La Modernización Militar y las Ciberactividades de China*

Dr. Larry M. Wortzel, PhD

Testimonio del Dr. Larry M. Wortzel ante la Comisión de Servicios Armados de la Cámara de Representantes

Como miembro de la Comisión de Revisión Económica y de Seguridad de EE.UU.-China, presentaré algunos de los hallazgos de la comisión sobre la modernización militar de China, las relaciones de seguridad EE.UU.-China, y las Ciberactividades de China detalladas en el *Informe Anual de 2013 al Congreso.*[1] Debo indicar que las opiniones que presento hoy, son mías. Quiero reconocer el excelente trabajo de nuestro personal en la preparación del informe anual, y especialmente la excelente investigación del equipo de política exterior y seguridad colaborando en la preparación de este testimonio.

La modernización militar de China

El Ejército Popular de Liberación (EPL), la institución militar de China, está en medio de un amplio programa de modernización que presenta retos importantes para los intereses de seguridad estadounidenses en Asia. Esta modernización incluye la creación de una arquitectura de vigilancia y ataque que apoye operaciones a mayores distancias de la costa de China. Convierte al EPL en una fuerza más formidable en todas las dimensiones de la guerra: aire, espacio, tierra,

* Reimpreso de nuestra AU revista Strategic Studies Quarterly, Vol 8, No. 1, Spring 2014.

03-Wortzel.indd 4 8/15/2014 8:50:45 AM

mar y en el espectro electromagnético. El EPL tiene nuevos buques de combate multimisión, aviones, submarinos y una nueva generación de misiles.

En primer lugar, los elementos principales de este programa—como el misil balístico antibuque DF-21D y el creciente número de submarinos avanzados armados con misiles crucero antibuque—están diseñados para limitar la libertad de acción estadounidense en el Pacífico Occidental. El EPL está ampliando y diversificando rápidamente su capacidad para realizar ataques convencionales contra bases, barcos y aviones estadounidenses y aliados en toda la región, incluyendo aquellas que anteriormente no podía alcanzar con armas convencionales, como las instalaciones militares estadounidenses en Guam. A medida que madura la capacidad anti-acceso y negación de área del EPL, aumentarán los costos y riesgos para Estados Unidos en caso de intervención en un potencial conflicto regional que involucre a China.[2] Los militares chinos, por cierto, conscientes de la historia de los siglos diecinueve y veinte, consideran a estas acciones como estrategias contra la intervención diseñadas para impedir la intervención de militares extranjeros en asuntos de soberanía o territoriales de China.

Es más, el rápido avance de la capacidad de proyección de poderío regional del EPL aumenta la capacidad de Beijing para usar la fuerza contra Taiwán, Japón y reclamantes rivales en el Mar del Sur de China. Lo que es más grave, como la doctrina militar china enfatiza los ataques preventivos, esto aumenta el riesgo en cualquier crisis. Muchos escenarios potenciales de seguridad podrían exigir que Estados Unidos defienda a sus aliados y socios regionales y mantenga el acceso abierto y seguro a las vías aéreas y marítimas comunes en el Pacífico Occidental.

Al mismo tiempo, el aumento del malestar sobre las capacidades de expansión de China y su mayor firmeza están haciendo que los aliados y socios estadounidenses en Asia aumenten sus propias fuerzas militares y fortalezcan las relaciones de seguridad entre sí. Estas tendencias podrían apoyar los intereses estadounidenses en Asia aligerando la responsabilidad operativa de Washington en la región. Por otro lado, si los vecinos de China buscan capacidad militar que se podría usar ofensiva o preventivamente debido a la percepción de que Estados Unidos sería incapaz de cumplir su compromiso al reajuste del equilibrio en Asia, esto podría socavar los intereses estadounidenses en la región.

En el informe anual de 2013 de la comisión, tratamos sobre los siguientes acontecimientos en la modernización militar de China:

Marina

Portaaviones. Desde la puesta en servicio de su primer portaaviones, el *Liaoning*, en septiembre de 2012, China continúa desarrollando una capacidad de aviación de ala fija necesaria para que el portaaviones lleve a cabo misiones de defensa aérea y ataque ofensivo. El *Liaoning* es un antiguo portaaviones ruso comprado de Ucrania. Fue reacondicionado y modernizado en China. La Marina del EPL realizó su primer despegue y aterrizaje exitoso en portaaviones con el Jian 15 (J-15) en noviembre de 2012, certificó a su primer grupo de pilotos de portaaviones y oficiales de señales de aterrizaje en el primer despliegue operativo del portaaviones entre junio y julio de 2013, y verificó el proceso de operaciones de la cubierta de vuelo en septiembre de 2013.[3] El *Liaoning* continuará realizando despliegues cortos y adiestramiento de aviación a bordo del barco hasta 2015 ó 2016, cuando el primer regimiento de J-15 de China debe estar listo para operación. El J-15 es una copia china del Su-33 ruso. Es probable que China siga al *Liaoning* con al menos dos cascos producidos en el país. El primero de estos parece estar en construcción y podría estar operativo antes de 2020.

Misiles balísticos de lanzamiento desde submarino. Se espera que el misil balístico de lanzamiento desde submarinos Julang-2 (JL-2) de China logre capacidad operativa muy pronto.4 El misil está en desarrollo desde hace varios años, lo que indica que las industrias militares chinas aún tienen problemas para desarrollar y poner en operación sistemas nuevos. El JL-2, cuando se

combine con el submarino nuclear con misiles balísticos clase Jin (SSBN) de la Marina del EPL, dará a China su primer disuasivo nuclear basado en el mar creíble. El sistema de armamentos Jin SSBN/JL-2 tendrá una autonomía de aproximadamente 4.000 millas náuticas, permitiendo que la Marina del EPL apunte al territorio continental de los Estados Unidos desde las aguas del litoral de China.[5] Se han desplegado tres Jin SSBN y probablemente se pongan en operación otras dos unidades en 2020.[6]

Capacidad de ataque a tierra desde el mar. Actualmente China no tiene la capacidad de atacar objetivos en tierra con misiles crucero desde el mar. Sin embargo, la Marina del EPL está desarrollando una capacidad de ataque a tierra, probablemente para su submarino de ataque con misiles guiados Tipo-095 y el destructor con misiles guiados Luyang III. Los submarinos modernos y las unidades de superficie armadas con misiles crucero de ataque a tierra (MCAT) complementarán el creciente inventario del EPL de MCAT basados en aire y tierra y misiles balísticos, mejorando la flexibilidad de Beijing para atacar objetivos terrestres a través del Pacífico Occidental, incluyendo las bases estadounidenses en Guam.[7]

Construcción naval. La Marina del EPL continúa aumentando constantemente su inventario de submarinos modernos y unidades de superficie. Se sabe que China está construyendo simultáneamente siete clases de barcos pero es posible que esté construyendo clases adicionales.[8] Las tendencias en el gasto en defensa, investigación y desarrollo, y construcción naval de China sugieren que la Marina del EPL continuará modernizándose. Para 2020, China tendrá unos 60 submarinos capaces de emplear misiles balísticos intercontinentales, torpedos, minas o misiles crucero de lanzamiento desde submarinos. La fuerza de combate de superficie de China también se ha modernizado y ampliado con unas 75 unidades de superficie capaces de realizar múltiples misiones o que han sido modernizadas significativamente desde 1992.[9] Las flotas de combate se apoyan en una fuerza de logística de combate que puede realizar reabastecimiento y reparaciones limitadas en marcha. Todas estas naves estarán equipadas para aprovechar un sistema interconectado redundante de comando, control, comunicaciones, computadoras, e inteligencia, vigilancia y reconocimiento (C4ISR) desplegado por el EPL.

Submarinos de ataque. China dispone de una fuerza formidable de 63 submarinos de ataque diésel-eléctricos y nucleares.[10] Estos submarinos están equipados con torpedos nucleares y convencionales, minas, y misiles crucero antibuque.[11] En 2012, China inició la construcción de cuatro "variantes mejoradas" de su submarino nuclear de ataque clase *Shang*. También continúa la producción del submarino diésel-eléctrico clase *Yuan*—algunos de los cuales incluirán un sistema de propulsión independiente del aire que hace posible operaciones de duración prolongada— y el SSBN clase *Jin*. Además, China está desarrollando dos nuevas clases de submarinos nucleares y podría diseñar y construir conjuntamente cuatro submarinos de ataque diésel-eléctricos avanzados con Rusia.[12] El creciente número de submarinos de China mejorará significativamente su capacidad para atacar barcos de superficie enemigos a través del Pacífico Occidental y proteger futuras patrullas disuasivas nucleares y grupos de combate con portaaviones.[13]

Fuerza Aérea

Aviones de caza. China también está desarrollando dos cazas de próxima generación, el J-20 y el J-31, que podrían ser de baja observabilidad y disponer de radar de matriz activo de escaneo electrónico.[14] La Fuerza Aérea del EPL realizó los primeros vuelos de prueba del J-20 y J-31 en enero de 2011 y octubre de 2012 respectivamente.[15] Estas aeronaves reforzarán la capacidad de China para proyectar poderío y obtener y mantener superioridad aérea en un conflicto regional.

