VIGILANCIA ELECTRÓNICA CHINA DE LARGO ALCANCE

Teniente Coronel (R) Timothy Thomas, Ejército de EUA

Esta semana el Congreso aprobó una legislación que requiere un informe por parte del Pentágono sobre las capacidades crecientes de guerra cibernética de China en sus evaluaciones del poder militar chino. La Ley de Autorización de Defensa Nacional del año fiscal de 2008, aprobada ayer por la Cámara de Representantes, incluye una disposición que exige que el informe anual sobre el Poder Militar de de República Popular de China incluya una nueva sección sobre "las iniciativas [de Pekín] para adquirir, desarrollar y desplegar capacidades de guerra cibernética" en sus evaluaciones sobre las capacidades chinas de guerra asimétrica.

—*Early Bird,* 14 de diciembre de 2007

DESDE EL AÑO 2005, el número de ataques cibernéticos chinos contra los sistemas estadounidenses han aumentado a una tasa alarmante. No obstante, el término "ataque" conlleva connotaciones indeseables; es más probable que estas incursiones injustificadas sean misiones de exploración para recolectar datos de inteligencia sobre los sistemas militares de EUA, identificar vulnerabilidades o introducir viruses o "puertas traseras" para lograr el acceso a nuestros sistemas, y para asegurar que el Ejército de Liberación Popular (ELP) de China tenga una ventaja inmediata en caso de guerra con EUA. Si las incursiones fuesen "ataques", nuestros sistemas estarían fuera de servicio y destruidos. Más bien, estas medidas de exploración computacional parecen someterse a una antigua estratagema china: "un ejército victorioso gana primero y luego busca el combate. Un ejército derrotado entabla primero el combate y luego busca la victoria." La exploración vía computadoras para hallar e identificar vulnerabilidades antes de la primera batalla se ajusta bien a esta estratagema.

Estados Unidos, indudablemente, no es el único país que acusa a China de incursiones injustificadas. Alemania, Inglaterra, Francia, Japón, Taiwán, Australia, entre otros, también han sido blancos de China. Cuando se considera estos acontecimientos a la luz de los antecedentes de fuentes abiertas sobre la teoría de las operaciones de información china en los últimos años, existen muchas pruebas circunstanciales para encontrarla culpable de estas acusaciones. Obviamente, la única prueba forense es clasificada y resguardada por las agencias de seguridad de los países que han sufrido invasiones electrónicas de China.

En el presente artículo se explica el pensamiento militar chino que sustenta sus actividades de ataques cibernéticos. Mientras otros artículos se concentran en quién sufrió ataques y cuántas veces, este artículo se

El Teniente Coronel (Retirado) Timothy L. Thomas, Ejército de EUA, es analista de mayor jerarquía en la Oficina de Estudios Militares Extranjeros en el Fuerte Leavenworth, Kansas. Recibió su licenciatura de la Academia Militar de EUA y su Maestría de la Universidad de Southern California.

concentra más en la teoría detrás de los ataques, especialmente el uso de estratagemas electrónicas por parte de la ELP para sus operaciones de redes computarizadas y el uso de terceros tales como los grupos de piratas informáticos (*hackers*) patrióticos. En este artículo se revisa las incursiones chinas desde el año 2005 y examina las evaluaciones de fuentes abiertas provistas por algunos de los teóricos más destacados de la guerra informática (GI) china.

El ELP ha seguido la teoría con la práctica. Las operaciones de redes computarizadas se han transformado en parte de las actividades estratégicas del ELP en tiempos de paz. Más preocupante es el motivo de estas incursiones. ¿Es la exploración? O, ¿es el motivo de estas incursiones colocar caballos de Troya u otro dispositivo en los sistemas de EUA y sus aliados para inutilizarlos o destruirlos en caso de guerra? A medida que se lee sobre las nuevas capacidades chinas en la guerra informática, se hace evidente que las intenciones potenciales de China generan interrogantes.

Las unidades de GI y la ofensiva activa

Aunque se desconoce el motivo preciso de los ataques cibernéticos de China, se puede seguir un razonamiento de causa y efecto en los textos chinos contemporáneos. La causa del encanto chino por las nuevas tecnologías de la información y de la informatización de sus fuerzas es el gran impacto que han tenido estas tecnologías en los asuntos militares, más notablemente el uso norteamericano de tecnología en Irak. El efecto de estas tecnologías en el pensamiento militar chino es su creencia de que sólo los países que toman la iniciativa en una guerra informática o que establecen la superioridad y control de la informática con antelación vencerán y que ello requiere la vigilancia y recolección de inteligencia antes de la primera batalla para preparar el terreno para el uso de sus fuerzas cibernéticas.

