

El Dragón y la Computadora

Por qué el Robo de la Propiedad Intelectual es Compatible con la Doctrina China de la Guerra Cibernética

PAULO SHAKARIAN

JANA SHAKARIAN

ANDREW RUEF

Un fragmento del próximo libro *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Introducción a la guerra cibernética: Un enfoque multidisciplinario), publicado por Syngress (ISBN: 978-0124078147), disponible a inicios de junio del 2013. Una versión completa del capítulo se puede comprar en línea en <http://store.elsevier.com/> a inicios de mayo del 2013.

DURANTE LOS últimos cinco años, los medios de comunicación parecen haber estado cubiertos de presuntos incidentes cibernéticos chinos. Estas actividades han incluido casos de robo de datos científicos protegidos,¹ monitoreo de las comunicaciones del Dalai Lama² y el robo de propiedad intelectual de *Google*.³ En un testimonio ante el Comité de Servicios Armados del Congreso, el General Keith Alexander, comandante del Comando Cibernético de Estados Unidos y jefe de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), declaró que China le está robando a Estados Unidos una “gran cantidad” de propiedad intelectual relacionada con la milicia.⁴ Evidentemente, el espionaje cibernético, que incluye el robo de propiedad intelectual, ya es un componente clave de la estrategia cibernética china. El informe recién publicado de la empresa de seguridad *Mandiant* ofrece un análisis técnico que nos lleva a la conclusión de que una organización dentro del Ejército Popular de Liberación de China (Unidad 61398) ha sido responsable de una gran cantidad de espionaje cibernético contra países de habla inglesa.⁵ En este artículo, destacamos algo de la doctrina china relevante que creemos condujo a la creación de organizaciones tales como la Unidad 61398 y otras.

Las actividades de extracción, monitoreo y robo de información digital descritas aquí se pueden catalogar fácilmente como incidentes de espionaje cibernético. La meta aparente de este tipo de operación cibernética no es ni desconectar las computadoras ni destruir los datos que contienen sino capturar los datos de la fuerza opositora. Siendo este el caso, dichas actividades no pueden catalogarse como ataques cibernéticos porque los sistemas que se atacan y sus datos tienen que permanecer intactos para poder obtener los datos deseados. Por ende, podemos definir el espionaje cibernético como el acto de obtener acceso a datos de un sistema de computadoras sin la autorización del dueño de ese sistema para fines de recopilación de inteligencia.

Sin embargo, al igual que los incidentes de ataque a las redes de computadoras, estos incidentes de espionaje cibernético también son claramente difíciles de atribuir. Entonces, ¿qué nos conduce a creer la participación de los chinos en los incidentes de espionaje cibernético? Si la atribución es tan difícil, ¿entonces por qué estas acciones provocan que corporaciones como *Google* y *Northrop Grumman*, al igual que diplomáticos de alto nivel como la Secretaria de Estado Hilary Clinton, hagan declaraciones severas contra el gobierno chino a raíz de esos ataques? El problema radica en el origen de los incidentes.⁶ A menudo las computadoras involucradas con el robo de información digital se rastrean a redes que están ubicadas en China continental. Además, el análisis forense del *malware* de esos incidentes a menudo indica el uso de herramientas

para crear *software* en el idioma chino. Aunque es prácticamente imposible implicar al gobierno de la República Popular China (RPC) en estas acciones de espionaje cibernético, el hecho de que consistentemente se pueden rastrear a China continental plantea graves preguntas de política. ¿Está el gobierno chino llevando a cabo investigaciones activas contra los *hackers* (piratas cibernéticos), y qué acciones legales están tomando una vez que se identifican estos *hackers*? ¿Está el gobierno chino compartiendo claramente la información de estas supuestas investigaciones con las víctimas del espionaje cibernético? ¿Qué medidas legales está tomando Beijing para evitar que los *hackers* individuales ataque organizaciones fuera de China? Estas preguntas deben ser consideradas seriamente a raíz de los intentos de espionaje cibernético y cuando hay pruebas de orígenes chinos.

¿Qué ganaría China al ofrecer un entorno tolerante para los *hackers*? Es poco probable que el gobierno chino—que se distingue por el monitoreo de estado⁷—no tuviese los recursos para disminuir esa actividad. Además, se puede esperar que la reprobación generada por la comunidad internacional sea indeseable diplomáticamente. Estas actividades le proveen a la RPC beneficios importantes. La naturaleza de la información robada—que va desde detalles sobre armamento norteamericano y secretos comerciales hasta las comunicaciones del Dalai Lama—son todas de un interés particularmente elevado para Beijing. Además, a fines de la década de los noventa e inicios de la del dos mil varios pensadores militares chinos escribieron acerca del tema de la guerra cibernética.⁸ Esos escritos indican que obtener un acceso no autorizado a los sistemas de computadoras con el propósito de extraer información es parte fundamental de la estrategia cibernética china.