Aviones de transporte de carga. En enero de 2013, China realizó el primer vuelo de prueba de su avión de transporte de carga desarrollado en el país, el Yun-20 (Y-20). Anteriormente China no tenía la capacidad de construir aviones de transporte pesado, por lo que se apoyaba en un pequeño número de aviones Ilyushin-76 (IL-76) rusos para puentes aéreos estratégicos desde

la década de 1990. Las especificaciones de los aviones, proporcionadas por medios chinos, indican que el Y-20 puede llevar aproximadamente el doble de carga útil que el IL-76 y unas tres veces la carga útil del C-130 de EE.UU.[16] El Y-20 mejorará la capacidad del EPL para responder a eventos de crisis de seguridad interna y contingencias fronterizas, apoyar operaciones militares internacionales de pacificación y asistencia humanitaria, y proyectar poderío en un conflicto regional.[17] Estas aeronaves más grandes y la flota ampliada aumentarán la capacidad del EPL para emplear el Décimo Quinto Ejército Aerotransportado, parte de la Fuerza Aérea del EPL.

Aviones bombarderos capaces de MCAT. En junio de 2013, la Fuerza Aérea del EPL comenzó a recibir nuevos aviones bombarderos Hongzha-6K (H-6K). El H-6K, una variante mejorada del H-6 (adaptado originalmente de un diseño soviético de fines de la década de 1950), ha ampliado su alcance desde unas 2.400 millas hasta 3.100 millas, y puede portar el CJ-10, el nuevo MCAT de larga distancia de China. El CJ-10 tiene un alcance de 900 a 1.200 millas.[18] El sistema de armas bombardero y MCAT ofrece a la Fuerza Aérea del EPL la capacidad de realizar ataques convencionales contra blancos regionales a través del Pacífico Occidental, incluyendo las bases estadounidenses en Guam.[19] Aunque se podría modificar el fuselaje del H-6K para portar un MCAT con carga nuclear de lanzamiento desde el aire, y los MCAT de china probablemente tienen la capacidad de portar una ojiva nuclear, no hay evidencia que confirme que China esté desplegando cabezas nucleares en ninguno de sus MCAT de lanzamiento desde el aire.[20] El H-6K podría también portar misiles crucero supersónicos antibuque.[21]

Espacio y contrarresto espacial

En mayo de 2013, China lanzó un cohete a una órbita terrestre casi geosincrónica, marcando el lanzamiento suborbital más elevado desde el Gravity Probe A de los Estados Unidos en 1976, y el lanzamiento suborbital más elevado de China que se conoce hasta la fecha. Aunque Beijing afirma que el lanzamiento fue parte de un experimento científico a gran altitud, los datos disponibles sugieren que estaba probando el vehículo de lanzamiento de una nueva capacidad antisatélite (ASAT) de gran altitud.[22] Si es cierto, tal prueba indicaría su intención de desarrollar una capacidad ASAT para atacar satélites en un rango de altitud que incluye el sistema de posicionamiento global (GPS) estadounidense y muchos de sus satélites militares y de inteligencia. En un potencial conflicto, esta capacidad podría permitir que China amenace la capacidad militar estadounidense de detectar misiles extranjeros y proporcionar comunicaciones, navegación y guía de misiles de precisión seguras.

Es más, en septiembre de 2013, China lanzó un satélite al espacio desde el Centro de Lanzamiento de Satélites de Jiuquan, en el oeste de China. Nuestro informe anual cita comentarios de Gregory Kulacki, de la Unión de Científicos Interesados, quien cree que este lanzamiento podría representar una capacidad de lanzar nuevos satélites en el caso de que China tuviera pérdidas en el espacio en combate espacial.[23]

China ha mejorado también su capacidad de defensa contra misiles balísticos desplegando el sistema de misiles superficie-aire (SAM) SA-20B fabricado en Rusia. En algunos casos, el sistema SAM CSA-9 producido en China también debe ser capaz de interceptar misiles balísticos.[24]

El 27 de diciembre de 2012, China anunció que su sistema regional de navegación por satélite Beidou estaba plenamente operativo y disponible para uso comercial. Con 16 satélites y una red de estaciones terrestres, Beidou ofrece a los suscriptores en Asia servicios de navegación de precisión y coordinación de tiempo de 24 horas.[25] China planea ampliar el sistema Beidou a un sistema global de navegación por satélite hacia 2020.[26] Beidou es una parte crítica de la meta declarada de China de prepararse para luchar guerras en "condiciones basadas en información", que incluye un fuerte énfasis en el desarrollo de las capacidades de C4ISR y guerra electrónica del EPL. El EPL está integrando Beidou en sus sistemas para mejorar su capacidad de comando

y control y ataques de precisión de larga distancia, y reducir la dependencia del EPL en los servicios de navegación de precisión y coordinación de tiempo extranjeros, como el GPS.[27]

Misiles balísticos intercontinentales estratégicos

China está aumentando su capacidad de disuasión nuclear mediante la modernización de su fuerza nuclear. Está adoptando medidas como desarrollar un nuevo misil balístico intercontinental (ICBM) transportado por carretera. Este misil podría ser equipado con un vehículo de reingreso múltiple programable independientemente (MIRV), permitiéndole portar hasta 10 ojivas nucleares.[28] Además de los MIRV, China podría también equipar sus misiles balísticos con ayudas de penetración y podría estar desarrollando la capacidad de transportar los ICBM por tren.[29] Además, de acuerdo con el informe del DoD al Congreso en 2011 sobre las fuerzas armadas de China, el EPL "ha desarrollado y utilizado [instalaciones subterráneas] desde que desplegó sus sistemas de misiles con combustible líquido más antiguos y continúa utilizándolos para proteger y ocultar sus misiles móviles con combustible sólido más nuevos y modernos".[30]

Gastos de defensa

Para apoyar su modernización militar, China continuó aumentando sus gastos de defensa en 2013. En marzo, China anunció que su presupuesto oficial de defensa para 2012 se incrementó en 10,7 por ciento en términos nominales a 117,39 miles de millones de dólares, indicando el apoyo del nuevo liderazgo a los actuales esfuerzos de modernización del EPL. Esta cifra representa un 5,3 por ciento del total del gasto de gobierno y aproximadamente 1,3 por ciento del producto interno bruto (PIB) estimado.[31] El presupuesto anual oficial de defensa de China se ha incrementado por 22 años consecutivos y se ha más que duplicado desde 2006. La mayoría de analistas occidentales concuerdan en que posiblemente Beijing retendrá la capacidad —incluso con menores tasas de crecimiento de su PIB y de los ingresos del gobierno— para financiar la modernización en marcha de sus fuerzas militare.[32]

Es difícil estimar el actual gasto de defensa de China debido a la incertidumbre para determinar cómo afecta la paridad del poder de compra de China al costo de las compras militares en el extranjero y de las mercancías y servicios internos de China, así como la omisión de importantes gastos relacionados con la defensa por parte de Beijing. Algunas compras de armas avanzadas, programas de investigación y desarrollo, gastos en seguridad nacional, y apoyo de los gobiernos locales al EPL no se incluyen en las cifras oficiales del gasto de defensa de China. El Instituto de Estudios Estratégicos Internacionales estima que el gasto de defensa real de China es entre 40 y 50 por ciento mayor que la cifra oficial.[33] El Departamento de Defensa de los Estados Unidos estimó que el gasto de defensa real de China en 2012 se situaba entre 135 y 215 mil millones de dólares, o aproximadamente 20 a 90 por ciento mayor que el presupuesto de defensa anunciado.[34]

