ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

60/2013 1 julio de 2013

*Eguskiñe Lejarza Illaro**

ESTADOS UNIDOS - CHINA: EQUILIBRIO DE PODER EN LA NUEVA CIBERGUERRA FRÍA

ESTADOS UNIDOS - CHINA: EQUILIBRIO DE PODER EN LA NUEVA CIBERGUERRA FRÍA

Resumen:

China y los Estados Unidos se han enfrentado durante los últimos meses a un cruce de acusaciones mutuas sobre ataques a las redes informáticas de sus infraestructuras críticas, y robos de información de sectores cruciales para los intereses nacionales. Aunque los gobiernos de Washington y Beijing han centrado sus esfuerzos diplomáticos en diseñar un marco de actuación en el ciberespacio, lo cierto es que ambos países se han embarcado en una carrera para incrementar sus capacidades defensivas en este ámbito, desembocando en lo que se podría denominar como la ciberguerra fría del siglo XXI.

Abstract:

China and the United States have faced during the last months to a mutual exchange of accusations over attacks on the computer networks of their critical infrastructure and information theft of crucial sectors for their national interests. Although the governments in Washington and Beijing have focused their diplomatic efforts on designing a framework for action in the cyberspace, the fact is that both countries have been embarked on a race to enhance its defensive capabilities in this area, leading to what might be called the XXI century cyber cold war.

Palabras clave:

República Popular China, Estados Unidos de América, ciberguerra, infraestructuras críticas.

Keywords:

China, United States of America, cyberwar, critical infrastructure.

ESTADOS UNIDOS - CHINA: EQUILIBRIO DE PODER EN LA NUEVA CIBERGUERRA FRÍA

"China's economic espionage has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy.
Beijing is waging a massive trade war on us all, and we should band together to pressure them to stop. Combined, the United States and our allies in Europe and Asia have significant diplomatic and economic leverage over China, and we should use this to our advantage to put an end to this scourge."
U.S. Rep. Mike Rogers, October, 2011
"It is unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence."
Chinese Defense Ministry, January, 2013[1]

INTRODUCCIÓN

Las acusaciones de ciberespionaje vertidas mutuamente durante los últimos meses por los gobiernos de Estados Unidos y China, han añadido más tensión al ya delicado equilibrio diplomático existente entre ambos países. Washington y Beijing ya se enfrentaban a otros focos de conflicto como las relaciones con Taiwán, el armamento nuclear de Corea del Norte, el libre comercio o las disputas territoriales marítimas que enfrenta a China con Japón y Taiwán por las llamadas Islas Senkaku[2]. A pesar de que los dos países han venido alertando de intrusiones informáticas contra objetivos financieros, económicos y militares de sus países desde hace años, el recrudecimiento de los mismos coincide temporalmente con el momento en que Estados Unidos estudia aumentar progresivamente su presencia en el Sudoeste Asiático hasta 2020[3].

Dejando aparte el complejo mapa estratégico político-militar al que se enfrentan los dos países, no hay que obviar otra cuestión sustancial en sus relaciones bilaterales como es el

[1] MANDIANT, APT1 Exposing One of China's Cyber Espionage Units, 2013, p. 1. Disponible en http://intelreport.mandiant.com/. Fecha de la consulta 04-06-2013.
[2] Las Islas Sensaku o Diayou (en Chino) son un conjunto de ocho islas localizadas en el Mar del Este de China/Mar de Japón. El conflicto territorial comienza en 1969 por cuestiones como la explotación de los recursos naturales, consideraciones geopolíticas por su situación estratégica en las rutas internacionales y razones de derechos históricos.
[3] Declaraciones de Leon Panetta en el IX Diálogo de Sangri-La (celebrado en Singapur en 2012) y organizado por el Instituto Internacional de Estudios Estratégicos. El Plan incluiría aumentar la presencia militar con seis portaaviones, la mayor parte de los cruceros de la Armada, destructores, barcos de combate en litoral y submarinos, a la vez que anunciaba un "un aumento en el número y tamaño de nuestros ejercicios en el Pacífico y Océano Indico". http://www.defense.gov/speeches/speech.aspx?speechid=1681