Para poder comprender la doctrina china, debemos tomar en cuenta cómo las tradiciones y la cultura de esa nación han moldeado su razonamiento militar en maneras muy diferentes a las de Occidente. En un artículo *SANS*⁹, el Cnel Edward Sobiesk destaca un ejemplo que ilustra las diferencias amplias entre la forma de pensar Occidental y la china que se destacan en un Informe al Congreso en el 2002 titulado *The Military Power of the PRC* (El poder militar de la RPC) por el Secretario de Defensa de EE.UU.¹⁰ En este informe se identifica que uno de los objetivos estratégicos de China es cómo maximizar la “configuración estratégica de poder” conocida como “shi”. En el informe, un pie de página para ‘shi’, reza como sigue: “No hay un equivalente occidental para el concepto ‘shi’. Los lingüistas chinos lo explican como ‘la alineación de las fuerzas’, la ‘inclinación de las cosas’ o ‘potencial que nace de la disposición’ de lo que solamente un estratega experto se puede aprovechar para garantizar la victoria sobre una fuerza superior”. Otra interpretación del “shi” se podría enfocar en establecer condiciones favorables. Si una nación estado logra alcanzar un nivel de “shi” más elevado que un rival, este último será derrotado fácilmente cuando el conflicto surja, porque cualquier batalla (inclusive de ser necesaria) se llevará a cabo en condiciones sumamente favorables para la primera nación—ya que ésta ha establecido las condiciones favorables mediante el logro del “shi”. Al lograr un nivel de acceso elevado a los sistemas de computadoras activos de un adversario—la información almacenada en esos sistemas ha perdido dos aspectos críticos—confidencialidad e integridad.¹¹ La *confidencialidad* garantiza que ningún individuo no autorizado pueda ver la información mientras que la *integridad* garantiza que la información, una vez extraída, no sea alterada. Eliminar estos aspectos de la información de un adversario puede contribuir en gran medida a establecer las condiciones en el campo de batalla—quizás inclusive evitar la batalla del todo. En vista de que el espionaje cibernético “shi” parece ser una herramienta estratégica formidable—al lograr acceso a los sistemas de computadora del opositor, la ventaja de la información del rival es disminuida a la vez que se logra lo mismo en el lado que la inicia.

De defensa activa a ofensiva activa

Tradicionalmente, el Ejército Popular de Liberación (EPL) estaba enfocado en la idea china tradicional de “defensa activa” que se refiere a la idea de no iniciar un conflicto pero estar preparado para responder a una agresión.¹² En un artículo del 2008 en la revista *Military Review*, Timothy Thomas destaca que a fines de la década de los noventa e inicios de la del 2000 se produjo un cambio de esta mentalidad, particularmente con respecto a la guerra cibernética. Este paradigma que parecía surgir en ese entonces era una “ofensiva activa”. Bajo esta rúbrica nueva, la idea de establecer las condiciones del campo de batalla (o sea, desarrollar el “shi”) es aún preeminente pero la manera en que se trata de lograr dio un giro diferente. En el campo de la cibernética esto incluye no solamente fortalecer las defensas de uno para disuadir el ataque, sino utilizar las operaciones cibernéticas para obtener el control en caso de un conflicto mayor.

Esta idea de “ofensiva activa” se introdujo en 1999 en el libro titulado *Information War* (Guerra informática) por Zhu Wenguan y Chen Taiyi. En este libro, ellos incluyen una sección titulada “*Conducting Camouflaged Attacks*” (Llevando a cabo ataques camuflajeados) en los que la anticipación y la ofensiva activa se plantean.¹³ Un componente clave de la ofensiva activa es la vigilancia de la red que incluye obtener un entendimiento del mando y control (C2, por sus siglas en inglés), guerra electrónica (EW, por sus siglas en inglés) y sistemas de armamento importantes del opositor. En el 2002 y el 2003, el General Dai Qingmin repitió algunas de esas ideas.¹⁴ Él recalcó que es necesario que la información y las operaciones cibernéticas sean “precursoras” (o sea, que se lleven a cabo antes que sucedan las operaciones) y “a largo plazo” (que se lleven a cabo durante la operación). ¿Dónde encaja el espionaje cibernético en este esquema? Por ejemplo, los *hackers* rusos se aprovecharon de los ataques cibernéticos de negación de servicios en las fases iniciales de la campaña de Georgia para obstaculizar el gobierno, la banca y los sitios web de los medios de comunicación de la fuerza opositora. O sea, la anticipación también puede adoptar otras formas más sutiles. Por ejemplo, tener acceso constante a los sistemas de informática tibetanos verdaderamente sería una ventaja y probablemente resultaría en la posibilidad de evitar completamente un conflicto abierto. El robo de secretos militares relacionados con sistemas de armamento nuevos le podría dar a los chinos la inteligencia técnica (TECHINT, por sus siglas en inglés) necesaria para encontrar vulnerabilidades o inclusive diseñar sus propias copias de dicho armamento. Robar propiedad intelectual de los vendedores de *software* le podría dar a los *hackers* chinos un caudal de conocimientos necesarios para identificar vulnerabilidades nuevas para futuros ataques cibernéticos y operaciones de espionaje cibernético.

La obra *Information War* y los escritos del General Dai ilustran la importancia del aspecto cibernético a las operaciones militares chinas. No obstante, muchos de los incidentes de espionaje cibernético que trataremos en este artículo tienen que ver con el robo de información de empresas privadas durante tiempos de paz. ¿Cómo se explica esto en la literatura china sobre la guerra cibernética? Las respuestas a preguntas de este tipo parecen radicar en el libro de 1999 titulado *Unrestricted Warfare* (Guerra irrestringida) por los Coroneles Qiao Liang y Wang Xiangsui del EPL.¹⁵ En esta obra, los autores afirman que la guerra moderna se extiende más allá de un simple ámbito militar. La guerra moderna incluye líderes políticos, científicos y económicos además del personal militar. La noción de una guerra “irrestringida” extiende no solo los ámbitos de la guerra sino también el tiempo en que esas acciones de guerra pueden ocurrir. Las operaciones “militares”—que ahora incluyen aspectos de información, económicos y psicológicos, pueden tener lugar durante tiempos de paz en esta perspectiva—apoyando aún más la noción de “ofensiva activa”. Esto puede que ayude a explicar por qué el inicio del siglo XXI ha estado cubierto con relatos de espionaje cibernético chino contra corporaciones y laboratorios científicos.

