro de Excelencia en la Defensa Cooperativa Cibernética de la OTAN, un grupo de expertos elaboró el Manual Tallín en el que se establecen normas del derecho internacional para los conflictos surgidos en la red. Ahí se considera que la Declaración de San Petersburgo de 1868 o la Convención de Ginebra de 1949 tiene la misma aplicación en la Internet como en cualquier conflagración armada. El general Michael Schmidt, editor de este compendio, sostiene que el texto viene a despejar la visión de que la red de redes es "como una especie de Far West" y que las leyes son tan válidas "para las armas cibernéticas como para cualquier otra arma". Algunos detractores denuncian que el epítome de la alianza militar europea incluye, además, la legitimación del asesinato selectivo de piratas informáticos.

"Un concepto clave que los gobiernos intentan proteger en el marco de una guerra cibernética es lo que se denomina como infraestructuras críticas de información o Scada (acrónimo de Supervisory Control and Data Adquisition, Supervisión, Control y Adquisición de datos), es decir, aquellos sistemas o redes informáticas que gestionan servicios públicos, como conductos de gas, tendido eléctrico, los sistemas de gestión hidrológicos y el control de transporte aéreo, ferroviario o vial de un territorio", afirma Saín. De hecho, hace poco más de una semana, una consultora de la CIA, Michelle Van Cleave, reconoció que hackers chinos logaron sustraer información clave sobre más de 79 mil instalaciones hidráulicas en EE.UU. En ese contexto, Barack Obama autorizó al Pentágono a realizar ataques cibernéticos a gran escala y el secretario de Defensa estadounidense encendió la alarma ante la posibilidad de un "ciber Pearl Harbour". Las declaraciones de Leon Panetta fueron realizadas luego de la intrusión del virus Shamoon, que inutilizó las computadoras de la petrolera saudí Aramco y de la empresa gasífera Rasgas, de Qatar. Una acción ofensiva que los norteamericanos conocen muy bien, desde que en 2010 el virus Stuxnet atacó los sistemas que controlan 4.700 máquinas centrifugadoras para enriquecer uranio en la planta atómica iraní de Natanz. Cerca de 800 fueron destruidas o dañadas por cambios abruptos en su velocidad. Teherán culpó a Tel Aviv y a Washington por la acometida.

Las Fuerzas de Defensa israelitas son fuentes de "extraordinarias investigaciones realizadas en el campo de la guerra informática, cosa que permite a Israel enfrentarse a rivales mucho más poderosos que él en este terreno", revela Glenny en su libro. Si la creación del Stuxnet es parte del trabajo conjunto entre la Unidad 8200 israelí y la Agencia Nacional de Seguridad estadounidense, entonces el gusano informático Duqu, un malware o software malicioso que infiltra instalaciones industriales en preparación de un ataque, tendría el mismo origen. La similitud del lenguaje utilizado para su construcción los emparienta con los creadores, de acuerdo a lo descubierto por Kaspersky Lab, una empresa del magnate ruso de la seguridad Eugeni Kaspersky, quien fue acusado en la revista *Wired* como una de las 15 personas más peligrosas del mundo por colaborar "con los Servicios Federales de Seguridad (FSB)" de Rusia. Esa afirmación de la publicación que dirigen Charles Townsend y Robert Sauerberg se sostiene en la colaboración que brindaron desde el FSB a la República Islámica de Irán al descubrir Kaspersky el virus Flame que afectó a unas 50.00 computadoras.

Por otro lado, la yihad islámica tiene su ciberguerrilla y hasta Hezbollah actúa en el ciberespacio. Los iraníes en el grupo Izz ad-Din al-Qassam Ciber Fighters cuentan con una suerte de comando virtual que centra sus acciones en bancos de Estados Unidos y portales que realicen actos ofensivos contra el islam. Incluso, en medio de la guerra civil siria, apareció el Syrian Electronic Army, que relacionan con el presidente sirio Bashar al Assad, al que se le atribuyen ataques contra medios de comunicación internacionales y mediante la utilización de cuentas de Twitter con informaciones falsas provocar la caída en 145 puntos el índice Dow Jones.

Según Richard Clarke, especialista en materia de seguridad nacional, terrorismo y cibercrimen y profesor universitario en la Harvard's Kennedy School of Government, en la ciberguerra el potencial militar de un Estado no se mide por la capacidad ofensiva en base a los recursos disponibles para atacar al enemigo, sino por el grado de vulnerabilidad que puede poseer una nación a partir de la dependencia a los sistemas controlados por computadora. En ese sentido, la formación de ejércitos sentados frente a una pantalla, más cercanos a los simpáticos nerds de series y películas que a los musculosos e imbatibles rambos, es ya una realidad en la que chinos y coreanos ganan en número, sólo la capacidad de anticipación y respuesta es lo que mantendrá en pie a los contendientes•

> Un informe de la CIA reconoce que, en menos de veinte años, Occidente perderá más de la mitad de su preponderancia global.

IGNACIO RAMONET
Director de *Le Monde español*

Cada cuatro años, con el inicio del nuevo mandato presidencial en Estados Unidos, el National Intelligence Council (NIC), la oficina de análisis y de anticipación geopolítica y económica de la Central Intelligence Agency (CIA), publica un informe que se convierte automáticamente en una referencia para todas las cancillerías del mundo. Aunque obviamente se trata de una visión muy parcial (la de Washington), elaborada por una agencia, la CIA, cuya principal misión es defender los intereses de Estados Unidos, el informe estratégico del NIC presenta una indiscutible utilidad porque resulta de una puesta en común –revisada por todas las agencias de inteligencia de EE.UU.– de estudios elaborados por expertos independientes de varias universidades y de muchos otros países (Europa, China, la India, África, América latina, mundo árabe, etc.).

El documento confidencial que el presidente Barack Obama encontró sobre la mesa de su despacho en la Casa Blanca el pasado 21 de enero, al tomar posesión de su segundo mandato, se acaba de publicar con el título: *Global Trends 2030. Alternative Worlds* (Tendencias mundiales 2030: nuevos mundos posibles).

La principal constatación es el declive de Occidente. Por vez primera desde el siglo XV, los países occidentales están perdiendo poderío frente a la subida de las nuevas potencias emergentes. Empieza la fase final de un ciclo de cinco siglos de dominación occidental del mundo. Aunque Estados Unidos seguirá siendo una de las principales potencias planetarias, perderá su hegemonía económica en favor de China. Y ya no ejercerá su "hegemonía militar solitaria" como lo hizo desde el fin de la Guerra Fría (1989). Vamos hacia un mundo multipolar en el que nuevos actores (China, la India, Brasil, Rusia, Sudáfrica) tienen vocación de constituir sólidos polos continentales y de disputarles la supremacía internacional a Washington y a sus aliados históricos (Japón, Alemania, Reino Unido, Francia).

Para tener una idea de la importancia y de la rapidez del desclasamiento occidental que se avecina, baste con señalar estas cifras: la parte de los países occidentales en la economía mundial va a pasar del 56%, hoy, a un 25% en 2030... O sea que, en menos de veinte años, Occidente perderá más de la mitad de su preponderancia económica... Una de las principales consecuencias de esto es que EE.UU. y sus aliados ya no tendrán proba-