hecho de que China es uno de los principales acreedores de Estados Unidos. Según datos del Departamento del Tesoro Estadounidense, el gigante asiático, con 1.264,9 mil millones de dólares ostentaba en abril de 2013 el primer puesto en la lista oficial de poseedores extranjeros de deuda pública norteamericana, por delante de Japón con 1.100,3 mil millones[4].

Las relaciones comerciales entre ambos países, existentes ya en el siglo XIX, empezaron a regularizarse de manera legal con la firma en 1979 del Tratado de Relaciones Comerciales. Tras ratificar varios acuerdos específicos en años sucesivos para promover el intercambio comercial entre ambos gobiernos, las relaciones Beijing-Washington atravesaron una delicada situación diez años después tras los sucesos de la Plaza de Tiananmen. EEUU impuso serias sanciones al gobierno chino que incluía el embargo a las exportaciones de este país.

La década de los años 90 reflejó las tensiones económicas entre ambos países, a pesar del esfuerzo diplomático para evitar una guerra comercial que desembocó en la firma de nuevos acuerdos con la llegada del siglo XXI. La regularización de sus relaciones comerciales y la firma de un Acuerdo Bilateral, trajeron consigo un considerable aumento del intercambio comercial que se vio multiplicado casi por cinco en la pasada década, lo que ha convertido a China en el principal cliente y acreedor de Estados Unidos.

Esta situación bien podría ejemplificar el término de interdependencia compleja acuñado por Robert O. Keohane y Joseph S.Nye[5], ya que el déficit de Estados Unidos y el interés de China, como país marcadamente exportador en invertir su superávit de divisas en Estados Unidos, hace que el gobierno chino necesite de la solvencia económica norteamericana para hacer frente a sus compromisos.

Pero para potenciar su avance económico, el gigante asiático ha trazado un importante andamiaje de relaciones comerciales, dirigidas a proyectar su presencia comercial en el Norte y Centro de Asia, que han beneficiado incluso a aliados de Estados Unidos dentro de este continente, como es el caso de Japón. En el 2011, ambas potencias asiáticas tomaban la determinación de abandonar el dólar como moneda de intercambio en sus transacciones comerciales, lo que implicaba que la intermediación de organismos económicos norteamericanos dejaría de tener presencia en los mismos[6]. Más allá de este trato que

[4] Información obtenida del Tesoro Norteamericano el 7 de junio de 2013 http://www.treasury.gov/resource-center/data-chart-center/tic/Documents/mfh.txt .

[5] Keohane, R.O., Nye, J.S., Power and Interdependence: Worlds Politics in Transition, Little, Brown, 1977.

[6] The People´s Bank of China. Enhanced Cooperation for Financial Markets Development between China and Japan (25-12-2011) disponible en http://www.pbc.gov.cn/publish/english/955/2011/20111225173248498166576/20111225173248498166576_.

promueve el uso de la propia moneda como agente de cambio, China ha establecido acuerdos con Corea del Sur y otros países dentro del marco de la Asociación de Naciones del Sudoeste Asiático (ASEAN), ha aumentado sus transacciones con India y Rusia o ha iniciado negociaciones con Seúl para constituir una zona de libre comercio.

EVOLUCIÓN DEL CONFLICTO

Dentro de esta compleja coyuntura económica, Estados Unidos daba la voz de alerta, el pasado mes de febrero, de que diversos organismos e instituciones públicas y gubernamentales, vinculadas al ámbito socio-económico norteamericano, habían sido objeto de ciberataques. Grandes empresas de comunicación como Google, Twitter o el New York Times, proveedores de defensa, plantas químicas, la red sanitaria e incluso empresas emblemáticas como Coca-Cola, veían vulnerada su seguridad informática en lo que Washington calificó como "un robo de los secretos corporativos"[7] orientado a manipular las infraestructuras críticas de Estados Unidos.