En ese mismo orden de ideas, el Coronel Wang Wei y el Mayor Yang Zhen del Departamento de Guerra y Comando de Informática de la Academia Militar Nanjing escribieron en *China Military Science* que en una guerra contra una sociedad centrada en la informática, el sistema político,

el potencial económico y los objetivos estratégicos de una nación serán blancos de gran valor.¹⁶ Luego pasan a describir que el método preferido para atacar dicha sociedad sería a través del uso de técnicas de guerra asimétrica. Guerra asimétrica se refiere a la capacidad de un combatiente de derrotar una fuerza superior empleando tácticas que le sacan provecho a las debilidades más importantes en sus sistemas de armamento, tácticas o tecnología de informática. Durante la guerra de Estados Unidos en Iraq del 2003 al 2011, los insurgentes a menudo empleaban ataques asimétricos tales como bombas en las carreteras a diferencia de ataques más tradicionales que de lo contrario los hubiesen expuesto a la potencia de fuego superior de los estadounidenses. El Coronel Wei y el Mayor Zhen apoyan los ataques asimétricos en un nivel más estratégico—específicamente haciendo un llamado a operaciones en tiempo de paz que tienen metas militares y económicas. Para lograr esas metas, bajo “condiciones informatizadas” ellos alegan que se debe llevar a cabo una guerra económica y comercial.¹⁷ Evidentemente, estos autores fueron influenciados por sus ideas anteriores de *Unrestricted Warfare*. Parece que las operaciones de espionaje cibernético en tiempo de paz lanzados desde China continental contra blancos científicos, militares y comerciales son compatibles con esta línea de razonamiento.

Otra línea de razonamiento en los escritos chinos para justificar sus aparentes acciones audaces en el ciberespacio es que ellos creen que esas actividades se pueden llevar a cabo con relativa impunidad. En un artículo del 2009 en *China Military Science*, el Coronel Superior Long Fangcheng y el Coronel Superior Li Decai expresan que las operaciones cibernéticas dirigidas contra blancos sociales, económicos y políticos se pueden llevar a cabo sin temor a que esas actividades conduzcan a enfrentamientos militares a gran escala.¹⁸ En ese caso, ellos por lo general consideran la guerra cibernética como un elemento de poder de persuasión—no obstante con grandes efectos. Luego pasan a alegar que el efecto final de esta forma de poder de persuasión sumamente eficaz es que la línea entre tiempo de paz y tiempo de guerra se vuelve borrosa. Esta confusión puede que sea un sello de las operaciones cibernéticas en general y podría conducir a la guerra metafórica sin final en el futuro cercano.

INEW y la cibernética en el EPL

La estrategia general de guerra de información (IW, por sus siglas en inglés) que el EPL emplea se conoce como Guerra electrónica integrada en la red (INEW, por sus siglas en inglés).¹⁹ Esta estrategia originalmente se esbozó en un libro escrito en 1999 por el General Dai Qingmin titulado *On Information Warfare* (Sobre la guerra informática). Esta integración de las operaciones cibernéticas a los recursos tradicionales de la guerra de la informática es un elemento clave de la estrategia INEW. La INEW depende de la aplicación simultánea de la guerra electrónica y de las operaciones cibernéticas para abrumar el mando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento (C4ISR, por sus siglas en inglés) del adversario. Por ende, la misión de las piezas clave de la guerra cibernética (ataque cibernético, espionaje cibernético y defensa cibernética) son elementos asignados del Estado Mayor del EPL a los cuales tradicionalmente se le otorgan roles similares en la guerra electrónica.

El Estado Mayor del EPL está dividido en varios departamentos. INEW por lo regular asigna tareas ofensivas (ataque cibernético y contramedidas electrónicas [ECM, por sus siglas en inglés] más convencionales) al 4º Departamento—que tradicionalmente ha desempeñado un papel más importante en la guerra de informática ofensiva.²⁰ Cabe destacar que el General Dai Qingmin fue ascendido a jefe del 4º Departamento en el 2000—quizás un indicio de que el EPL tenía intenciones de adoptar su visión de INEW. Las tareas de defensiva e inteligencia—específicamente defensa cibernética y espionaje cibernético—están asignadas al 3º Departamento—que tradicionalmente se enfocaba en la inteligencia de señales (SIGINT, por sus siglas en inglés).²¹ Se piensa que el 3º Departamento es la sede de las Agencias de Reconocimiento Técnico cuya misión normal es la recopilación de SIGINT. A fines de la década de los años noventa, varias de estas

agencias recibieron reconocimientos relacionados con investigaciones en la guerra informática.²² Algunos analistas creen que esto es señal del papel que desempeñan en las operaciones cibernéticas.²³