En términos históricos, el ELP basó su filosofía estratégica en la "defensa activa", que significa que China nunca atacaría primero a otro país pero estaría preparada para reaccionar en caso que fuese atacada. Esta filosofía ha cambiado en los últimos años con la llegada de la era cibernética. Ha habido un flujo constante de descripciones de las operaciones cibernéticas ofensivas de las FF.AA. chinas y las unidades cibernéticas que participan en las mismas en fuentes abiertas. El hecho de que el ELP reconozca abiertamente la necesidad de operaciones ofensivas refleja una desviación enorme del pensamiento militar tradicional. Además, el ELP ha declarado públicamente que la dependencia norteamericana en los sistemas computarizados es una gran vulnerabilidad que lista para ser explotada. Si China espera equilibrar la gran ventaja norteamericana en la aplicación práctica de la teoría de las operaciones de información (en Kosovo, Irak y Afganistán), tiene que explotar esta vulnerabilidad. Con el fin de entender este cambio de una mentalidad defensiva a una ofensiva en las operaciones, debemos examinar primero los acontecimientos del año 1999.

El año 1999

Hace casi una década, los teóricos chinos de las operaciones de información ya discutían las acciones ofensivas. El libro *Information War* por Zhu Wenguan y Chen Taiyi, publicado en el año 1999, contiene una sección denominada "Conducting Camouflaged Preemptive Attacks" (Llevando a cabo Ataques Preventivos Camuflados). Los autores observan que se necesita una ofensiva preventiva activa para interrumpir y destruir las fuerzas computarizadas ofensivas de sus enemigos.[1] Parece que una parte de los ataques preventivos son la vigilancia de redes, que incluye la recolección de datos sobre el rendimiento, propósito y estructura de los sistemas relacionados con el C4I (mando, control, comunicaciones, computadoras e inteligencia), la guerra electrónica y sistemas de armas. Los autores también observan que, en el sentido más amplio, la vigilancia es un elemento de ataque de informaciones computacionales. Declaran:

> Con el fin de llevar a cabo la vigilancia de computadoras, podemos usar las redes de informaciones computacionales establecidas en tiempos de paz y entrar en ellas como distintos usuarios para realizar la vigilancia en un área más amplia que el campo de batalla. Podemos aprovechar las capacidades de los expertos en computación, específicamente los *hackers*, para completar las tareas de vigilancia computacional… se puede ver que el uso de *hackers* para adquirir las informaciones milita-

> res de las redes computarizadas es un método muy eficaz. Es necesario familiarizarnos con los protocolos de redes y acumular la inteligencia acerca de estas redes.[2]

Los autores agregan que el ELP estableció pequeñas brigadas de fuerzas computarizadas ofensivas y defensivas para realizar estos ataques.[3] El adiestramiento ofensivo incluye cómo diseñar y organizar las invasiones con viruses y cómo ganar el acceso a las redes computarizadas de sus adversarios. Las brigadas ofensivas deben estudiar y analizar repetidas veces las capacidades enemigas. También tienen que distinguir entre la verdad y la decepción, determinar con precisión los centros de control computarizado de un enemigo e interferir estas redes de manera selectiva.[4]

En noviembre de 1999, un artículo del periódico *Jiefangjun Bao* (Diario del Ejército de Liberación) expresó que China podía desarrollar una especialidad de guerra informática—una "fuerza de red"—para complementar el Ejército, la Armada y la Fuerza Aérea. (Aunque el artículo indica que esta iniciativa era muy probable que se hiciera realidad, no existen pruebas para confirmar el establecimiento de esta especialidad hasta el día de hoy.) La tarea de esta fuerza sería la de proteger la soberanía de sus propias redes y realizar la guerra de redes. Los elementos de la guerra de redes incluyen las tecnologías "ofensivas" y "defensivas", de "detección", de "mascarada" (engaño) y de "recuperación". La tecnología de mascarada habilitaría a un individuo a fingir ser un comandante para asumir control de una red.[5]

El año 2000

La idea de concentrarse en las actividades de exploración y de estratagema surgió tan temprano como el año 2000. En un artículo en *Jiefangjun Bao* se comenta que las unidades de nivel ejército hacia arriba deben enfocar sus estudios en la exploración y alarma temprana, coordinación de mando y la aplicación de estrategia.[6] Un artículo en que se confirmó este pensamiento apareció en el diario oficial del ELP, el *China Military Science* (de importancia equivalente del *Joint Force Quarterly* en EUA). En este artículo se expresa que las estratagemas deben crear oportunidades y momentos adecuados para circular viruses.[7]

En otro artículo de *China Military Science* se esclareció la postura ofensiva descrita en el año 1999. En ese artículo, el General Dai Qingmin opina que la ofensiva es tan importante como la defensa activa, y señala, "Dado que el elemento clave para lograr la iniciativa en las operaciones yace en la competencia activa con un enemigo por la superioridad de información, China debe establecer esta visión para las operaciones de información como la "ofensiva activa". Su punto de vista es que se necesita la ofensiva activa para mantener el control sobre la información, adueñarse de la iniciativa y desestabilizar la superioridad enemiga. Los métodos ofensivos de información pueden ayudar a sabotear el sistema de información de un adversario.[8]