Relaciones de seguridad entre EE.UU. y China

Las relaciones entre militares estadounidenses y chinos se profundizaron y ampliaron en 2013 después de varios años de contratiempos. Entre 2012 y 2013, el número de contactos entre militares de EE.UU. y China ha subido a más del doble, desde aproximadamente 20 hasta 40.[35] En particular, el contacto entre la Marina estadounidense y la Marina del EPL ha aumentado de manera significativa durante este período. Los contactos claves entre militares en 2013 incluyeron la primera visita a puerto de un barco de la Marina estadounidense a China desde 2009, la primera visita a puerto de un barco chino a Estados Unidos desde 2006, y el segundo ejercicio

contra la piratería entre Estados Unidos y China de todos los tiempos. Adicionalmente, en marzo de 2013 China aceptó la invitación, extendida primero por el ex Secretario de Defensa Leon Panetta en septiembre de 2012, para participar en el Ejercicio Multilateral de la Cuenca del Pacífico liderada por Estados Unidos cerca de Hawaii en 2014.[36]

El DoD sostiene que una fuerte relación entre militares desarrolla familiaridad en el nivel operativo. El DoD afirma que esto reduce el riesgo de conflicto debido a accidentes y cálculos erróneos, crea líneas de comunicación en el nivel estratégico que podrían ser importantes durante una crisis, contribuye a mejorar las relaciones bilaterales generales, y crea oportunidades para obtener mayores contribuciones de China para la seguridad internacional. El comandante del Comando del Pacífico de EE.UU., Almirante Samuel Locklear, dijo en julio de 2013, "El avance que estamos realizando entre nuestras dos fuerzas armadas es bastante admirable. . . porque podemos sostener un buen diálogo en áreas donde estamos de acuerdo, y hay muchos lugares donde estamos de acuerdo como dos naciones, y podemos también abordar directamente temas de una manera real en donde discrepamos".[37]

Han habido ocho rondas de diálogo estratégico entre China y Estados Unidos, gestionadas actualmente por el Foro del Pacífico–CSIS. Éste es un diálogo Track 1.5 que incluye la asistencia de algunos representantes del gobierno estadounidense, pero virtualmente todos los participantes chinos son de alguna parte de su gobierno. Las últimas rondas de diálogo han tratado sobre algunos de los temas estratégicos más importantes que enfrentan China y Estados Unidos, incluyendo la estabilidad estratégica nuclear; la relación entre ciberataques, guerra en el espacio y estabilidad nuclear; la defensa contra misiles balísticos; y la alerta estratégica temprana. En el diálogo han participado oficiales de las fuerzas de misiles estratégicos de China. Veo esto como uno de los diálogos más productivos que han tenido lugar con China. El EPL es un participante activo. Idealmente tales discusiones deberían ser conversaciones directas, gobierno a gobierno, pero es alentador que el EPL y el Ministro de Relaciones Exteriores de China participen en estos asuntos.

En otro acontecimiento positivo, a mediados de noviembre, el Ejército Estadounidense y las fuerzas de tierra del EPL realizaron su primer ejercicio conjunto de todos los tiempos. El ejercicio se centraba en la asistencia humanitaria en desastres y se realizó en Hawaii.[38]

Mi propia experiencia en contactos directos entre militares con China me lleva a aconsejar cautela en lo que hacemos con el EPL y lo que les mostramos. En mi opinión, no se deben abolir las sensatas limitaciones que el Congreso impone a los intercambios militares con China en la Ley de Autorización de Defensa Nacional (NDAA) de 2000. El informe anual de la comisión también refleja este sentimiento. Los contactos entre militares con China requieren supervisión cuidadosa para garantizar que Estados Unidos no aumente la capacidad de China contra nuestras propias fuerzas, Taiwán, o nuestros amigos y aliados en la región Asia-Pacífico.

En 2013 se realizaron contactos más amplios entre militares de China y Estados Unidos en el contexto de los esfuerzos de China para proyectar las relaciones bilaterales como un "nuevo tipo de relación entre países principales". Este concepto, promovido fuertemente en 2013 por el Presidente de China Xi Jinping y otros oficiales chinos de alto nivel, plantea que Estados Unidos y China deben, como potencias principales, buscar la cooperación en una gama de temas bilaterales y globales tratando de evitar la clase de competencia dañina que a menudo caracteriza a las relaciones entre las potencias dominantes y las emergentes.[39] La cooperación es algo bueno, pero los líderes militares estadounidenses no pueden perder de vista el récord del EPL en cuanto a derechos humanos. Esto dicta limitaciones prácticas sobre lo que hacemos con las fuerzas armadas de China. La misión principal de los militares chinos es mantener al Partido Comunista Chino (PCC) en el poder, tal como lo vimos en la forma en que se usó al EPL durante la Masacre de Tiananmen del 4 de junio de 1989 y en Tíbet.

Ciberactividades de China

Mientras China continúa desarrollando su fuerza naval, fuerza aérea, fuerzas de misiles, y capacidades espaciales y anti espaciales, en los artículos militares chinos, el ciberespacio es un componente cada vez más importante del poderío nacional amplio de China y un elemento crítico de su competencia estratégica con Estados Unidos.[40] Beijing parece reconocer que las ventajas actuales de Estados Unidos en el ciberespacio permiten que Washington recopile inteligencia, ejerza comando y control de fuerzas militares, y apoye operaciones militares. Al mismo tiempo, los líderes de China temen que Estados Unidos pueda usar la Internet abierta y las ciberoperaciones para amenazar la legitimidad del Partido Comunista Chino.

Desde el *Informe Anual al Congreso de 2012* de la comisión, ha surgido fuerte evidencia de que el gobierno chino está ordenando y ejecutando una campaña de ciberespionaje en gran escala contra Estados Unidos. Hasta la fecha, China ha comprometido una variedad de redes estadounidenses, incluyendo las del DoD y de empresas privadas. Estas actividades están diseñadas para lograr varios objetivos amplios de seguridad, políticos y económicos.

No hay indicaciones de que la revelación pública del ciberespionaje chino en detalle técnico durante 2013 haya hecho que China cambie su actitud respecto al uso del ciberespionaje para hacerse de propiedad intelectual e información patentada. El informe de Mandiant, una empresa privada estadounidense de ciberseguridad, sobre las actividades de ciberespionaje de la Unidad 61398 del EPL dio lugar a que la unidad modificara sus "herramientas e infraestructura" informáticas para hacer que las futuras intrusiones sean más difíciles de detectar y atribuir.[41] Hay unas 16 unidades y agencias de reconocimiento técnico (inteligencia de señales) en el EPL, y al menos siete unidades de guerra electrónica y medidas de contrarresto electrónico.[42] Cada una de las siete regiones militares de China es apoyada por un regimiento de medidas de contrarresto electrónico, y parece que la Segunda Fuerza de Artillería del EPL tiene su propia unidad de apoyo.[43] Estas organizaciones se centran en penetraciones de sistemas informáticos, ciberespionaje y guerra electrónica.

Cuando se le confronta con acusaciones públicas de Estados Unidos sobre ciberespionaje, Beijing usualmente trata de refutar la evidencia indicando la anonimidad del ciberespacio y la falta de información forense técnica verificable. También cambia el foco de los medios presentándose como la víctima de las ciberactividades de Washington y pidiendo una mayor cooperación internacional en ciberseguridad.[44] En una conferencia de prensa un día después que Mandiant publicó su informe en febrero de 2013, un vocero del Ministerio de Relaciones Exteriores de China dijo, "La especulaciones y acusaciones sin fundamento sobre ataques de piratas informáticos, con varios fines, son poco profesionales e irresponsables y no ayudan a resolver el problema". También enfatizó que los ciberataques son un serio problema para China.[45]

Sin embargo, varios informes públicos del gobierno estadounidense, reconocimientos de empresas privadas que han sido blanco de ciberespionaje, investigaciones por empresas de ciberseguridad, y los informes de la prensa estadounidense contradicen las perennes negaciones de Beijing. Aunque la atribución es difícil y demanda grandes habilidades, el análisis de tendencia está permitiendo que los profesionales de ciberseguridad desarrollen un entendimiento más amplio de los ciberactores, herramientas, tácticas, técnicas y procedimientos de China.