Para fortalecer a los especialistas de guerra informática en el 3^{er} y el 4^o GSD, los chinos también han establecido unidades de milicia de guerra informática.²⁴ Esas milicias pueden considerarse como una “guardia nacional cibernética” ya que constan en su mayoría de personal de la tecnología de informática comercial (IT, por sus siglas en inglés) y de entornos académicos. Informes de fuentes abiertas indican que estas unidades fueron creadas desde el 2003 al 2008 en las provincias de Guangzhou, Tianjin, Henan y Ningxia.²⁵ Inclusive hay pruebas de que algunas de esas milicias recibieron tareas en tiempo de guerra específicas—la mayoría de las cuales parecen estar enfocadas en el ataque cibernético.²⁶

Las ideas principales de las operaciones cibernéticas chinas surgieron de los escritos de oficiales del ELP a fines de la década de los noventa y finalmente implementadas en la estrategia INEW que coinciden con las responsabilidades de ataque cibernético y de espionaje cibernético con organizaciones que llevan a cabo operaciones similares en el ámbito de la guerra electrónica.²⁷ Aunque la comunidad de *hackers* chinos saltó a la fama a fines de los años noventa e inicios del 2000 con ataques que aparentemente tenían metas congruentes con el gobierno, el ELP en un final desaprobó esas acciones.²⁸ Como resultado, muchos de los “*hackers*” se han convertido en “sombbrero blanco” ya sea transformando sus grupos de *hackers* en empresas asesoras u obteniendo empleo con el gobierno o el ámbito académico.²⁹ El ámbito académico chino también parece estar sumamente involucrado con la guerra cibernética—no tan solo en las investigaciones sino también posiblemente con las operaciones.³⁰

Estudio de un caso práctico sobre la guerra cibernética mediante el robo de propiedad intelectual: Operación Aurora

El 20 de enero de 2010, *Google* anunció una noticia impactante. La empresa publicó en su *blog* oficial que había sido víctima de una guerra cibernética originando de China. Según el *blog*, la finalidad de la operación fue lograr acceso a las cuentas de correo electrónico *Gmail* de los activistas chinos de derechos humanos.³¹ Como resultado de esta operación de espionaje cibernético, *Google* anunció que ya no censuraría los resultados en su buscador principal en China—*google.cn*—una medida que causó consternación con la RPC. La empresa expresó que si no podía funcionar su buscador sin censura, estaría dispuesta a cerrar operaciones en China.

Literalmente minutos después del anuncio de *Google*, *Adobe*—otro vendedor importante de *software*—anunció que sus sistemas corporativos también habían sido víctimas de los *hackers*.³² Resulta que tanto *Google* como *Adobe* fueron blancos del mismo adversario—un adversario que llevó a cabo la misma operación contra 32 otras empresas. Entre ellas se encontraban *Dow Chemical*, *Northrop Grumman*, *Symantec* y *Yahoo*.³³ Parece que el propósito de la operación era extraer no tan solo información acerca de los activistas chinos de derechos humanos, sino también de la propiedad intelectual—principalmente el código fuente de *software* diseñado comercialmente.³⁴

Esta operación—conocida como “Operación Aurora”—es el tema de esta sección. Se aprovechó de las ingenierías sociales junto con un virus *Trojan* conocido como *Hydraq* para robar propiedad intelectual. Varios analistas tienen la firme sospecha de la participación de la RPC. En esta sección analizamos el ataque y las pruebas de la participación de la RPC y discutimos las consecuencias del robo de propiedad intelectual de las corporaciones.

Este acto de espionaje cibernético empleó una vulnerabilidad en *Microsoft Internet Explorer* que fue explotada por un *software* conocido designado como *Trojan.Hydraq* por la empresa de seguridad, *Symantec*. Al igual que con varias de las operaciones de espionaje cibernético discutidas en este artículo, la Operación Aurora fue iniciada con *spear phishing* (ataques a una organización determinada). En el caso del robo en *Google*, se cree que ese *spear phishing* inicial fue dirigido a

un empleado que utilizaba el *software* de *chat* instantáneo, *Microsoft Messenger*. Supuestamente el usuario recibió un enlace a un sitio web malicioso durante uno de sus *chats*.³⁵ Se desconoce si las operaciones contra las otras empresas también fueron iniciadas con *software* de *chat*. Con base en operaciones similares parece posible que el correo electrónico puede que se halla usado como una manera para iniciar la infiltración del *software* malicioso. En cualquier caso, la comunicación inicial a estas empresas tenía tres características. Primero, fueron enviadas a un grupo selecto de individuos, lo que sugiere que este tipo de ataque (*spear phishing*) indica que los *hackers* contaban con alguna fuente de inteligencia adicional con respecto a sus blancos. Segundo, las comunicaciones fueron diseñadas de manera que parecían haber originado de una fuente confiable, lo que también muestra que los infractores estaban operando con perfiles de sus blancos. Tercero, todos contenían un enlace a un sitio web—al hacer clic iniciaba una serie de eventos.