Dai, quien fue nombrado jefe del Cuarto Departamento (Guerra Electrónica) del Estado Mayor del ELP, también señala que las estratagemas de las operaciones de información se pueden formular antes de comenzar una guerra para servir como una "espada afilada" que sabotea y debilita a un enemigo superior, mientras protege la capacidad de combate de China. La guerra de información puede servir como una especie de capacidad invisible de combate para evadir el combate con un enemigo más fuerte.[9] Si una meta futura de la guerra informática es derrotar a fuerzas superiores con fuerzas inferiores por medio de estratagemas, entonces estos métodos son una de las medidas chinas para combatir la alta tecnología de EUA.[10] Por ende, las estratagemas podrían ser una de las "armas mágicas" que la cultura estratégica china está siempre enfatizando.

Por último, en el artículo de Dai, publicado en el número de agosto de 2000 del *China Military Science*, él discute el uso de datos electrónicos como estratagemas y el desarrollo de una capacidad integrada de guerra electrónica de redes. Cuando este artículo se relaciona con el concepto de la ofensiva activa, representa uno de los artículos más importantes escritos en China sobre la guerra informática.

Otras publicaciones de menor importancia también analizan las operaciones ofensivas. En una versión puesta en la Internet en el año 2000 de la *Computer and Information Technology*, los analistas del Instituto de Ingeniería Electrónica del ELP en Hefei discuten la necesidad de disponer de equipos de enfrentamiento de redes y el requerimiento de realizar operaciones defensivas como ofensivas.[11] En septiembre de 2000,

el periódico *Guangjiao Jing* reportó que el ELP había establecido recientemente departamentos de guerra informática en las organizaciones a nivel de cuartel general.[12] Por eso, la idea de la operaciones ofensivas no se limitaba sólo a Dai.

El año 2001

El libro *Science of Strategy*, publicado por la Universidad de Defensa Nacional de China, incluye una sección sobre las operaciones ofensivas en la guerra informática. El libro establece que la guerra estratégica de informática debe "usar la ofensiva como la estrategia principal pero estar preparado tanto para la ofensiva como la defensiva." Además, se señala, "Debemos usar la estrategia de un ataque preventivo y tomar la iniciativa. Realizar activamente una ofensiva de información es la clave para adueñarse de la superioridad de información y la iniciativa en el campo de batalla."[13] En este sentido, el planteamiento parece estar relacionado principalmente con las acciones durante la guerra y no con las acciones en tiempos de paz.

En el *Science of Strategy* también se describe el tipo de guerra necesario para combatir en contra de las redes. Se indica que en una guerra de aniquilación, se debe atacar los nodos para desmembrar las redes antes de lanzar un ataque contra los sistemas de armas. Los sistemas de información y de apoyo deben ser siempre los primeros objetivos para causar el desequilibrio operativo. Se señala en *Strategy of Science*, "Después de los ataques para ocasionar daños a una red y de las operaciones continuas que persistentemente debilitan al enemigo, entonces lance enérgicamente un ataque de aniquilación." Las instalaciones terrestres de guerra informática, los medios de transmisión, las estaciones de recepción y las capacidades que garantizan el flujo de informaciones deben ser destruidas en ese orden. Este tipo de ataque permite que se "quite el leño debajo de la caldera".[14] Aunque este escenario parece relacionarse con las condiciones de la guerra, también puede ser fácilmente adaptado a las condiciones de la paz.

De ese modo, la informática ha estimulado el pensamiento estratégico chino; ahora los teóricos militares sustentan que aquellos que no toman acciones preventivas perderán la iniciativa en lo que puede ser una guerra de operaciones de información muy corta. Ellos sugieren que en los conflictos modernos, es más fácil lograr una meta de guerra en una sola campaña o batalla que en cualquier otro momento del pasado. Esta lógica proporciona aún más ímpetu al ELP para continuar sus actividades de exploración cibernética en tiempo de paz y con ello prepararse para "obtener el triunfo".[15]

El año 2002

En un artículo de junio de 2002 se declara que las unidades del ELP estaban preparándose para interferir "con informaciones en términos de orden, tiempo, flujo, contenido y forma; eliminando trozos de informaciones, para crear informaciones fragmentadas; e introduciendo informaciones que consideran informaciones irrelevantes para confundir y engañar a unos y otros."[16] El autor agrega que en un enfrentamiento computarizado las dos partes pueden intentar invadir las redes de información de su contraparte mediante la introducción de virus de computadoras a los software descargables, los que pueden ser activados cuando fuese necesario, con el fin de sabotear los sistemas computarizados de la parte opuesta.[17]

El general Dai Qingmin escribió en el año 2002 que una prioridad para el ELP era la de adquirir equipamiento para llevar a cabo las operación de información ofensivas, y que el ELP debe tomar y mantener la iniciativa.[18] Otras publicaciones también expresaron sus opiniones sobre este tema.