En el Discurso sobre el Estado de la Unión del 2013, el Presidente Norteamericano Barack Obama reconocía que:

"Estados Unidos también debe hacerle frente a la amenaza real y creciente de ataques cibernéticos. Sabemos que los piratas informáticos roban las identidades de personas e infiltran correos electrónicos privados. Sabemos que empresas extranjeras sustraen nuestros secretos corporativos. Y nuestros enemigos buscan la capacidad de sabotear nuestra red de energía eléctrica, nuestras instituciones financieras, y nuestros sistemas de control del tráfico aéreo. No podemos mirar hacia atrás en años venideros y preguntarnos por qué no hicimos nada ante las serias amenazas a nuestra seguridad y nuestra economía"[8].

La Administración Obama se apresuraba entonces a emitir una Orden Ejecutiva reconociendo que "la amenaza cibernética a las infraestructuras críticas continúa creciendo y representa uno de los desafíos más graves a la seguridad nacional que debemos confrontar. La seguridad nacional y económica de Estados Unidos depende del funcionamiento fiable de las infraestructuras críticas nacionales ante semejantes amenazas"[9].

---

html . Fecha de la consulta 08-06-2013.

[7] Barack Obama. Discurso sobre el Estado de la Unión 2013 (13-02-2013). Disponible en http://www.whitehouse.gov/state-of-the-union-2013. Fecha de la consulta 08-06-2013.

[8] Ibídem.

[9] The White House, Executive Order-Improving Critical Infrastructure Cybersecurity. February 12, 2013. Disponible en http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-

La Orden, emitida el 12 de Febrero, definía, en su sección 2, el termino infraestructura crítica como "aquellos sistema y activos, ya sean físicos o virtuales, tan vitales para Estados Unidos, que la incapacidad o destrucción de los mismos, podrían tener un debilitante impacto en la seguridad, la economía, la salud pública nacional o cualquier combinación de ambas materias"[10].

El aspecto novedoso lo introducía la sección cuatro, desde la que se instaba a las entidades privadas de Estados Unidos a compartir con el gobierno información sobre la frecuencia, volumen y calidad de los ciberataques sufridos, con el fin de preservar la seguridad nacional. Esta medida redundaría además en la salud económica del país, ya que se da la circunstancia de que gran parte de las infraestructuras básica, como centrales energéticas o de agua potable, se encuentran en manos privadas.

Esta vulnerabilidad y la duda razonable de que los organismos y compañías que controlan infraestructuras críticas de la nación estaban siendo objeto de sustracciones ilegítimas de información sensible, hacía más urgente la necesidad de que gobierno y empresas compartieran información sobre posible ciberataques.

Pero este planteamiento no es nuevo. En 2009, un informe realizado por la empresa de Seguridad Informática McAfee bajo el título "Criminología Virtual" alertaba ya de que:

"Las infraestructuras críticas de los países - el sistema bancario y financiero, las redes de suministro de electricidad, las refinerías de petróleo y gas, los oleoductos y gaseoductos, los servicios públicos de abastecimiento de agua o los sistemas de telecomunicaciones - son probables objetivos de guerras futuras. En muchos países, especialmente en Occidente, la privatización de estos servicios públicos implica que las empresas privadas quedarán inevitablemente atrapadas en un fuego cruzado"[11].

En el mismo informe, los expertos consideran que:

"El sector privado debe colaborar con el gobierno para hallar nuevas medidas de defensa, como clasificar los activos de redes informáticas, desarrollar planes de reducción de impacto y respuesta rápida, crear redes independientes para los sistemas más críticos y desarrollar

infrastructure-cybersecurity. Fecha de la consulta 06-06-2013.

[10] Ibídem.