Una vez que el usuario hacía clic en el enlace, el buscador visitaba un sitio en Taiwán. Este sitio web, a su vez, ejecutaba un código *JavaScript* malicioso—este es el código fuente que opera en un sitio web que generalmente se utiliza para proveerle al usuario características interactivas. El código *JavaScript* malicioso se aprovechó de una debilidad en el buscador *Microsoft Internet Explorer* que en aquel entonces se desconocía. A menudo una vulnerabilidad nueva de esa índole se le llama una “intrusión de día cero”. El malévolo código *JavaScript* procede a descargar un segundo pedazo de *malware* de Taiwán—disfrazado de un archivo de imagen. Este segundo *software* malicioso pasaría a funcionar en *Windows* y establecería una puerta trasera permitiéndole al espía cibernético acceso al sistema que se va a atacar.³⁶ Una puerta trasera se refiere a un método de lograr acceso a un sistema que le permite al intruso a circunvalar el mecanismo de seguridad normal. El uso de una intrusión de día cero es importante porque identificar una vulnerabilidad de ese tipo probablemente requeriría un esfuerzo de ingeniería hábil. Esto, junto con la campaña de *spear phishing* sumamente precisa (sugiriendo que los *hackers* tenían acceso a información de inteligencia adicional sobre sus blancos), podría dar a entender el apoyo de una organización más grande—quizás una nación estado.

Robo de propiedad intelectual

Varios meses después que *Google* anunció que había sido atacada, el *New York Times* informó que se habían comprometido mucho más que tan solo cuentas de correo electrónico de activistas chinos de derechos humanos. Nombrando una fuente no identificada con conocimiento directo sobre la investigación de *Google*, el periodista John Markoff escribió que el código fuente al sistema moderno de contraseñas de *Google* probablemente había sido robado durante la Operación Aurora.³⁷ El sistema, conocido como *Gaia*, fue concebido para permitirles a los usuarios del *software* de *Google* utilizar un solo nombre de usuario y contraseña para tener acceso a una variedad de servicios de *Google*. Este *software* también se conoce como “*Single Sign-On*”. Markoff informó que *Google* enfrentó el problema añadiendo una capa adicional de codificación a su sistema de contraseña.

La puesta en peligro de *Gaia* es importante por más de un motivo. Primero, obtener el código fuente del *software* de un sistema comercial es robo de la propiedad intelectual y por ende ilegal en Estados Unidos. Al igual que con los datos robados durante *Titan Rain*, el código fuente le permitiría a ciertos diseñadores crear *software* ilícito similar a *Gaia*. Si consideramos la Operación Aurora como las acciones de una nación estado, se podría pensar que el robo de propiedad intelectual es una forma de guerra económica—nivelar el campo de juego tecnológico para reducir la ventaja de la capacidad industrial de una nación adversaria. Evidentemente, esto está en línea con las ideas chinas de *Unrestricted Warfare*—donde varias formas de guerra informática ocurren constantemente (inclusive durante tiempos de paz) y atacan todos los aspectos del poder de una nación (incluyendo la industria).

Sin embargo, más allá de las ventajas económicas obtenidas por el robo de códigos fuentes, implicaciones importantes de seguridad también son inminentes—en particular en el caso de *Gaia*. Por ejemplo, los analistas que trabajan con los *hackers* probablemente determinarían las vulnerabilidades técnicas en el sistema de contraseñas.

Si bien está claro que el robo de propiedad intelectual es una consideración importante para las corporaciones, también plantea una pregunta importante. ¿Cómo pudieron los *hackers* obtener el código fuente para un sistema como *Gaia* al hacer uso de una cifra relativamente pequeña de sistemas de computadoras comprometidos? Resulta que muchas corporaciones trabajan con servidores especializados como almacenes para este tipo de datos—a menudo correctamente referidos como “depósitos de propiedad intelectual”. Las ubicaciones centralizadas de este tipo de datos facilitan que los equipos trabajen en colaboración en un proyecto y compartan información entre ellos. Estos sistemas a menudo toman la forma de sistemas de Gestión de Configuración de *Software* (SCM, por sus siglas en inglés) tales como *IBM Rationale*[®] o sistemas de gestión de contenido tales como *Microsoft SharePoint*[®].

La Operación Aurora invalidó una suposición importante hecha por muchos administradores de sistemas y vendedores de almacenes IP de *software* en ese momento. Los profesionales que operan esas redes dan por sentado que no habría acceso a la propiedad intelectual a causa de las contramedidas de seguridad adoptadas para proteger a la red en general. El resultado de esta perspectiva y menos enfoque en la seguridad de un depósito IP que se encuentra dentro del perímetro de la red de una corporación. Al utilizar una vulnerabilidad de día cero para su misión, los infractores detrás de la Operación Aurora pudieron aprovecharse de esa suposición.

El robo de la propiedad intelectual presenta otra dificultad importante—determinar qué se robó en realidad. A raíz de la Operación Aurora, el investigador de seguridad, George Kurtz, escribió un artículo titulado “*Where’s the body?*” (¿Dónde está el cadáver?).³⁸ A diferencia de un robo físico donde es relativamente fácil definir qué fue lo que se robó, con el espionaje cibernético y la extracción de datos eso es mucho más difícil de establecer. Aunque los administradores de sistemas tienen a la mano unas cuantas herramientas—tales como el análisis de registros de servidores y del tráfico en la red—en las operaciones avanzadas de espionaje cibernético los *hackers* a menudo toman varias medidas para encubrir sus pasos y operar en una manera que dificulta determinar cuáles datos fueron robados. Aunque los vendedores de seguridad proveen soluciones de *software* para ayudar con este problema, determinar “¿dónde está el cadáver?” a raíz de una operación de espionaje cibernético aún es una tarea difícil.

Indicadores de la participación de la RPC

Resulta interesante que el anuncio de *Google* sobre la violación de seguridad parece implicar la participación de los chinos—o al menos sugiere descuido por parte del gobierno. A continuación se ofrecen algunos indicadores que la Operación Aurora fue ejecutada con el pleno conocimiento o inclusive bajo la dirección del gobierno chino.