El periódico *Jiefangjun Bao*, por ejemplo, publicó un artículo en agosto de 2002 sobre los tipos de ataques contra redes. Fueron clasificados como "premeditados" (p. ej., un virus de computadora resistente inserto en un software), la contaminación (dirigida a la calidad de la información) "fuerte" (que se refiere a la modulación forzosa de viruses de computadora en las ondas electromagnéticas) y la fisión (la fuerte capacidad regeneradora de un virus).[19] Todas estas se pueden introducir en tiempos de paz, salvo, tal vez, la variedad "fuerte".

El año 2003

En el 10º Congreso Popular Nacional del año 2003, los representantes del ELP revelaron que ese año se activaría las primeras unidades de guerra informática de alta tecnología en Pekín. En el informe, se declaró que las unidades serían incorporadas a todos los ejércitos del ELP. Estas

unidades estarían dotadas de equipamiento de alta tecnología y podrían llevar a cabo la guerra de redes en la Internet y pasar datos por medio de sensores satelitales remotos.[20] Se desconoce la diferencia existente entre la "primera" unidad de guerra informática y las brigadas del mismo tipo que se discutían en el libro chino *Information War* de 1999.

En el año 2003, el General Dai nuevamente destacó la importancia de llevar a cabo estos ataques de información.[21] Dai escribió que la guerra informática es "preliminar" (comienza antes que otras operaciones) y "permanente" (ocurre durante toda la operación). Tal vez el énfasis actual en ganar la iniciativa y en las guerras cortas son las razones principales que dan a Dai la impresión de que la prevención mediante la guerra informática sea necesaria en una guerra futura.[22] Él observa:

> Acciones como la guerra de inteligencia, la guerra psicológica, el engaño de campaña previo al combate parecen ser aún más importantes que la implementación de planeamiento sin obstáculos y la ejecución de la guerra. Por eso, la guerra informática debe comenzar antes de formular los planes de guerra y a medida que se formulan.[23]

Unidades específicas del componente de la reserva también llevan a cabo actividades de la guerra informática. Por ejemplo, a fines de 2003, en la publicación mensual de la Academia de Ciencia Militar del ELP, *Guogang*, dio instrucciones específicas sobre las actividades de ataque de redes a las unidades de la reserva. El autor Li Mingrang señala que las tropas de asalto de informaciones en el papel de "primeras fuerzas" deben generarse de la gente talentosa de las secciones de comunicaciones, telecomunicaciones y financieras y de los institutos de investigación científica y de las escuelas de enseñanza superior. Se deben desarrollar las estratagemas para incrementar la supervivencia de los sitemas.[24] Li agrega:

> No hay escasez de expertos en computación y especialistas de redes, cualquiera de estos podría transformarse en un guerrillero de redes, el cual por sí solo podría abrir un nuevo campo de batalla sin el uso de pólvora y mediante ataques de hostigamiento en las redes, tales como enviar grandes cantidades de datos desde muchas direcciones y concentrándolas en alguna estación de red enemiga para interferir su *router* y paralizar así una estación de redes… y una vez que exista un requerimiento militar, entrar en el sistema de redes para recolectar datos de inteligencia o bien activar virus o detonar "bombas" para lograr el objetivo de combate de destruir la red.[25]

Las fuerzas de la reserva tienen la responsabilidad de formular estrategias ofensivas.

En su libro *Deciphering Information Security*, publicado en 2003, el "padre de la guerra informática" de China, el Coronel (R) Shen Weiguang escribió sobre el desarrollo de una universidad de seguridad de informaciones con un programa de especialización en la seguridad de informaciones militares. Esta especialidad enseña, unos 20 tópicos aproximadamente, "Un estudio de métodos de ataque de hackers", "Detección de intrusiones en redes y defensa contra ataques", "Ataques de informaciones y tácticas de defensa", "Diseño y aplicación de programas de virus computarizados", "Estructuras de sistema de seguridad de redes" y "Exploración para detección de problemas ocultos en redes".[26] Muchos de estos temas se ajustan a las actividades de incursión de las operaciones de redes computarizadas de tiempos de paz definidas por el ELP.

El año 2005

En el libro *Study Guide for Information Operations Theory*, publicado en el año 2005, el General Dai y sus socios definieron 400 términos relacionados con las operaciones de información, y muchos de estos se relacionan con las actividades preventivas o de exploración. Aquí sólo se describe la guerra de redes informáticas:

> La guerra de redes informáticas está compuesta por la exploración de redes informáticas, ataques contra redes computacionales y defensa de las mismas. En su mayor parte, las operaciones incluyen el uso de guerreros de redes armados y equipados. Los medios de las operaciones incluyen una variedad de virus, bombas lógicas y armas chip que han sido desarrolladas con la tecnología computacional. La guerra de redes actuará tanto como un medio de disuasión así como un medio de guerra y puede tener un impacto considerable y profundo en la

política, la economía y las FF.AA. de un enemigo. También es un importante recurso de combate para una fuerza militar menos equipada que enfrenta a otra fuerza que cuenta con capacidades formidables de alta tecnología.[27]