Amenazas a la seguridad nacional de Estados Unidos

El ciberespionaje chino contra el gobierno estadounidense y la base industrial de defensa presenta una amenaza importante para las operaciones de las fuerzas militares estadounidenses, la seguridad y el bienestar del personal militar, la efectividad del equipo, y el estado de disponibilidad. Aparentemente, China utiliza estas intrusiones para tapar brechas en sus propios programas de investigación, asignar blancos futuros, recopilar inteligencia sobre estrategias y planes

estadounidenses, habilitar futuras operaciones militares, acortar los cronogramas de investigación y desarrollo (I+D) para las tecnologías militares, e identificar vulnerabilidades en los sistemas estadounidenses y desarrollar medidas de contrarresto.[46]

La doctrina militar en China también exige ataques sobre la estructura crítica del territorio nacional del oponente en caso de conflicto. En julio de 2013, un investigador de amenazas en Trend Micro, una empresa privada de ciberseguridad japonesa, anunció que había detectado una intrusión informática china, desde diciembre de 2012, de una trampa "honeypot".[47] Había creado la trampa honeypot para simular el sistema de control industrial de una planta de agua en Estados Unidos. El investigador atribuyó la intrusión a la Unidad 61398, según los análisis forenses.[48] Si resulta cierto, esto sugiere que la Unidad 61398 está recopilando inteligencia de infraestructura crítica además de otros objetivos. Tales actividades son consistentes con la doctrina del EPL, que explica que una función de las operaciones de redes de computadora en tiempo de guerra es "perturbar y dañar las redes de las instalaciones de infraestructura del [adversario], como sistemas de generación de energía eléctrica, sistemas de telecomunicaciones, y sistemas educativos".[49]

En años recientes se han identificado varios casos de ciberespionaje chino orientados a programas de seguridad nacional de Estados Unidos. En mayo de 2013, el *Washington Post* describió un informe clasificado de la Junta de Ciencia de Defensa, que lista más de 24 diseños de sistemas de armamentos estadounidenses que según junta habían sido accedidos por intrusos informáticos. Según el *Washington Post,* "Oficiales superiores militares e industriales con conocimiento de las intrusiones dijeron que la gran mayoría eran parte de una campaña amplia de espionaje chino contra los contratistas de defensa y las agencias de gobierno de los Estados Unidos". La lista incluye el sistema de misiles Patriot, el sistema de defensa con misiles balísticos Aegis, el avión caza F/A-18, el avión de combate multifunción V-22 Osprey, y el Buque de combate para litoral.[50]

La información obtenida de las intrusiones en las redes de contratistas militares estadounidenses probablemente mejora el conocimiento de China sobre los sistemas de armamentos estadounidenses, habilita el desarrollo de medidas de contrarresto, y acorta los tiempos de investigación y desarrollo para tecnologías militares de China.[51] Además, las mismas intrusiones que los ciberactores chinos emplean para espionaje también se podrían emplear para preparar ciberoperaciones ofensivas. Los ciberactores chinos podrían insertar funciones latentes en el código del software o los componentes del equipo estadounidense que podrían emplearse en un conflicto potencial entre Estados Unidos y China.

En años recientes ha habido inquietudes sobre los riegos de seguridad en la cadena de suministro del DoD. En una reunión en mayo de 2013, los comisionados y oficiales del DoD discutieron la interpretación de la ley estadounidense en relación a las fuentes de adquisiciones. Los funcionarios del DoD indicaron que un estándar de evaluación de adquisiciones más estricto que tenga en cuenta las inquietudes de adquisiciones solo se aplicaría a los artículos de la Lista de Municiones de Estados Unidos. Los artículos que no estén en la lista se juzgan por un estándar diferente, que algunos oficiales creen que podría excluir las inquietudes sobre el origen de los productos. Por ejemplo, los artículos adquiridos por las instalaciones de mantenimiento de C4ISR no están sujetos a un control más estricto. Los comisionados plantearon su preocupación de que esta interpretación de la ley estaba limitando la capacidad del departamento para abordar riesgos potenciales provenientes de ciertas fuentes de adquisición. Los comisionados exhortaron al DoD a ampliar el alcance del estándar más estricto a artículos que no están en la lista de municiones.

Actualmente el DoD está yendo en esa dirección. La Sección 806 de la NDAA del Año Fiscal 2011 (Ley Pública 111-383), tiene por objeto abordar el problema, pero aún no se ha implementado plenamente. La Sección 806 autoriza al Secretario de Defensa y a los Secretarios del Ejército, la Marina y la Fuerza Aérea a rechazar fuentes de adquisiciones de tecnología de informa-

03-Wortzel.indd 11 8/15/2014 8:50:46 AM

ción alegando protección de la seguridad de la cadena de suministro si el DoD recomienda hacerlo.[52] El Departamento está en el proceso de implementar la Sección 806, habiendo realizado ejercicios de simulación y redactado la Regla Suplementaria del Reglamento de Adquisiciones Federales de Defensa que implementa la Sección 806. En mayo, la regla estaba siendo sometida a coordinación entre agencias.[53] Estos cambios en el sistema de adquisiciones del DoD podrían darle a los oficiales la flexibilidad necesaria para proteger todos los sistemas del DoD. Sin embargo, el avance ha sido lento y el problema que resaltaron los comisionados persistirá hasta que se implemente la nueva política, planteando potencialmente una amenaza a la seguridad nacional. Por lo tanto, en el *Informe Anual al Congreso de 2013,* la comisión recomienda al Congreso que exhorte a la administración para que acelere el avance de la implementación de la Sección 806 de la NDAA del Año Fiscal 2011.

Los desarrollos en la computación en nube en China pueden presentar riesgos de ciberseguridad para los usuarios y proveedores estadounidenses de servicios de computación y pueden también tener consecuencias para la seguridad nacional de Estados Unidos. En base a los hallazgos de un informe de Defense Group, Inc. para la comisión, la relación entre el Ministerio de Seguridad del Estado (MSS) y la Zona Especial de Computación en Nube de Chongqing representa una amenaza de espionaje potencial para las empresas extranjeras que usen servicios de computación en nube proporcionados desde la zona o que basen sus operaciones allí.[54] Además, el plan de enlazar los centros de datos de 21Vianet en China y los centros de datos de Microsoft en otros países sugiere que el gobierno chino podrá algún día ganar acceso a los centros de datos fuera de China a través de centros de datos chinos.[55] Teniendo en cuenta los temas sobre espionaje, en el *Informe Anual de 2013*, la comisión recomienda que el Congreso ordene a la administración que prepare un inventario del uso existente de plataformas de computación y servicios en nube del gobierno federal y determine dónde se encuentran localizados geográficamente los servicios de almacenamiento de datos y computación. Tal inventario debería prepararse anualmente y reportarse a los comités de jurisdicción adecuados.

La computación en nube también puede mejorar la capacidad de C4ISR del EPL. DGI indica que la computación en nube "podría habilitar el desarrollo y despliegue más efectivo y flexible de los equipos militares, mientras que al mismo tiempo mejora la capacidad de supervivencia de los sistemas de información del EPL al dotarlos de mayor redundancia (permitiendo que las capacidades de un sistema sobrevivan la inhabilitación o destrucción de cualquier nodo individual)".[56]

Amenaza para la industria estadounidense

El ciberespionaje de China contra las empresas comerciales estadounidenses presenta una amenaza importante para los intereses y la competitividad de las empresas estadounidenses en industrias importantes. Este ciberespionaje complementa al espionaje humano tradicional. Mediante estos esfuerzos, el EPL y las industrias de defensa de China pueden dar saltos en tecnologías y sistemas y llenar las brechas en sus propias capacidades de investigación y desarrollo, ahorrando tiempo y dinero. El General Keith Alexander, Comandante del Cibercomando Estadounidense, estimó que el costo para las empresas estadounidenses del hurto de propiedad intelectual es de unos 250 mil millones de dólares al año, aunque no todas las pérdidas se pueden atribuir a la actividad china.[57] Las entidades chinas empeñadas en el ciberespionaje y otras formas de espionaje económico probablemente consideran que robar propiedad intelectual e información patentada es más económico que invertir en los lentos programas de investigación y desarrollo.[58] Estos robos apoyan a los planes nacionales de desarrollo de ciencia y tecnología que el gobierno de la RPC administra y dirige centralmente.