[11] McAfee, Informe sobre Criminología Virtual 2009. "La era de la ciberguerra, casi una realidad" disponible en http://www.mcafee.com/mx/resources/reports/rp-virtual-criminology-report-2009.pdf, p. 3. Fecha de la consulta 19-06-2013.

una visión sinóptica de la actividad de la red, con el fin de mejorar la concienciación sobre el problema en los distintos sectores"[12].

Precisamente por ello, la Orden Ejecutiva de Obama daba un plazo de 240 días para configurar las Bases de un Marco de Trabajo para Reducir los Ciberriesgos de las Infraestructuras Críticas "que incluirá un conjunto de normas, metodologías, procedimientos y procesos que alineará la política, los negocios y los enfoques tecnológicos para abordar los ciberriesgos"[13].

En el 2007, McAfee había realizado una encuesta entre seiscientos responsables de Tecnologías de la Información y Seguridad, procedentes de empresas de administración de infraestructuras críticas de siete sectores en 14 países de todo el mundo, cuyas conclusiones presentó en el informe "Infraestructuras críticas en la época de la ciberguerra"[14]. De este estudio se desprendía que la mayor parte de los ejecutivos encuestados, reconocían la presencia de gobiernos extranjero tras los ataques sufridos a través de la red, contra las infraestructura critica de sus países. China y Estados Unidos se perfilaban, según los encuestados, como los principales ciberagresores, a pesar de que se reconocía que aseverar la identidad de los autores era una tarea muy difícil.

Paradójicamente, y según se desprende de una estadística incluida en el mismo informe sobre la percepción de 14 países acerca de la procedencia de las amenazas virtuales, China encabezaba el ranking de aquellos que consideraban que sus infraestructuras criticas habían sido atacadas por gobiernos extranjeros. Le siguen, Japón, Francia, Australia, India y Rusia. Estados Unidos ocupa el séptimo lugar, y España, el último[15].

Además de las brechas de seguridad que suponen estas intromisiones, hay un importante factor económico a tener en cuenta: Los grandes ciberataques son costosos. Según indica el informe, los costes del tiempo de inactividad asociado a un incidente importante de ciberseguridad[16] podrían ser muy altos.

De media, los encuestados calcularon que 24 horas de inactividad por un ataque de magnitud supondrían 6,3 millones de dólares para su empresa. Los costes más elevados se registraron en el sector del petróleo y el gas, donde la media ascendía a 8,4 millones de

[12] Ibídem, p. 23.
[13] The White House, op. cit.
[14] MacAfee, En el Punto de Mira. "Las infraestructuras críticas en la era de la ciberguerra" disponible en http://resources.mcafee.com/content/EMEA_CIPreport_ES. Fecha de la consulta 19-06-2013.
[15] Ibídem, p. 4.
[16] Según el informe de McAfee, "se considera un incidente importante de ciberseguridad "el que provoque la interrupción grave de servicios durante al menos 24 horas, la pérdida de vidas o lesiones personales, o la quiebra de una compañía". Ibídem p. 10.

dólares diarios. Los más bajos se produjeron en el sector gubernamental y el de agua y saneamiento.

Aunque la Orden Legislativa emitida desde el Capitolio, anunciaba el inicio de la adopción de medidas para contrarrestar las intrusiones, la Administración Obama no hacía ninguna referencia a la autoría de las mismas.

INFORME MANDIANT

Habría que esperar pocos días después, cuando la Firma de Seguridad Informática norteamericana Mandiant, contratada por alguna de las víctimas de los ciberataques para limpiar y rastrear sus sistemas, ponía nombre al autor de las intrusiones: relacionaba implícitamente a la Unidad 61398 del Ejército Popular de Liberación Chino (PLA), presuntamente encargada de la ciberinteligencia, con el denominado ATP1 (Advanced Persistent Threat), el más "activo" de los más de 20 grupos originados en China y dedicados a actividades no legítimas en las redes[17].