Dai también analizó la importancia de la conducción de la guerra, concentrándose en la disuasión informática como un concepto que se debe considerar y desarrollar más a nivel estratégico. Entre otros que han escrito sobre el tema de la disuasión informática se incluye Shen Weiguang. El libro *Science of Military Strategy* dedica un capítulo entero al tema. En esta última fuente, se explica cómo la disuasión informática (intimidación mediante la demostración de poder de información) puede ser útil en el logro de metas nacionales y militares. Los métodos de disuasión incluyen la tecnología informática (innovaciones de hardware y software), armas informáticas (enmascaramiento o desinformación), así como supresión de recursos de información (análoga a la interferencia activa). Según algunos autores chinos, las teorías de disuasión contra-información también se deben considerar.

En *Warfare Strategy Theory* (2005), Yao Youzhi asevera que la estrategia ha avanzado un punto en que las consideraciones tecnológicas dominan y el uso de la tecnología ha llegado a ser un elemento estratégico. Cualquier estrategia que se aleje de poner énfasis en las armas de alta tecnología no tiene valor útil, según Yao. Eso también significa que China debe formular contra-estrategias adecuadas.[28] Afirma:

> Es necesario ser perito en la utilización de la superautopista de la información, creando información engañosa, difundiendo la incertidumbre de la batalla, e interfiriendo y destruyendo la percepción de la situación estratégica del enemigo, usando así la estrategia para controlar al adversario. Es necesario ser un especialista en el uso del engaño electrónico, camuflaje electrónico, interferencia electrónica, ataques con virus, así como interferencia y engaño satelital, llevando al enemigo a extraer conclusiones erróneas y logrando la meta de engaño estratégico.[29]

Aunque concebidas para uso en la guerra, algunas de estas técnicas también sirven como medidas preventivas en tiempos de paz.

En los comandos de estructura vertical del pasado, una fuerza calculaba su poder al sumar todas sus partes. Hoy en día, el poder de combate es el producto de elementos operativos en el cual las tecnologías informáticas constituyen una multiplicación potencialmente exponencial.[30]

Yao escribe que la guerra "informatizada" ha alterado el significado tradicional de "ataque, captura, control y defensa" dado que los ataques de precisión han hecho posible la destrucción del sistema de guerra completo de un enemigo. El objetivo principal ahora es el sistema de información estratégica de un enemigo. Todas las actividades giran en torno a lograr la supremacía en el campo de batalla, y la supremacía de información es el fundamento de la supremacía en el campo de batalla. Destruir directamente la voluntad de un enemigo ha reemplazado al aniquilamiento de la capacidad militar de un adversario. Este énfasis en la información invita a métodos completamente nuevos en las futuras guerras.[31]

El año 2007

El autor Zhang Zhibin observa en *Jiefangjun Bao*, el 13 de marzo de 2007, que la relación dialéctica que existe entre la ofensiva y defensiva en la guerra de redes debe colocar un énfasis equilibrado en cada cual. Una teoría de disuasión de redes implica que se necesitan ambas capacidades, la ofensiva para asustar a cualquier fuerza enemiga potencial, y la defensiva para frustrar cualquier ataque. Dice Zhang:

> Sólo con un buen trabajo de la defensa positiva, China puede asegurar ganar la iniciativa en la guerra de redes. Por ello, China debe tomar medidas incansables para hallar estas oportunidades preventivas mediante el desarrollo de tecnologías y sistemas de redes así como efectuar la investigación e implementación de las correspondientes operaciones de redes defensivas.[32]

Otros artículos del año 2007 recalcan la necesidad de acciones por parte del ELP para tomar control de redes, incluyendo el acceso, si es posible. Dos libros sobre el tema de las operaciones de información de China de este autor *Dragon Bytes* y *Decoding the Virtual Dragon*, hacen mención a este enfoque de control.

Foto AP, Andy Wong

Una pantalla de computadora que muestra un sitio militar en una base del Ejército en Tianjin, en las afueras de Pekín, 30 de julio de 2007. Redes de computadores han sido seleccionadas por espías cibernéticos que se dice en los medios de prensa que son dirigidas por las fuerzas armadas de China, pero China niega su participación.

Probables ataques cibernéticos chinos contra EUA

En los últimos años, las capacidades de guerra informática y de operaciones de información chinas se han tornado más visibles y preocupantes. China ha usado estas capacidades no sólo en contra de EUA sino, según se dice, contra Japón, Taiwán, Alemania, Inglaterra y Australia también. Debido a la naturaleza de las operaciones de redes computarizadas, se desconoce el número exacto de ocurrencias de exploración de guerra informática o eventos ofensivos que han ocurrido o el motivo de estas incursiones. Estos acontecimientos se han filtrado al dominio público incluyendo los siguientes:

• El espionaje realizado contra las computadoras del Departamento de Defensa de EUA, reportado en la revista *Time*. El artículo trataba de un grupo ilegal de espionaje cibernético al que los investigadores federales denominaron con la clave de *Titan Rain.*[33]