Las primeras señales de la participación china se publicaron en enero de 2010—varias semanas después del mensaje de *blog* de *Google*. Un informe publicado por la empresa de seguridad *VeriSign* alegaba que los “IP fuentes” y el servidor de descarga (*drop server*) repositorio del ataque corresponden a una sola entidad extranjera que consta o bien de agentes del estado chino o *proxys* del mismo”.³⁹ Los investigadores en *VeriSign* también descubrieron que los *hackers* Aurora utilizaron *HomeLinux DynamicDNS* y tomaron prestadas direcciones IP de la empresa norteamericana *Linode* (una compañía que se especializa en el alojamiento de servidores privados virtuales). Estas son las mismas circunstancias de los ataques DDoS en julio de 2009 contra Corea del Sur y Washington, D.C. Cuando se consideraron con otras circunstancias similares, los investigadores de *VeriSign* concluyeron que Aurora y los ataques contra Washington, D.C., y Corea del Sur posiblemente los llevó a cabo la misma entidad.

Pocas semanas después, periodistas del *New York Times*. John Markoff y David Barboza, publicaron un artículo que alegaba que los investigadores habían identificado que dos escuelas chinas de estudios superiores habían participado en el ataque—*Shanghai Jiaotong University* y *Lanxiang Vocational School*.⁴⁰ El *Security Engineering Institute* de ésta es el lugar de trabajo de Peng Yinan (supuestamente el hacker chino “CoolSwallow”). Cuando los periodistas del *New York Times* llevaron a cabo una entrevista telefónica anónima con un profesor de ese instituto, se sorprendieron con la respuesta cándida. Él declaró que el *hacking* de las redes de computadoras extranjeras por parte de los estudiantes era “bastante normal”.⁴¹ Sin embargo, como una explicación alternativa, el profesor declaró que la dirección IP de la Universidad también pudo haber sido pirateada y según él eso “sucedió a menudo”.⁴² En la *Lanxiang Vocational School*, los investigadores pudieron identificar una clase específica dictada por un profesor ucraniano quien se sospechaba estaba involucrado en la Operación Aurora.⁴³ Cuando se le confrontó con la sospecha, el decano del departamento de ciencias computacionales ahí (identificado por los medios de comunicación solamente como el Sr. Shao) expresó que los estudiantes en la escuela sencillamente no tendrían la capacidad de llevar a cabo un ataque de ese tipo. No obstante, sí admitió que los estudiantes de la escuela a menudo eran reclutados en la milicia.⁴⁴

Los informes sobre la participación china pudieron haber inspirado el discurso de la Secretaria de Estado estadounidense, Hillary Clinton, sobre libertad en la *Internet* pronunciado poco después del anuncio de *Google*.⁴⁵ En este discurso ella hizo un llamado a China para que llevara a cabo una investigación transparente sobre las violaciones de *Google*. Este fue quizás la declaración más contundente hecha por un funcionario de alto rango del gobierno estadounidense planteado en respuesta al incidente de guerra cibernética en ese momento.

La Operación Aurora ilustra la evolución continua del espionaje cibernético a inicios del siglo XXI. En este caso de espionaje cibernético, la información específica fue considerada tan importante que los operadores utilizaron una explotación de día cero y *spear phishing* para lograr el acceso a los sistemas corporativos, localizar los depósitos de propiedad intelectual del blanco y robar secretos de la compañía. Reportada originalmente por *Google*, esta operación afectó a más de treinta empresas de renombre. La información robada probablemente solo fue para promover ganancias económicas, pero también es posiblemente beneficiosa para la inteligencia técnica, tales como la evaluación de vulnerabilidades—posiblemente para utilizarla en ataques cibernéticos adicionales. La Operación Aurora anuló las suposiciones existentes acerca de los depósitos de propiedad intelectual en las corporaciones y destacó una vez más la dificultad de determinar los pormenores de los datos capturados. Los informes de los medios de comunicación de la posible participación de China resultaron en una declaración diplomática por parte de la Secretaria de Estado de EE.UU. La Operación Aurora no es única. En su secuela, ha habido otras maniobras cibernéticas atribuidas a China con la meta de robar propiedad intelectual. Una serie de eventos conocidos como *Nitro*⁴⁶ (dirigidos en contra de la industria química) y *Night Dragon*⁴⁷ (contra el sector de energía) son tan solo dos ejemplos. Por último, hay muchos posibles efectos de segundo y tercer orden de un vendedor importante de *software* como *Google* o *Adobe* que ha sido pirateado. Se desconoce qué consecuencias tendría el posible conocimiento de *software* ampliamente usado, tal como el sistema de contraseña *Gaia* de *Google*, en las operaciones cibernéticas de seguimiento. Aunque en la actualidad no está conectado con Aurora, recientemente se reveló que el sistema de certificados de *software* de *Adobe* fue pirateado—permitiendo que *software* malicioso creara suplementos (*add-ons*) supuestamente seguros a muchos de los *software* de esa empresa.⁴⁸ En este caso, un servidor de desarrollo en *Adobe* fue asaltado. Es un ejemplo claro de cómo la seguridad cibernética de los propios sistemas de un vendedor de *software* importante puede tener un impacto directo en una población de usuarios sumamente grande—por ende ofreciéndole amplias oportunidades a un adversario que lleva a cabo ataques cibernéticos de seguimiento.