Según el informe, Mandiant era conocedora ya en 2010 de que:

"El Gobierno Chino puede autorizar esta actividad, pero no hay forma de determinar la medida de su participación. Ahora, tres años después, tenemos la evidencia necesaria, para cambiar nuestra evaluación. Los detalles que hemos analizado durante cientos de investigaciones convencen de que los grupos que realizan estas actividades se basan principalmente en China y el gobierno chino es consciente de ellos"[18].

Después de rastrear las "huellas digitales" dejadas por el APT 1 en sus ataques informáticos, el informe localiza el epicentro de sus operaciones en el distrito de Pudong, un área comercial y financiera emergente de la ciudad de Shanghái. Asimismo, en un intento de establecer una relación directa entre la Unidad y el APT1, puntualiza que "la Unidad 61398 del Ejército Popular de Liberación Chino (PLA) es similar a APT1 en misión, capacidades y recursos", a la vez que confirma que ambos ejercen su actividad desde la misma área geográfica[19].

Entre las claves de sus investigaciones, la compañía norteamericana revela que la naturaleza del trabajo de la Unidad 61398 es considerada por China como un secreto de Estado; y que

[17] MANDIANT, op. cit. p. 2.
[18] Ibídem, p. 2.
[19] Ibídem, p. 2.

está formada "por cientos o quizás miles de personas a juzgar por su infraestructura física"[20]. Este personal, añaden, debe cumplir una serie de requisitos como dominar perfectamente el inglés o ser experto en seguridad informática y operaciones en red.

El reclutamiento de los profesionales que conformarían la plantilla de la citada Unidad se realizaría desde las facultades de Ciencia e Ingeniería de Universidades como el "Harbin Institute of Technology" y la "Zheijiang University Scholl of Computer Science and Technology"[21].

El objetivo de los ataques iba dirigido, según Mandiant, a empresas y organismos de países angloparlantes cuya información pudiera beneficiar a aquellas áreas definidas por el Gobierno China como de "crecimiento estratégico" en su 12th Five Year Plan[22].

En la página 2 de este documento, el Gobierno chino marca siete sectores de crecimiento considerado como prioritario para la nación y que son

- Nuevas energías (solar, aire y nuclear).
- Conservación de la energía y protección del medio ambiente.
- Biotecnología.
- Nuevos materiales.
- Nuevas Tecnologías (infraestructura de seguridad en internet, redes de banda ancha, convergencia de redes).
- Fabricación de equipos de alta gama (aeroespaciales y de comunicaciones).
- Fabricación de vehículos de energía limpia.

La compañía basa esta hipótesis en el hecho de que determinadas actividades industriales o empresariales norteamericanas, como las dedicadas a tecnologías de la información, aeroespacial, administraciones públicas, satélites y telecomunicaciones, investigaciones científicas y energía, han sufrido más duramente los efectos de la campaña de ciberespionaje chino. Las relacionadas con educación, sanidad, metales y minería, alimentación y agricultura y servicios financieros, apenas carecen de interés para los delincuentes informáticos[23].

[20] Ibídem, p. 3.
[21] Ibídem, p. 10-11.
[22] China´s 12th Five-Year Plan: Overview. March 2011, p.2. Disponible en http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Publicationseries/5-years-plan/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf. Fecha de la consulta 03-06-2013.
[23] MANDIANT, op. cit. p. 24.

A lo largo del informe, Mandiant revela que el APT1 ha robado sistemáticamente cientos de terabytes procedentes de al menos 141 organizaciones desde 2006, con el fin de apropiarse de cantidades masivas de propiedad intelectual. El grupo utilizaría además una técnica metódica y bien definida que se inicia con una agresiva campaña de phishing, para proceder a desplegar armas digitales personalizadas que concluye con la exportación de paquetes comprimidos de archivos con datos robados a China, antes de comenzar el ciclo otra vez[24].