• Las tentativas chinas de cegar un satélite norteamericano, reportadas en *Defense News*. En el informe se discutía ataques con láseres de alta potencia contra un satélite de EUA.[34]

• Ataques de hackers chinos contra la red de la Escuela Superior de Guerra de la Armada de EUA, reportados en *Federal Computer Week*. Este ataque supuestamente se originó en China y causó un apagón total de servicio.[35]

• La destrucción china de un antiguo satélite meteorológico con un misil anti-satélite, reportado en *National Public Radio*. En el informe se citó a un comentarista de la Universidad Popular en Pekín. Este señaló, "la tecnología de destrucción de satélites es lógica en el desarrollo de misiones y una capacidad de guerra infomática."[36]

• Un sofisticado ataque a las computadoras en el Laboratorio Nacional de Oak Ridge en el estado de Tennessee en octubre y noviembre de 2007. El ataque fue en forma de correos electrónicos falsos que, al abrirlos, permitió a los hackers a penetrar la seguridad de las computadoras del laboratorio.[37]

• Ataques por hackers contra Japón y Taiwán, reportados en la prensa de estos dos países.[38] En los informes se notó que estos ataques fueron represalias por las interpretaciones anti-chinas de la historia en Japón y por las reivindicaciones taiwaneses de independencia.

El 5 de septiembre de 2007, el periódico *Kansas City Star* publicó un artículo en que China negó haber efectuado ataques contra algún país. El portavoz del ministerio Jian Yu observó, "El Gobierno de China siempre se ha opuesto el crimen dirigido a causar daño a la Internet, incluyendo el hacking, y ha tomado medidas duras contra este delito de acuerdo con la ley."[39] Rechaza las acusaciones de ataques chinos contra las computadoras en el Pentágono, clasificándolas como "infundadas". Un portavoz del Pentágono rehusó identificar a China como el perpetrador, pero el *Financial Times,* publicado en Gran Bretaña, cita a un alto funcionario norteamericano no identificado que afirma que el seguimiento de la fuente de estas intrusiones apuntaba al ELP.

Una semana antes, la revista *Der Spiegel* de Alemania, reportó que el ELP se había infiltrado en los sistemas de información del Gobierno. En el informe se dijo que los hackers habían sido localizados en Guangzhou y Lanzhou.[40] Así, las pruebas circunstanciales continúan aumentando. Es difícil pensar que Alemania, Australia Japón, Taiwán y EUA están conspirando para acusar a China y presentarla como una nueva amenaza. De hecho, mediante operaciones cibernéticas no provocadas, China parece haberse acusado a sí misma sin la ayuda de ningún otro país.

El uso de terceros por China

Una de las estratagemas de China es "atacar con una espada prestada". Es posible que el uso de hackers patrióticos corresponda a esta estratagema. En un artículo reciente en la revista *Time* se discutió el empleo de un grupo del Programa de Explotación de Redes de Hackers (*NCPH*) para lograr esta meta. Según el artículo, el ELP había desarrollado un concurso para hackers y que el ganador recibiría un salario mensual de las Fuerzas Armadas. Se señaló que el grupo *NCPH* no sólo ganó el concurso y estaba recibiendo el estipendio, sino que el ELP también utilizó el *NCPH* para enseñar técnicas y procedimientos a otros integrantes del equipo de guerra cibernética del ELP. El personal de una sucursal norteamericana de la empresa Verisign, iDefense, ha afirmado que el *NCPH* creó 35 programas para introducir virus *Trojan* (que toman control parcial de computadoras) y que estos programas atacaron agencias gubernamentales de EUA. El iDefense de Verisign acusó al NCPH de desviar millares de documentos no clasificados de EUA. Estas actividades corresponden al enfoque preventivo del ELP.[41]

El concepto de "guerra popular" también se ajusta al llamado hacking patriótico. La "guerra popular" en la era cibernética significa que los ciudadanos participan en las actividades de hacking o ataques cibernéticos contra los sistemas enemigos. Más de 250 grupos de hackers operan actualmente en China.[42] La cantidad podría crear una calidad propia con la variedad e intensidad de incursiones que podrían efectuar. No se podría vincular las fuentes de estas incursiones al ELP, si los grupos de hackers son ciudadanos particulares (o, en realidad, integrantes de las Fuerzas Armada de servicio activo o de la Reserva realizando operaciones cibernéticas en sus computadoras en casa). De nuevo, sólo existen pruebas circunstanciales como base, pero estas pruebas se están tornando abrumadoras.

Conclusiones

La teoría china durante los últimos años indica que China quiere ser especialista en la ofensiva activa, la exploración cibernética, estratagemas cibernéticas y las actividades de explotación computacional en caso de que China entre en una guerra. Si China piensa que puede adueñarse de la iniciativa al adquirir la superioridad de información o al prevenir ataques cibernéticos, entonces los años venideros, puede traer desafíos a este sector. Así como continúa siendo fácil medir la intención de los despliegues de tropas, es más difícil medir la intención de un electrón chino. ¿Está introduciendo un virus, haciendo exploración o causando un apagón de sistemas? El mundo entrará en un territorio incierto a medida que los países intentan formular respuestas y desarrollar acciones de gestión de consecuencias contra las intrusiones electrónicas verdaderamente dañinas.