En este artículo hemos discutido varias ideas patrocinadas por pensadores militares de China sobre la guerra informática—destacando las ideas de *Unrestricted Warfare*—en las que se piensa que las operaciones cibernéticas se extienden a tiempos de paz e incluye ámbitos militares, políticos, económicos y científicos. Analizamos cómo los chinos estructuraron a sus guerreros cibernéticos en torno a la estrategia INEW. En el ELP, las operaciones cibernéticas se colocaron bajo la responsabilidad de organizaciones con misiones similares en el ámbito de la guerra electrónica. Por último, pudimos ver cómo esas ideas pueden haberse puesto en práctica con la Operación Aurora donde una explotación de día cero le permitió a los operadores robar propiedad intelectual de los depósitos en *Google*, *Adobe* y muchas otras compañías importantes a fines del 2009. □

Notas

1. Steve DeWeese, Bryan Krekel, George Bakos, Christopher Barnett, *Capability of the People's Republic of China to Conduct of Cyber Warfare and Computer Network Exploitation* (Capacidad de la República Popular China de llevar a cabo guerra cibernética y explotación de redes de computadoras), *Northrop Grumman*, octubre de 2009.

2. *Information Warfare Monitor, Tracking Gh0stNet: Investigating a Cyber Espionage Network* (Rastreado a Gh0stNet: Investigando una red de espionaje cibernético), marzo de 2009.

3. Kim Zetter, “Google Hackers Targeted Source Code of More Than 30 Companies” (*Hackers de Google atacaron los códigos fuente de más de 30 compañías*), *Wired Threat Level*, 13 de enero de 2010, consultado el 8 de enero de 2012. Disponible en: <http://www.wired.com/threatlevel/2010/01/google-hack-attack/>.

4. J. Nicholas Hoover. (2012, marzo, 27). *NSA Chief: China behind RSA Attacks* (Jefe de NSA: China detrás de ataques RSA). *InformationWeek*. Obtenido de: http://www.informationweek.com/news/government/security/232700341?cid=RSSfeed_IWK_All.

5. “APT1: Exposing One of China's Cyber Espionage Units” (APT1: Exponiendo una de las unidades de espionaje cibernético de China), *Mandiant*. Obtenido de: <http://intelreport.mandiant.com/>.

6. El origen no puede referirse solamente al IP fuente mencionado (rastreado a través de *proxies* intermedios) sino también el origen del *software* determinado por el análisis técnico del código (por ejemplo, el origen basado en la versión del compilador y el lenguaje del sistema operativo empleado para crear el *software* en cuestión).

7. “Chinese Internet Giants Agree to Help Government Monitor Information” (Gigantes de *Internet* chinos acuerdan ayudar al gobierno a monitorear información), *Voice of America News*, 5 de noviembre de 2011, <http://www.voanews.com/content/chinese-internet-giants-agree-to-help-government-monitor-information-133327903/168182.html> (consultado el 25 de marzo de 2013).

8. Timothy Thomas, “China's Electronic Long-Range Reconnaissance” (Reconocimiento electrónico a gran distancia de China), *Military Review*, Noviembre-Diciembre 2008, 47-54.

9. Edward Sobiesk, “Redefining the Role of Information Warfare in Chinese Strategy” (Definiendo nuevamente el papel que desempeña la guerra de informática en la estrategia china), *SANS Institute InfoSec Reading Room*, marzo de 2003, http://www.sans.org/reading_room/whitepapers/warfare/redefining-role-information-warfare-chinese-strategy_896 (consultado el 22 de diciembre de 2011).

10. Oficina del Secretario de Defensa de los Estados Unidos de Norteamérica, Informe al Congreso sobre el Poder Militar de la República Popular China, 12 de julio de 2002, 5-6.

11. W. V. Maconachy, Corey D. Schou, Daniel Ragsdale, Don Welch, “A Model for Information Assurance: An Integrated Approach” (Un modelo para garantía en la información: Un método integrado), *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security* (Ponencias del Taller IEEE 2001 sobre garantía y seguridad de la información), junio de 2001, <http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf> (consultado el 22 de diciembre de 2011).

12. Timothy Thomas, “China's Electronic Long-Range Reconnaissance”, *Military Review*, Noviembre-Diciembre de 2008, 47-54.

13. *Ibid.*

14. *Ibid.*

15. Sobiesk, 8.

16. Timothy Thomas, “Google Confronts China's Three Warfares” (*Google enfrenta las tres guerras de China*), *Parameters*, Verano 2010, 101-105.

17. Wang Wei and Yang Zhen, “Recent Development in the Study of the Thought of People's War under Informatized Conditions” (Desarrollos recientes en el estudio de la opinión de la guerra popular bajo condiciones de informática), *China Military Science*, 2ª edición 2009.

18. Long Fangcheng y Li Decai, “On the Relationship of Military Soft Power to Comprehensive National Power and State Soft Power” (Sobre la relación del poder de persuasión militar a poder nacional exhaustivo y poder de persuasión estatal), *China Military Science*, Issue 5, 2009, 120-29.