El gobierno chino, principalmente a través del EPL y el Ministerio de Seguridad del Estado, apoya estas actividades proporcionando a las empresas de propiedad del estado información y

datos extraídos a través de ciberespionaje para mejorar su ventaja competitiva, acortar los tiempos de investigación y desarrollo, y reducir los costos. La fuerte correlación entre empresas estadounidenses expuestas y las industrias designadas por Beijing como industrias "estratégicas" indica además un grado de auspicio estatal y posiblemente hasta apoyo, dirección y ejecución del espionaje económico chino.[59] Tal apoyo del gobierno permite que las empresas chinas superen en la competencia a las empresas estadounidenses, que no tienen la ventaja de usar los datos de inteligencia del gobierno para beneficio económico.[60]

Es difícil cuantificar los beneficios que las empresas chinas obtienen del ciberespionaje. No sabemos todo acerca de las clases de información que se busca y obtiene, ni tampoco sabemos siempre qué actor chino robó la información. Algunos robos pueden producirse pero nunca se detectan. En términos de inteligencia empresarial, algunos blancos del robo informático incluyen información relacionada a negociaciones, inversiones, y estrategias corporativas incluyendo correos electrónicos de ejecutivos, planes empresariales de largo plazo, y contratos. Además del robo informático, las empresas chinas casi con certeza adquieren información mediante actividades de espionaje tradicional, lo que limita nuestra capacidad de identificar el impacto del ciberespionaje en particular. No obstante, es claro que China no es solo el líder global en el uso de métodos informáticos para robo de propiedad intelectual, también representa la mayoría de los casos de robo de propiedad intelectual a nivel global.[61] En varias ocasiones en años recientes, los actores chinos han utilizado las ciberactividades para obtener información sensible o patentada de empresas estadounidenses:

- En el informe de Mandiant mencionado anteriormente, hay evidencia que desde 2006 la Unidad 61398 del EPL ha penetrado las redes de por lo menos 141 organizaciones, incluyendo empresas, organizaciones internacionales, y gobiernos de otros países. Estas organizaciones se encuentran localizadas o tienen oficinas matrices en 15 países y representan 20 sectores principales, desde tecnología de la información hasta servicios financieros. Entre las organizaciones afectadas, el 81 por ciento estaban localizadas en Estados Unidos o tenían oficinas matrices en Estados Unidos. Según Mandiant, la Unidad 61398 obtuvo acceso a una amplia variedad de información intelectual e información confidencial mediante estas intrusiones.[62] La Unidad 61398 es la Segunda Oficina del departamento de reconocimiento técnico del EPL, y tiene base en Shanghai.[63]
- En otro ejemplo destacado de una empresa china que supuestamente buscaba acceder a propiedad intelectual de una empresa estadounidense mediante ciberespionaje, el Departamento de Justicia (DoJ) en junio de 2013, presentó cargos contra Sinovel Wind Group, una firma del sector energía de China, alegando que Sinovel robó propiedad intelectual de la empresa American Superconductor (AMSC) basada en Massachusetts.[64] Una vez que Sinovel pudo reproducir tecnología de AMSC después de robar código fuente confidencial, la firma china rompió la asociación, canceló las órdenes existentes, y devastó los ingresos de AMSC. Esta empresa ha enjuiciado en China a Sinovel buscando compensación, un esfuerzo que todavía continúa y le ha ocasionado gastos legales de más de 6 millones de dólares.[65] Mientras estos juicios se mueven lentamente por el sistema legal chino, y añade más costos legales a ASMC, Sinovel aprovecha las ganancias de la tecnología robada.[66]

Disuasión del robo informático chino

Es claro que revelar el nombre de los perpetradores en China en un intento de avergonzar al gobierno chino no es suficiente para desanimar a las entidades chinas del ciberespionaje contra las empresas estadounidenses. La mitigación del problema requerirá un enfoque bien coordinado entre el gobierno estadounidense y la industria. El Congreso, la administración Obama y

los expertos externos discuten muchas acciones potenciales. Estas acciones incluyen vincular el ciberespionaje económico a las restricciones comerciales, prohibiendo que las empresas chinas que utilizan propiedad intelectual de Estados Unidos tengan acceso a los bancos estadounidenses y prohibiendo el viaje a Estados Unidos de organizaciones chinas que participan en el ciberespionaje. La Comisión de Revisión Económica y de Seguridad de EE.UU. - China recomienda que el Congreso tome las siguientes medidas:

- Adopte una legislación que aclare las acciones que pueden tomar las empresas para realizar el seguimiento de propiedad intelectual robada mediante ciberintrusiones.
- Enmiende la Ley de Espionaje Económico (18 U.S.C. § 1831-1839) para permitir un derecho privado de acción cuando ocurra robo de secretos comerciales.
- Apoye los esfuerzos de la administración para lograr un alto estándar de protección de los derechos de propiedad intelectual en la Asociación Transpacífico y la Asociación Transatlántica de Comercio e Inversiones.
- Aliente a la administración a asociarse con otros países para establecer una lista internacional de individuos, grupos y organizaciones que participan en el ciberespionaje comercial. La administración y los gobiernos socios deben desarrollar un proceso para la validación, la adjudicación y el acceso compartido de la lista.
- Inste a la administración para que continúe mejorando su intercambio de información sobre amenazas informáticas con el sector privado, particularmente con las empresas pequeñas y medianas.

Es mi opinión personal que el Presidente ya tiene la autoridad para imponer sanciones sobre personas, industrias de gobierno y empresas de China a través de la Ley de Facultades para Emergencia Económica Internacional.[67] Si la magnitud del daño a la economía estadounidense es tan grande como el que cita el General Alexander, el Presidente debería ejercitar esa autoridad.

Mantener el "reajuste del equilibrio" militar estadounidense en Asia

En enero de 2012, la *Guía Estratégica de Defensa* del DoD declaró que los militares estadounidenses "reajustarán necesariamente el equilibrio hacia Asia" enfatizando las alianzas existentes, ampliando las redes de cooperación con los socios "emergentes", e invirtiendo en capacidades militares para garantizar el acceso y la libertad de maniobra en la región.[68] El Jefe de Operaciones Navales Estadounidenses, Almirante Jonathan Greenert, explicó la función de la Marina de los Estados Unidos en el reajuste del equilibrio: "Siguiendo las órdenes de la *Guía Estratégica de Defensa* de 2012 . . . la Marina de los [Estados Unidos] ha formulado e implementado un plan para reajustar el equilibrio de nuestras fuerzas, sus puertos de base, y nuestro capital intelectual y asociaciones hacia la región Asia-Pacífico".[69] Concretamente, la Marina de los Estados Unidos busca aumentar su presencia en la región Asia Pacífico de unos 50 barcos en 2013 hasta 60 barcos en 2020 y "reajustar el equilibrio de los puertos de base a 60 por ciento" en la región para 2020.[70]

Sin embargo, el informe anual de la comisión señala que el Secretario de Defensa Chuck Hagel, en julio de 2013, dijo que Washington tendría que escoger entre una fuerza militar moderna y más pequeña y una más antigua y más grande si continúa la provisión de fondos con recortes automáticos.[71] El Almirante Greenert ha advertido que las restricciones en el entorno del presupuesto actual podrían retrasar o impedir que la marina estadounidense logre sus objetivos de reajuste del equilibrio.[72] Hay una creciente preocupación en Estados Unidos y entre sus aliados y socios de que el DoD no pueda cumplir su compromiso de reajustar el equilibrio debido a los presupuestos de defensa decrecientes y las crisis emergentes en otros lugares del mundo. Esto podría dar lugar a que algunos países de la región se adapten cada vez más a China

o busquen capacidades militares que podrían ser usadas ofensivamente o de manera preventiva. Cualquiera de los dos escenarios podría socavar los intereses estadounidenses en la región.

Los exhorto a tener en cuenta que hacia 2020, China podría tener una fuerza naval y fuerza aérea en Asia que supere en número y casi iguale la capacidad técnica de nuestras propias fuerzas. Si nuestra fuerza militar se reduce a causa de nuestros problemas de presupuesto, podremos tener el 60 por ciento de nuestras fuerzas en la región Asia-Pacífico, pero 60 por ciento de 200 barcos es mucho menos que 60 por ciento de una fuerza naval de 300 barcos. Puede que eso no sea suficiente para disuadir a China o tranquilizar a nuestros amigos y aliados en la región. ❑

Notas

1. El informe completo se puede ver en http://www.uscc.gov/Annual_Reports/2013-annual-report-congress.

2. Acciones "Anti-acceso" (A2) son aquellas que tienen por objeto retardar el despliegue de las fuerzas del adversario en el teatro de operaciones o hacer que las fuerzas operen desde distancias más alejadas del conflicto de las que éstas podrían preferir. Las acciones A2 afectan el movimiento hacia el teatro. Acciones de "Negación de área" (NA) son aquellas que tienen por objeto impedir las operaciones del adversario dentro de áreas donde las fuerzas amigables no pueden o no intentarán impedir el acceso. Las acciones NA afectan el movimiento dentro del teatro. *Air Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges (Batalla Aire Mar: Colaboración del servicio para enfrentar los desafíos Anti-acceso y Negación de área)* (Alington, VA: Oficina de Combate Aire-Mar de EE.UU., mayo de 2013), 2–4.