Los chinos observan que las tácticas y técnicas de las operaciones de información permiten más énfasis en el principio de la ofensiva que en la guerra tradicional. Una fuerza más débil, por ejemplo, puede ocasionar más daños a una fuerza superior con un ataque de información asimétrico oportuno y definido en forma precisa. China se describe con frecuencia como la parte más débil en la relación sino-EUA. Piensa que las operaciones ofensivas tales como la disuasión de informaciones, el bloqueo del flujo de informaciones, la creación de poder informacional (el camuflaje electrónico, engaño de redes, etc.), contaminación de información, hostigamientos informacionales, destrucción de nodos, parálisis de sistemas y destrucción de entidades electrónicas son elementos claves para lograr la vitoria en un conflicto moderno con EUA.

Se debe recordar que este análisis surge sólo de información de fuentes abiertas y comentarios públicos del ELP y que el entendimiento chino de la intersección de estrategia y tecnología informacional, especialmente en su relación con el conflicto real, no es amplio en un sentido práctico. Los chinos han tenido poca experiencia reciente con conflictos. Sus fuerzas no han entablado una guerra real hace décadas. Desde una perspectiva teórica, no obstante, china ha escrito mucho sobre el uso de la tecnología informática y la prevención electrónica, dando a ambos temas mucha consideración. Las intrusiones cibernéticas de China sugieren que los chinos están adquiriendo bastante experiencia práctica y teórica en tiempo de paz.

Se pueden interpretar los comentarios públicos del ELP, ya sea, como una tentativa de cooperar con el Occidente u oponerlo vigorosamente. Tal vez el ELP está siendo muy abierto

y transparente en sus estrategias cibernéticas, tal vez más abierto que en cualquier otro sector de las operaciones militares. (El ELP es mucho más abierto con su pensamiento de la guerra informática, por ejemplo, que Rusia). Si la intención del ELP es oponer al Occidente, de hecho, podría estar ocultando conceptos valiosos de la guerra informática en los "reglamentos" del ELP (el equivalente de doctrina en el ELP) en las direcciones del estado mayor y las instituciones de investigación. Los reglamentos que rigen la guerra informática no están disponibles para otros países, mientras la doctrina no clasificada de EUA se puede acceder libremente en la Internet. El ELP mantiene sus reglamentos bien resguardados. En este caso, la falta de transparencia introduce ambigüedad indeseable. EUA y otros países bajo la amenaza de incursiones del ELP pueden reaccionar con severidad a algunos escenarios desarrollados por los chinos y, así, causar sin querer el estallido de un conflicto.

No se sabe cómo y cuándo China pueda usar sus conceptos activos-ofensivos para propósitos que excedan a la exploración, pero, como conceptos generales, son preocupantes. Es de mal agüero para la cooperación y estabilidad futura si los teóricos chinos piensan en realidad (como declaran abiertamente) que China puede contrarrestar la superioridad informacional de un adversario sólo si China lanza el primer ataque. Sin duda alguna, China continuará usando la tecnología en conjunto con estratagemas innovadoras para tratar de engañar a nuestros sistemas de alta tecnología o posiblemente incluso forzar errores en los procesos cognitivos de los que toman decisiones en EUA. Vivimos en tiempos interesantes.***MR***

NOTAS

1. Zhu Wenguan y Chen Taiyi, *Information War* (lugar y editorial no declarados, 1999), capítulo 5 (*Computer Operations*). Ese capítulo discute las operaciones de información computacionales ofensivas y defensivas.

2. *Ibíd.*

3. *Ibíd.*

4. *Ibíd.* En algún momento en la discusión, los autores declaran: "Necesitamos observar la estrategia de nuestras fuerzas militares de ofensiva activa y asegurar que en el entrenamiento en los conflictos computacionales, tanto la defensa como la ofensiva son socios principales."

5. Leng Bingling, Wang Yulin y Zhao Wenxiang, "Bringing Internet Warfare into the Military System is of Equal Significance with Land, Sea, and Air Power," *Jiefangjun Bao* (Diario del Ejército de Liberación Popular), 11 de noviembre de 1999, pág. 7, conforme traducido y accedido en el sitio web del *Foreign Broadcast Information Service* (Servicio de Informaciones de Transmisiones del Extranjero - *FBIS*), 15 de noviembre de 1999.

6. Fan Changlong, "Stand in the Forefront of the New Military Revolution in Deepening Troop Training through Science and Technology," *Jiefangjun Bao*, 4 de abril de 2000, pág. 6, conforme traducido y accedido en el sitio web de *FBIS*, 6 de abril de 2000.