Del total de las organizaciones que han visto vulnerados sus sistemas de seguridad, 115 están localizadas en Estados Unidos, y siete entre Canadá y Reino Unido. De las 19 restantes, 17 utilizaban la lengua inglesa como herramienta para sus operaciones, entre ellas se incluyen aquéllas destinadas a cooperación internacional, agencias en desarrollo, gobiernos extranjeros que utilizan el inglés como una de sus múltiples lenguas oficiales y multinacionales que utilizan esta lengua para el desarrollo de sus negocios. Las dos organizaciones restantes son calificadas por Mandiant como "anomalías" entre los objetivos del cibergrupo[25].

En lo que se refiere a la autoría física de los ciberataques, Mandiant pone nombre propio a tres de los actores implicados en los ataques. Tras un amplio seguimiento de sus actividades en la red, la compañía cita a UglyGorilla, quien ya en 2004 expresó públicamente su interés por las "cibertropas" chinas, DOTA y finalmente SuperHard, al que identifican como uno de los cerebros de la creación de familias de malware dañinos como Auriga o Bangat[26].

Uno de los datos aportados por la compañía norteamericana, que podría ayudar a establecer un vínculo más directo entre los ciberataques y el gobierno Chino, es que atribuye a la empresa de propiedad estatal China Telecom, en colaboración con la Unidad 61398, la construcción de la infraestructura de redes informáticas para las operaciones. Mandiant aporta un documento interno de China Telecom en el que admite su colaboración implícita para la construcción de líneas de comunicación de fibra óptica "basada en el principio de que la construcción de la defensa nacional es importante"[27]. "Además, la carta utiliza el nombre de "Unidad 61398" junto con el comentario "GSD 3rd Department, 2nd Bureau". En otras palabras, según el organigrama del Partido Comunista Chino, este 2nd Bureau dependería directamente del 3er Departamento del Ejército Popular de Liberación Chino, como se indica en la figura 1. Las funciones de este 3er Departamento, en equiparación con sus homólogos americanos, consistirían en aquellas asignadas a la Agencia de Seguridad Nacional (U.S

[24] Ibídem, p. 27.
[25] Ibídem, p. 21.
[26] Ibídem, p. 5.
[27] Ibídem, p. 17-18.

National Security Agency, conocida como NSA), el Instituto de Lenguas de Defensa y partes de las asignadas a la Agencia de Sistemas de Información de Defensa[28].