3. "Chinese Aircraft Carrier Returns to Home Port (Portaaviones chino vuelve a puerto de origen)", *Renmin Ribao (People's Daily)*, 22 de septiembre de 2013, http://english.peopledaily.com.cn/90786/8407244.html; "China's Carrier-Borne Jet Pilots Receive Certification (Pilotos de aviones a reacción de portaaviones de China reciben certificación)", Xinhua, 4 de julio de 2013, http://english.peopledaily.com.cn/90786/8310416.html; "China's First Aircraft Carrier Leaves Homeport for Sea Trials (Primer portaaviones de China deja puerto de origen para pruebas en el mar)", Xinhua, 11 de junio de 2013, http://news.xinhuanet.com/english/china/2013-06/11/c_132447284.htm; "China's Aircraft Carrier Anchors in Military Port (Portaaviones de China ancla en puerto militar)", Xinhua, 7 de febrero de 2013, http://www.china.org.cn/china/NPC_CPPCC_2013/2013-02/27/content_28071340.htm; y "China Now Capable to Deploy Jets on Aircraft Carrier: Navy (China ahora puede desplegar aviones a reacción en portaaviones: Marina)", Xinhua, 25 de noviembre de 2013, OSC ID: CPP20121125968098, http://www.opensource.gov.

4. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013 (Informe Anual al Congreso: Acontecimientos militares y de seguridad que involucran a la República Popular China 2013)* (Washington: DoD, 2013), 31.

5. *The People's Liberation Army Navy: A Modern Navy with Chinese Characteristics (La Marina del Ejército de Liberación Popular: Una armada moderna con características chinas)* (Suitland, MD: Oficina de Inteligencia Naval [ONI], 2009), 23.

6. *PLA Navy Orders of Battle 2000–2020 (Órdenes de Combate de la Marina del EPL 2000-2020)*, respuesta escrita a la solicitud de información proporcionada a la Comisión de Revisión Económica y de Seguridad de EE.UU.-China (Suitland: ONI, 24 de junio de 2013); y *Annual Report to Congress (Informa Anual al Congreso),* 10, 31.

7. *Informe Anual al Congreso*, 6–7; y J. Michael Cole, "China's Growing Long-Range Strike Capability (Crece la capacidad de ataque de larga distancia de China)", *Diplomat*, 13 de agosto de 2012, http://thediplomat.com/flashpoints-blog/2012/08/13/chinas-growing-long-range-strike-capability/.

8. Andrew Erickson y Gabe Collins, "China Carrier Demo Module Highlights Surging Navy (Módulo de demostración de portaaviones de China resalta una marina emergente)", *National Interest,* 6 de agosto de 2013, http://nationalinterest.org/commentary/china-carrier-demo-module-highlights-surging-navy-8842; *PLA Navy Orders of Battle 2000–2020 (Órdenes de combate de la Marina del EPL 2000-2020); e Informe anual al Congreso, 5–7.*

9. *PLA Navy Orders of Battle 2000–2020 (Órdenes de Combate de la Marina del EPL 2000-2020).*

10. Ibíd.

11. Sobre Sobre armas nucleares, incluyendo torpedos, minas, misiles crucero antibuque, y ADMs/minas, véase Robert S. Norris, Andrew S. Burrows, y Richard W. Fieldhouse, *British, French, and Chinese Nuclear Weapons (Armas nucleares británicas, francesas y chinas), Nuclear Weapons Databook, vol. 5* (Boulder, CO: Westview Press, 1994), 359; Gregory B. Owens, "Chinese Tactical Nuclear Weapons (Armas nucleares tácticas chinas)" (tesis de maestría, Naval Postgraduate School, junio de 1996), 4; "Global Nuclear Stockpiles, 1945–1997 (Reservas nucleares globales 1945-1997)", *Bulletin of the Atomic Scientists,* noviembre/diciembre de 1997, 67; "Estimated Nuclear Stockpiles 1945–1993 (Reservas nucleares estimadas 1945-1993)", *Bulletin of the Atomic Scientists,* diciembre de 1993, 57; y Robert S. Norris, "Nuclear Arsenals of the United States, Russia, Great Britain, France and China: A Status Report (Arsenales nucleares de Estados Unidos, Rusia, Gran Bretaña, Francia y China: Un informe de situación)", presentación en el Quinto Seminario ISODARCO en Beijing Sobre Control de Armas, Chengdu, China, noviembre de 1996. Sobre torpedos, véase "Archive of Nuclear Data (Archivo de información nuclear)", http://www.nrdc.org/nuclear/nudb/datab17.asp; y Ronald O'Rourke, *China Naval Modernization (Modernización naval de China)* (Washington: Servicio de Investigación del Congreso [CRS], 5 de septiembre de

2013), http://www.fas.org/sgp/crs/row/RL33153.pdf. Según sinodefense.com, en diciembre de 2005 China compró torpedos Tipo 53-65 de Rusia y 40 torpedos Shkval en 1998.

12. "China 'Buys Fighter Jets and Submarines from Russia' (China 'Compra aviones de caza y submarinos de Rusia'", *BBC News,* 25 de marzo de 2013, http://www.bbc.co.uk/news/world-asia-21930280; y Robert Foster, "Russia to Sell, Co-Produce Lada-class Submarines to China (Rusia venderá o coproducirá submarinos clase Lada con China)", *Jane's Defence Weekly*, 20 de diciembre de 2012, http://www.janes.com/article/19682/russia-to-sell-co-produce-lada-class-submarines-to-china.

13. *PLA Navy Orders of Battle 2000–2020 (Órdenes de Combate de la Marina del EPL 2000-2020); y el Informe Anual al Congreso, 5–7.*

14. Roger Cliff, "Chinese Military Aviation Capabilities, Doctrine, and Missions (Capacidad, doctrina y misiones de la aviación militar china)", en *Chinese Aerospace Power: Evolving Maritime Roles (Poderío aeroespacial chino:* Funciones marítimas cambiantes), editores Andrew S. Erickson y Lyle J. Goldstein (Annapolis, MD: Naval Institute Press, 2011), 252; y Richard Fisher, "Deterring China's Fighter Buildup (Disuadir el aumento de aviones de caza de China)", *Defense News,* 19 de noviembre de 2012, http://www.defensenews.com/article/20121119/DEFFEAT05/311190005/.

15. *Informe Anual al Congreso,* 8; y Fisher, "Deterring China's Fighter Buildup (Disuadir el aumento de aviones de caza de China)".

16. "Resumen: PRC Expert Says Yun-20 Transport Makes Strategic Air Force Possible (Resumen: Experto de la RPC dice que el avión de transporte Yun-20 hace posible la Fuerza Aérea Estratégica)", OSC ID: CPP20130128787028, Open Source Center, 27 de enero de 2013, http://www.opensource.gov.

17. "Summary: Guangdong Journal Views Strategic Card of 'Yun-20' Jumbo Air Freighter (Resumen: Diario de Guandong ve carta estratégica en el transporte aéreo Jumbo 'Yun-20')", OSC ID: CPP20130214695013, 31 de enero de 2013; y Andrew Erikson y Gabe Collins, "The Y-20: China Aviation Milestone Means New Power Projection (El Y-20: Hito de la aviación china indica nueva proyección de poderío)", *Wall Street Journal: China Real Time Blog,* 28 de enero de 2013, http://blogs.wsj.com/chinarealtime/2013/01/28/the-y-20-china-aviation-milestone-means-new-power-projection/.

18. Zachary Keck, "Can China's New Strategic Bomber Reach Hawaii? (¿Puede el nuevo bombardero estratégico chino llegar a Hawaii?)" *Diplomat*, 13 de agosto de 2013, http://thediplomat.com/flashpoints-blog/2013/08/13/can-chinas-new-strategic-bomber-reach-hawaii/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+the-diplomat+%28The+Diplomat+RSS%29; Noam Eshel, "Chinese Air Force Gets More H-6K Strategic Bombers (Fuerza Aérea China recibe más bombarderos estratégicos H-6K)", *Defense Update*, 25 de junio de 2013, http://defense-update.com/20130625_h-6k-bombers-delivered-to-pla-air-force.html; y Chen Boyuan, "H-6K Bombers Delivered to PLA Air Force (Se han entregado bombarderos H-6K a la Fuerza Aérea del EPL)", *China.org,* 22 de junio de 2013, http://www.china.org.cn/china/2013-06/22/content_29197824.htm.

19. *Informe Anual al Congreso*, 33, 42, 81.