7. Niu Li, Li Jiangzhou y Xu Dehui, "Planning and Application of Strategies of Information Operations in High-Tech Local War," *Zhongguo Junshi Kexue* (Ciencia Militar China) nro. 4, 2000, págs. 115-22, conforme traducido y accedido en el sitio web de *FBIS*, 9 de noviembre de 2000.

8. Dai Qingmin, "Innovating and Developing Views on Information Operations," *Zhongguo Junshi Kexue*, fecha no dada.

9. *Ibíd.*

10. *Ibíd.*

11. Yang Jian, Zhang Youhua y Lu Zhankun, (sin título), *Jisuanji Yu Xinxi Jishu* (versión en línea de Computadoras e Informática), *Anhui Computer Subscriber Association* y *Anhui Computer Society*, 16 de marzo de 2000, conforme traducido y accedido en el sitio web de *FBIS*, 18 de abril de 2000.

12. "China's IWCapabilities," *Guangjiao Jing*, Hong Kong, 16 de septiembre de 2000.

13. *Ge Zhenfeng*, capítulo 16, sección 4, pág. 366. El autor agradece al Dr. Gary Bjorge, Instituto de Estudios de Combate en Fuerte Leavenworth, Kansas, por la traducción de extractos del libro.

14. *Ge Zhenfeng*, capítulo 24, sección 6, pág. 493.

15. Peng y Yao, págs. 418-19.

16. Wen T'ao, "PLA Bent on Seizing 'Information Control.'" *Hong Kong Ching Pao*, 1 de junio de 2002, nro. 299, págs. 44-46, conforme traducido y accedido en el sitio web de *FBIS*, 5 de junio de 2002.

17. *Ibíd.*

18. Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," *Zhongguo Junshi Kexue*, febrero de 2002, 112-17, conforme traducido y accedido en el sitio web de *FBIS*, 24 de junio de 2002.

19. Fan Yongsheng y Wu Xinghan, "War on Networks: Modern 'Contradictory' Offensive, Defensive Warfare," *Jiefangjun Bao*, 14 de agosto de 2002, pág. 11, conforme traducido y accedido en el sitio web de *FBIS*, 14 de agosto de 2002.

20. "PLA to Organize First Information Warfare Units," *Mingpao News*, 12 de marzo de 2003, disponible en: http://full.mingpaonews.com/20030312.

21. *Direct Information War*, pág. 170.

22. *Ibíd.*, pág. 169.

23. *Ibíd.*

24. Li Mingrang, "Develop the Advantage of People's War under the Conditions of Innovation and Informatization," *Guofang*, 15 de noviembre de 2003, págs. 7-8, conforme traducido y accedido en el sitio web de *FBIS*.

25. *Ibíd.*

26. Shen Weiguang, *Deciphering Information Security* (Xinhua Publishing House; Julio de 2003), págs. 127-241.

27. *Ibíd.*, pág. 211.

28. Yao Youzhi, Editor Jefe, *Warfare Strategy Theory* (Liberation Army Press, 2005), págs. 475-76.

29. *Ibíd.*

30. *Ibíd.*, págs. 346-49.

31. *Ibíd.*, págs. 99-101.

32. Zhang Zhibin, "Offense is Not Necessarily the Best Defense—Preliminary Study and Thinking on the Dialectical Relationship between Offense and Defense in Network Warfare," *Jiefangjun Bao*, 13 de marzo de 2007, conforme traducido y accedido en el sitio web de *Open Source Center*, 9 de abril 2007.

33. Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," *Time*, 29 de agosto de 2005, www.time.com.

34. Vago Muradian, "China Tried to Blind U.S. Sats with Laser," *Defense News*, 25 de septiembre de 2006, pág. 1.

35. Josh Rogin, "Network Attack Disables Naval War College," *Federal Computer Week*, 30 de noviembre de 2006, disponible en: www.fcw.com.

36. Anthony Kuhn, *National Public Radio*, 19 de enero de 2007, entrevista con representante de Pekín.

37. "Oak Ridge National Lab Reports 'Sophisticated' Cyber Attack Netted Personal Data on Visitors," *The Associated Press*, 6 de diciembre de 2007, disponible en: www.iht.com/bin/printfriendly.php?id=8626732.

38. "Chinese Hackers Attack Taiwan Military Computers," *Taipei P'ing-kuo Jih-pao* (versión en línea), 15 de mayo de 2006, conforme descrito el reportaje en CPP20060516310002 del *Open Source Center*.

39. Tim Johnson, "China Denies Cyber-Attack," *Kansas City Star*, 5 de septiembre de 2007, pág. A5.

40. *Ibíd.*

41. Simon Elegant, "Enemies at the Firewall," *Time*, 19 de diciembre de 2007, disponible en: www.time.com/time.

42. Conversación con Scott Henderson, cuyo libro sobre hackers chinos, *Dark Visitor*, de próxima publicación. Ese libro probablemente es la mejor obra no clasificada sobre hackers chinos.