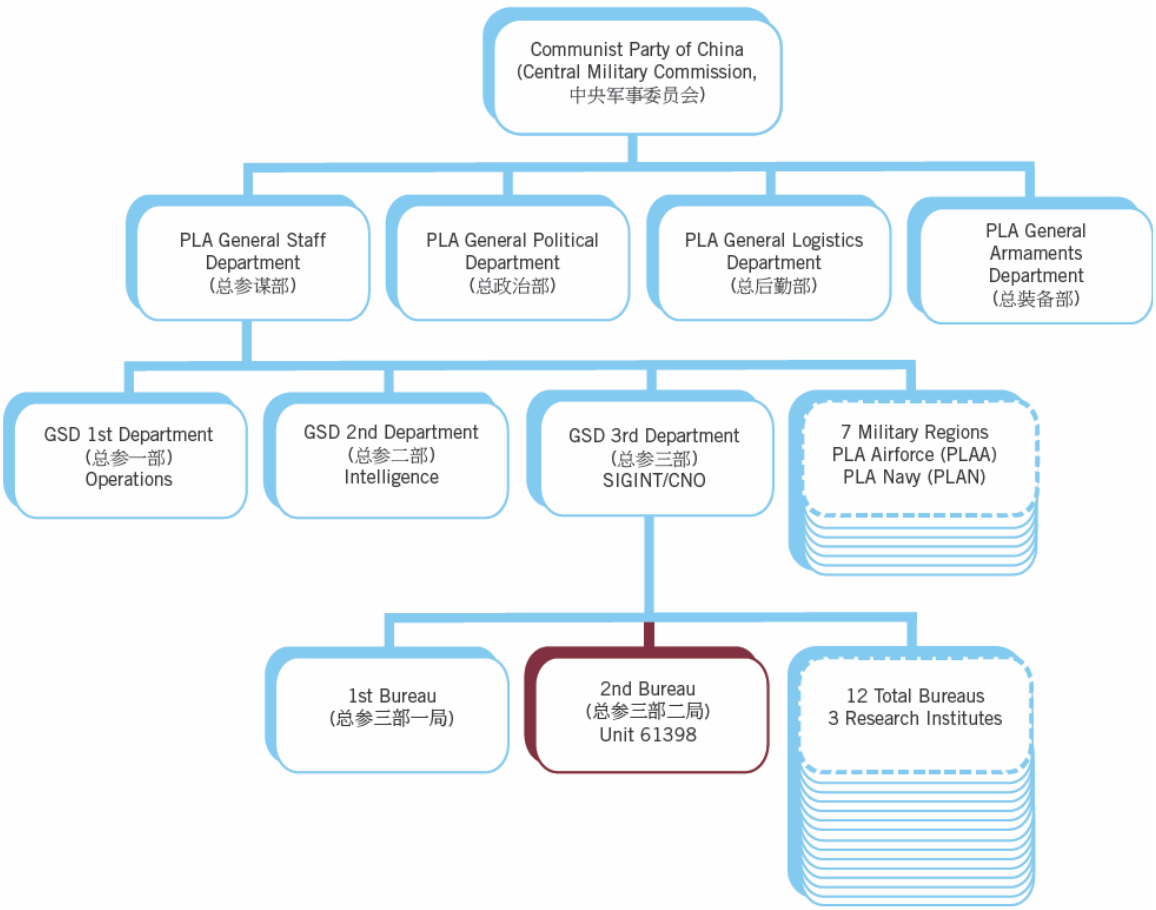

Figura 1: Situación de la Unidad 61398 dentro del Ejército Popular de Liberación Chino[29].

Como conclusión a su informe, Mandiant lanza una seria advertencia sobre las ciberactividades del llamado APT1, afirmando que es capaz de continuar con su rápida y extensiva campaña de ciberespionaje "porque está actuando con el pleno conocimiento y cooperación del Gobierno. Es tiempo ya de conocer que la amenaza se está originando en China, y nosotros queríamos aportar algo para armar y preparar profesionales de la seguridad que combatan este amenaza efectivamente"[30].

Las reacciones al informe Mandiant no se hicieron esperar. El portavoz de Exteriores chino Hong Lei, afirmaba que "los ataques de los hacker son transnacionales y se pueden ocultar. Determinar su origen es muy difícil".

[28] Ibídem, p. 8.
[29] Ibídem, p. 8.
[30] Ibídem, p. 59.

Qian Xiaoqian, Viceministro chino de Información, negó rotundamente que su país abusara de los recursos de internet, a la vez que puntualizó que éste había sido víctima de 6.600 ataques, realizados por ordenadores ubicados en Estados Unidos durante los pasados meses de enero y febrero. "No debemos militarizar el ciberespacio. Estos ataques violan los derechos de otros países y los estándares morales"[31].

Para avalar la tesis gubernamental, la agencia oficial Xinhua hacía público un informe, elaborado por el Centro de Coordinación Nacional de Respuestas a Emergencias de Red (CNCERT), en el que se detalla que 85 páginas web de instituciones y compañías estatales chinas, habían sido atacadas desde el exterior entre septiembre de 2012 y febrero de 2013. El documento ubica en Estados Unidos el epicentro de operaciones del 73,1% de los servidores que utilizaron sistemas de control para apoderarse ilegítimamente de los datos contenidos en los ordenadores chinos. Entre los objetivos vulnerados figura la web oficial de El Diario Pueblo (people.com.cn), el Portal de Información Gubernamental (China.com.cn), además de agencias del gobierno, una compañía de seguros de la propiedad y un centro de investigación de virus en el centro de China[32].