20. Ian Easton, *The Assassin under the Radar: China's DH-10 Cruise Missile Program (El asesino bajo el radar: El progrma de misiles crucero DH-10 de China)* (Arlington, VA: Project 2049 Institute, octubre de 2009), 1–6, http://project2049.net/documents/assassin_under_radar_china_cruise_missile.pdf.

21. Keck, "Can China's New Strategic Bomber Reach Hawaii? (¿Puede el nuevo bombardero estratégico chino llegar a Hawaii?)"

22. Andrea Shalal-Esa, "RPT-China's Space Activities Raising U.S. Satellite Security Concerns (Informe: Actividades espaciales de China suscita inquietud sobre seguridad de satélites estadounidenses)", Reuters, 14 de enero de 2013, http://www.reuters.com/article/2013/01/14/china-usa-satellites-idUSL2N0AJ10620130114; "Beijing to Trigger Arms Race by Testing Anti-Satellite Missiles (Beijing provocará carrera armamentista con prueba de misiles antisatélite)", Central News Agency (Taipei), 13 de enero de 2013, OSC ID: CPP20130115968204; Gregory Kulacki, "Is January Chinese ASAT Testing Month? (¿Es enero el mes de prueba de los ASAT chinos?)" *All Things Nuclear, Insights on Science and Security,* 4 de enero de 2013. http://allthingsnuclear.org/is-january-chinese-asat-testing-month/; *China: Informe de actividades del EPL 16–31 de octubre de 2012* (Washington: DoD, 31 de octubre de 2012), OSC ID: CPP20121120440020; "China Dismisses Report on Planned Test Launch of Anti-Satellite Missile (China desestima informe sobre lanzamiento de prueba de misiles antisatélite planeado)", Xinhua, 25 de octubre de 2012, OSC ID: CPP20121025968325; y Bill Gertz, "China to Shoot at High Frontier (China disparará a la frontera elevada)", *Washington Free Beacon,* 16 de octubre de 2012, http://freebeacon.com/china-to-shoot-at-high-frontier/.

23. Gregory Kulacki, " 'Kuaizhou' Challenges U.S. Perceptions of Chinese Military Space Strategy (El 'Kuaizhou' reta las percepciones de EE.UU. sobre la estrategia espacial militar china)", *All Things Nuclear, Insights on Science and Security,* 27 de septiembre de 2013, http://allthingsnuclear.org/kuaizhou-challenges-u-s-perceptions-of-chinese-military-space-strategy/.

24. *Informe Anual al Congreso,* 35-36.

25. "'Beidou,' China's Pride (El 'Beidou', orgullo de China)", *Bingqi Zhishi (Ordnance Knowledge)*, 1 de agosto de 2012, OSC ID: CPP20121016680010.

26. "China Targeting Navigation System's Global Coverage by 2020 (China busca cobertura mundial del sistema de navegación para 2020)", Xinhua, 3 de marzo de 2012, http://news.xinhuanet.com/english/sci/2013-03/03/c_132204892.htm.

27. "Navy North Sea Fleet's New Smart Target Ship Emits Electromagnetic Jamming against Missiles (Nuevo barco de adquisición inteligente de objetivos de la Flota del Mar del Norte de la Marina emite interferencias electromagnéticas contra misiles)", *PLA Daily*, 4 de agosto de 2013, OSC ID: CHO2013080530196614; Yu Hu, "PLA Jinan MR Extends Military Use of the Beidou Satellite Navigation System (Región Militar Jinan del EPL amplía el uso militar del sistema de navegación por satélite Beidou)", *Jinan Qianwei Bao (Jinan Front News)*, 17 de enero de 2012, OSC ID: CPP20130222667020; y Sun Chao, Zhang Jun, y Wang Jun, "PLA Chengdu MR Sichuan Div Uses Satellite Navigation to Standardize Time (División Sichuan de la Región Militar Chengdu del EPL utiliza navegación por satélite para normalizar la hora)", *Chengdu Zhanqi Bao (Chengdu Battle Standard News)*, 3 de noviembre de 2011, OSC ID: CPP20130223667002.

28. Bill Gertz, "China Conducts another Mobile ICBM Test (China realiza otra prueba de ICBM móvil)", *Washington Free Beacon,* 14 de agosto de 2013, http://freebeacon.com/china-conducts-another-mobile-icbm-test/.

29. *Informe Anual al Congreso,* 30; y Bill Gertz, "Riding the Nuclear Rails (En el tren nuclear)", *Washington Free Beacon,* 25 de enero de 2013, http://freebeacon.com/riding-the-nuclear-rails/.

30. *Informe Anual al Congreso*, 36.

31. "Facts Figures: China's 2013 Draft Budget Report (Cifras reales: Informe de presupuesto preliminar de 2013 de China)", Xinhua, 5 de marzo de 2013, OSC ID: CPP20130305968101; "China Boosts Defense Spending as Military Modernizes Arsenal (China aumenta el gasto de defensa mientras los militares modernizan su arsenal)", Bloomberg, 5 de marzo de 2013, http://www.bloomberg.com/news/2013-03-05/china-boosts-defense-spending-as-military-modernizes-its-arsenal.html; Luo Zheng, "Investment in Our National Defense Expenditure Mutually Conforms with National Security and Development Interests—Interview with Sun Huangtian, Deputy Director of PLA General Logistics Department, on 2013 National Defense Budget (La inversión en nuestros gastos en defensa nacional se ajusta mutuamente a los intereses de seguridad y desarrollo nacional —Entrevista con Sun Huangtian Subdirector del Departamento de Logística General del EPL, sobre el Presupuesto de Defensa Nacional de 2013)", *PLA Daily*, 6 de marzo de 2013, OSC ID: CPP20130307088001; "China Boosts Defense Spending as Military Modernizes Arsenal (China aumenta el gasto de defensa mientras los militares modernizan su arsenal)", Bloomberg, 5 de marzo de 2013, http://www.bloomberg.com/news/2013-03-05/china-boosts-defense-spending-as-military-modernizes-its-arsenal.html.

32. Adam Liff y Andrew Erickson, "Demystifying China's Defence Spending: Less Mysterious in the Aggregate (Desmitificando el gasto de defensa de China: Menos misterioso colectivamente)", *China Quarterly,* 2013, http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=8874207.

33. Instituto de Estudios Estratégicos Internacionales, "China's Defence Spending: New Questions (Gasto en defensa de China: Nuevas interrogantes)", *Strategic Comments*, 2 de agosto de 2013, http://www.iiss.org/en/publications/strategic%20comments/sections/2013-a8b5/china–39-s-defence-spending–new-questions-e625.

34. *Informe Anual al Congreso*, 45.

35. Ibíd., 69-71. Estos contactos incluyen visitas de alto nivel, intercambios recurrentes, intercambios académicos, intercambios funcionales, y ejercicios conjuntos.

36. Shirley Kan, U.S.–*China Military Contacts: Issues for Congress (Contactos entre militares de Estados Unidos y China: Asuntos para el Congreso)* (Washington: CRS, 25 de julio de 2013).

37. Karen Parrish, "U.S.–China Military Ties Growing, Pacom Commander Says (Crecen las relaciones militares entre EE.UU. y China, dice el Comandante del Pacom)", US Armed Forces Press Service, 11 de julio de 2013, http://www.defense.gov/news/newsarticle.aspx?id=120440.

38. Michelle Tan, "Army Hosts China in First Joint Field Exercise (El Ejército comparte con China el primer ejercicio de campo conjunto)", *Army Times,* 12 de noviembre de 2013, http://www.armytimes.com/article/20131112/NEWS/311120006/Army-hosts-China-first-joint-field-exercise.

39. Caitlin Campbell y Craig Murray, *China Seeks a "New Type of Major-Country Relationship" with the United States* (China busca un "Nuevo tipo de relación entre países principales" con Estados Unidos) (Washington: Comisión de Revisión Económica y de Seguridad de EE.UU.–China, 25 de junio de 2013), http://origin.www.uscc.gov/sites/default/files/Research/China%20Seeks%20New%20Type%20of%20Major-Country%20Relationship%20with%20United%20States_Staff%20Research%20Backgrounder.pdf; Michael S. Chase, "China's Search for a 'New Type of Great Power Relationship' (Búsqueda de China de un 'Nuevo tipo de relación entre grandes potencias", *Jamestown Foundation China Brief* 12, no. 27 (7 de septiembre de 2012): 14, http://www.jamestown.org/uploads/media/cb_09_04.pdf.