19. Steve DeWeese, Bryan Krekel, George Bakos, Christopher Barnett, *Capability of the People's Republic of China to Conduct of Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, octubre de 2009.
20. *Ibíd.*
21. *Ibíd.*
22. *Ibíd.*
23. *Ibíd.*
24. *Ibíd.*
25. *Ibíd.*
26. *Ibíd.*
27. *Ibíd.*
28. *Ibíd.*
29. *Ibíd.*
30. *Ibíd.*
31. David Drummond, "A new approach to China" (Un nuevo acercamiento a China), *The Official Google Blog*, 12 de enero de 2010. Consultado el 8 de enero de 2012. Disponible en: <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.
32. Pooja Prasad, "Adobe Investigates Corporate Network Security Issue" (Adobe investiga problema de seguridad de la red de la corporación), *Adobe Featured Blogs*, 12 de enero de 2010. Consultado el 8 de enero de 2012. Disponible en: http://blogs.adobe.com/conversations/2010/01/adobe_investigates_corporate_n.html.
33. Kelly Jackson Higgins, "More Victims Of Chinese Hacking Attacks Come Forward" (Se presentan más víctimas de ataques piratas chinos), *Dark Reading*, 14 de enero de 2010, consultado el 8 de enero de 2012. Disponible en: <http://www.darkreading.com/security/attacks-breaches/222301032/index.html>.
34. Kim Zetter, "Google Hackers Targeted Source Code of More Than 30 Companies", *Wired Threat Level*, 13 Jan. 2010, accessed 8 Jan. 2012. Available at: <http://www.wired.com/threatlevel/2010/01/google-hack-attack/>.
35. John Markoff, "Cyberattack on Google Said to Hit Password System" (Se dice que ataque cibernético a Google atacó sistema de contraseñas), *New York Times*, 19 de abril de 2010. Disponible en: <http://www.nytimes.com/2010/04/20/technology/20google.html>, accessed 15 Jan., 2012.
36. McAfee Labs y McAfee Foundation Professional Service, "Protecting Your Critical Assets: Lessons Learned from Operation Aurora" (Protegiendo sus recursos críticos: Lecciones aprendidas de la Operación Aurora), *McAfee White Paper*, 2010.
37. John Markoff, "Cyberattack on Google Said to Hit Password System", *New York Times*, 19 de abril de 2010. Disponible en: <http://www.nytimes.com/2010/04/20/technology/20google.html>, consultado el 15 de enero de 2012.
38. George Kurtz, "Where's the body" (¿Dónde está el cadáver?), *McAfee Blog Central*, 25 de enero de 2010. Disponible en: <http://siblog.mcafee.com/cto/where%E2%80%99s-the-body/>, consultado el 15 de enero de 2012.
39. Informe de VeriSign iDefense Security Lab citado por Ryan Paul, "Researchers identify command servers behind Google attack" (Investigadores identifican servidores del comando detrás de ataque a Google), *ArsTechnica*, enero de 2010. Disponible en: <http://arstechnica.com/security/news/2010/01/researchers-identify-command-servers-behind-google-attack>.ars, consultado el 15 de enero de 2012.
40. John Markoff and David Barboza, "Two Chinese Schools Said to be Tied to Online Attacks" (Se dice que dos escuelas chinas están ligadas a ataques en línea), *New York Times*, 19 de febrero de 2010.
41. *Ibíd.*
42. *Ibíd.*
43. Al momento de este artículo, la extensión de la participación de la clase y el nombre del profesor ucraniano no están disponibles en informe de fuente abierta.
44. *Ibíd.*
45. Hillary Rodham Clinton, "Remarks on Internet Freedom" (Comentarios sobre libertad en la Internet), 21 de enero de 2010. Disponible en: <http://www.state.gov/secretary/rm/2010/01/135519.htm>, consultado el 15 de enero de 2010.
46. Eric Chien, Gavin O'Gorman, "The Nitro Attacks, Stealing Secrets from the Chemical Industry" (Los ataques Nitro, robándole secretos a la industria química), *Symantec Security Response*, 2011.
47. "Global Energy Cyberattacks: 'Night Dragon'", *McAfee White Paper*, 10 de febrero de 2011.
48. Lucian Constantin, "Hackers Compromise Adobe Server, Use it to Digitally Sign Malicious Files" (Hackers comprometen servidor Adobe, lo emplean para firmar digitalmente archivos maliciosos), *CIO*, 27 de septiembre de 2012, disponible en: http://www.cio.com/article/717494/Hackers_Compromise_Adobe_Server_Use_it_to_Digitally_Sign_Malicious_Files, consultado el 14 de octubre de 2012.

Las opiniones en este artículo son las de los autores y no necesariamente reflejan las opiniones ni del Departamento de Defensa de Estados Unidos, ni del Ejército de Estados Unidos, ni de la Academia Militar de Estados Unidos.



El Dr. Paulo Shakarian, PhD, cuenta con un doctorado en ciencias computacionales y es un Mayor en el Ejército de Estados Unidos. Actualmente es profesor adjunto en *West Point* donde dicta clases en ciencias computacionales y tecnología de informática. Ha escrito más de veinte artículos publicados en varias revistas científicas y militares. Anteriormente sus obras han sido publicadas en *The Economist*, *WIRED* y *Popular Science*.



La Sra. Jana Shakarian cuenta con una maestría en sociología y antropología y anteriormente se desempeñó en calidad de científica investigadora en el Laboratorio para Dinámica Computacional Cultural de la University of Maryland y como asesora independiente con el *Network Science Center* en *West Point*.



El Sr. Andrew Ruef es ingeniero ejecutivo de sistemas en la empresa *Trail of Bits* (New York, NY) donde lleva a cabo análisis de seguridad de informática. Cuenta con casi una década de experiencia en la industria de seguridad en la red de computadoras e ingeniería de *software*.