40. Larry M. Wortzel, *The Dragon Extends its Reach: Chinese Military Power Goes Global* (El dragón amplía su alcance: Poderío militar chino adquiere nivel global) (Washington: Potomac Books, 2013) 17, 40–41, 134, 145–48.

41. Dan Mcwhorter, "APT1 Three Months Later—Significantly Impacted, Though Active & Rebuilding (APT1 tres meses después — Afectada de manera importante, aunque activa y en reconstrucción)", *M-unition*, 21 de mayo de 2013, https://www.mandiant.com/blog/apt1-months-significantly-impacted-active-rebuilding/; y Richard Bejtlich (oficial jefe de seguridad en Mandiant), entrevista telefónica con personal de la comisión, 21 de agosto de 2013.

42. *Directorio de Personalidades Militares de la RPC* (Washington: Agencia de Inteligencia de Defensa, marzo de 2013).

43. Ibíd.

44. William C. Hannas, James Mulvenon, y Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization (Espionaje industrial chino: Adquisición de tecnología y modernización militar)*, (London and New York: Routledge, 2013), 226.

45. "2013 Nian 2 Yue 19 Ri Waijiaobu Fayanren Honglei Zhuchi Lixing Jizhehui (El vocero del Ministerio de Relaciones Exteriores Hong Lei Preside en conferencias de prensa regulares, 19 de febrero de 2013)," Ministerio de Relaciones Exteriores, Beijing, http://www.fmprc.gov.cn/mfa_chn/fyrbt_602243/t1014798.shtml.

46. Comisión de Revisión Económica y de Seguridad EE.UU.–China, *Informe Anual al Congreso de 2012* (Washington: Government Printing Office, noviembre de 2012), 166.

47. Una honeypot es parte de una honeynet, que es una red de computadoras falsa o de despiste, diseñada para atraer a un adversario para identificarlo o darle información falsa. Las honeynet pueden proporcionar inteligencia relativa a "herramientas, tácticas y motivos" del adversario. Proyecto Honeynet, "Short Video Explaining Honeypots (Vídeo corto que explica las honeypot)", http://old.honeynet.org/misc/files/HoneynetWeb.mov.

48. Tom Simonite, "Chinese Hacking Team Caught Taking over Decoy Water Plant (Equipo de piratería informática chino pillado apoderándose de planta de agua señuelo)", *MIT Technology Review*, 2 de agosto de 2013, http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/.

49. Wortzel, *Dragon Extends its Reach (El dragón amplía su alcance),* 142.

50. Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies (Informe confidencial lista diseños de sistemas de armas de Estados Unidos puestos en peligro por ciberespías chinos)", *Washington Post*, 27 de mayo de 2013, http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

51. Ibíd.

52. Ley de Autorización de Defensa Nacional para el Año Fiscal 2011 (L.P. 111-383), Congreso No. 111, segunda sesión, 7 de enero de 2011, http://www.gpo.gov/fdsys/pkg/PLAW-111publ383/pdf/PLAW-111publ383.pdf.

53. Asistente especial al oficial de información jefe del DoD, Oficina del Secretario Asistente de Defensa para Asuntos Legislativos, entrevista por correo electrónico con personal de la comisión, 28 de mayo de 2013.

54. Leigh Ann Ragland y otros, *Red Cloud Rising: Cloud Computing in China (Surge la nube roja: Computación en nube en China)* (Vienna, VA: Defense Group Inc. para la Comisión de Revisión Económica y de Seguridad de EE.UU.–China, septiembre de 2013), 32–34, http://origin.www.uscc.gov/sites/default/files/Research/Red%20Cloud%20Rising_Cloud%20Computing%20in%20China.pdf.

55. Ibíd., 39.

56. Ibíd., 38.

57. Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History' (Jefe de NSA: El cibercrimen constituye la 'Mayor transferencia de riqueza en la historia' ", *Foreign Policy*, 9 de julio de 2012, http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

58. Mike McConnell, Michael Chertoff, y William Lynn, "China's Cyber Thievery is a National Policy—And Must Be Challenged (El robo cibernético de China es una política nacional, y debe ser confrontado)," *Wall Street Journal*, 27 de enero de 2012, http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html.

59. Comisión sobre el Robo de Propiedad Intelectual, *The IP Commission Report* (Washington: National Bureau of Asian Research, mayo de 2013), 12, http://ipcommission.org/report/IP_Commission_Report_052213.pdf; y Comisión de Revisión Económica y de Seguridad de EE.UU.–China, *Informe Anual al Congreso de 2012,* 156.

60. A fines de la década de 1980 y comienzos de la de 1990 se realizó un debate en el Congreso sobre si la comunidad de inteligencia (IC) de Estados Unidos debía compartir información y/o activos de inteligencia con las empresas estadounidenses para proporcionarles una ventaja contra los competidores extranjeros. En 1991, el Director de la Agencia Central de Inteligencia Robert Gates, en un discurso a la IC, estableció claramente que la CIA se limitaría a ayudar a las empresas estadounidenses a salvaguardarse de las operaciones de inteligencia extranjeras. Robert Gates, "The Future of American Intelligence (El futuro de la inteligencia estadounidense)", discurso a la Comunidad de Inteligencia, Washington, DC, 4 de diciembre de 1991.

61. Comisión sobre el Robo de Propiedad Intelectual Estadounidenses, *IP Commission Report*, 3, 18.

62. *APT1: Exposing One of China's Cyber Espionage Units (APT1: Revelando una de las unidades de ciberespionaje de China)* (Alexandria, VA: Mandiant, febrero de 2013), 2, 3, 4, 9, 21–23, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

63. APT1, 9.

64. "Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets (Sinovel Corporation y tres individuos son acusados en Wisconsin de robar secretos comerciales de AMSC)", comunicado de prensa del Departamento de Justicia, 27 de junio de 2013, http://www.justice.gov/opa/pr/2013/June/13-crm-730.html.

65. Melanie Hart, "Criminal Charges Mark New Phase in Bellwether U.S.–China Intellectual Property Dispute (Acusaciones criminales marcan nueva fase en disputa clave sobre propiedad intelectual entre Estados Unidos y China)", Center for American Progress, Washington, DC, 27 de junio de 2013, http://www.americanprogress.org/issues/china/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/.

66. Ibíd.

67. 50 U.S.C. § 1701, http://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter35&edition=prelim.

68. *Sustaining U.S. Global Leadership: Priorities for 21st Century Leadership (Mantenimiento del liderazgo global de Estados Unidos: Prioridades para el liderazgo del siglo 21)* (Washington: DoD, enero de 2012), http://www.defense.gov/news/Defense_Strategic_Guidance.pdf.

69. Jonathan Greenert, "Foreword (Prólogo)", en U.S. *Navy Program Guide* 2013 *(Guía del Programa de la Marina de Estados Unidos para 2013)* (Washington: DoD, 2013), http://www.navy.mil/navydata/policy/seapower/npg13/top-npg13.pdf.

70. *U.S. Navy Program Guide 2013 (Guía del Programa de la Marina de Estados Unidos para 2013).*

71. "Statement on Strategic Choices and Management Review, Pentagon press briefing remarks by Secretary of Defense Chuck Hagel (Declaración sobre opciones estratégicas y revisión administrativa, comentarios de prensa del Pentágono por el Secretario de Defensa Chuck Hagel)," Washington, DC, 31 de julio de 2013, http://www.defense.gov/speeches/speech.aspx?speechid=1978.

72. Comité de la Cámara de Representantes sobre los Servicios Armados, *Audiencia sobre la Planificación de los Recortes Automáticos en el año Fiscal 2014 y Perspectivas de los Servicios Militares sobre las Opciones Estratégicas y Revisión Administrativa,* Congreso Nº. 113, primera sesión, 18 de septiembre de 2013.

El Dr. Larry M. Wortzel, PhD, fue nombrado miembro de la Comisión de Revisión Económica y de Seguridad de EE.UU.-China en 2001 y sirvió dos períodos como presidente de la Comisión. Es un coronel retirado del Ejército de los Estados Unidos que pasó gran parte de su carrera militar de 32 años en la región Asia-Pacífico. El Coronel Wortzel fue agregado asistente del Ejército en China desde 1988 hasta 1990 y agregado del Ejército en China entre 1995 y 1997. Es autor de *The Dragon Extends its Reach: Chinese Military Power Goes Global (El dragón amplía su alcance: Poderío militar chino adquiere nivel global)* (Potomac Books, Inc., 2013). Un graduado del Armed Forces Staff College y del U.S. Army War College, Wortzel obtuvo su maestría y Ph.D. en ciencias políticas en la Universidad de Hawaii.