INFORME DEL PENTÁGONO

A pesar de la controversia política suscitada entre Washington y Pekín, tras la publicación del estudio de Mandiant, el conflicto se recrudeció a principios de mayo cuando el Pentágono responsabilizaba formalmente al Gobierno Chino de los ataques informáticos sufridos por organismos, empresas y agencias estadounidenses en su Informe Anual al Congreso. El "Annual Report to Congress Military and Security Developments Involving the People´s Republic of China 2013"[33], elaborado por el Departamento de Defensa, desgrana las actuales capacidades militares que está desarrollando y las que ya dispone el Ejército Popular de Liberación. Entre ellas hay que citar las llamadas Operaciones Militares de Información, punto en el que hacen especial hincapié sobre el nivel de maduración del denominado "Chinese Information Operations Estrategy (IO)". El informe del departamento de Defensa desvela que el funcionamiento del IO estaría fundamentado en cinco claves muy concretas:

[31] The Camberra Times, 10-04-2013. Disponible en http://www.canberratimes.com.au/it-pro/security-it/cyber-attacks-hurt-chinas-credibility-us-official-20130410-2hkpc.html . Fecha de la consulta 07-06-2013.
[32] Xinhua, 10-03-2013. Disponible en http://news.xinhuanet.com/english/china/2013-03/10/c_132223206.htm. Fecha de la consulta 03-06-2013.
[33]Departamento de Defensa de los EE.UU, "Annual Report to Congress Military and Security Developments Involving the People´s Republic of China 2013". Disponible en http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf. Fecha de la consulta 06-06-2013.

- La defensa es una prioridad fundamental, por lo que el "Computer Network Defense" (CDN) debe ser visto como una alta prioridad en tiempo de paz.
- Las Operaciones de Información son vistas como una "arma de guerra no convencional", la cual debe ser establecida en la fase inicial del conflicto y continuar durante todas las etapas de la guerra.
- IO es caracterizada como una arma anticipativa para ser usada bajo la intención de conseguir información dominante y controlar el espectro electromagnético.
- IO es considerada como una herramienta que permitiría a China luchar y ganar en una campaña de información.
- Los potenciales adversarios de China, en particular, los Estados Unidos, son percibidos como "dependientes de información"[34].

Según el Pentágono, el Ejército Popular de Liberación Chino realiza frecuentes ejercicios militares, en los que demuestra los avances en tecnología de la información conjuntamente con fuerzas militares convencionales[35].

Bajo el epígrafe Ciberactividades dirigidas contra el Departamento de Defensa, el informe acusa formalmente a China de actividades ilegitimas en el ciberespacio: "En 2012, numerosos sistemas informáticos de todo el mundo, incluyendo aquellos que pertenecen al Gobierno de Estados Unidos, continúan siendo objetivo de intrusiones, alguna de las cuales parecen ser atribuibles directamente al gobiernos y militares chinos. Estas intrusiones están dirigidas a obtener información"[36].

El informe continúa afirmando que China utiliza las capacidades de sus redes informáticas para incrementar sus conocimientos de inteligencia, que luego podrían ser utilizados "contra la diplomacia y la economía de Estados Unidos, así como las industrias base en el sector de Defensa que desarrollan los Programas norteamericanos en esta materia"[37]. El hecho de que la citada información pueda ser utilizada en beneficio de la industria de defensa china, sus industrias de alta tecnología e intereses políticos, es percibido como una clara amenaza.

A pesar del hermetismo del Pentágono sobre información vulnerada al Departamento de Defensa en esta grave brecha de seguridad, The Washington Post[38] filtraba una lista confidencial que incluía cerca de 24 nuevas armas utilizadas por el ejército, así como varios

[34] Departamento de Defensa de los EE.UU. op. cit. p. 10.
[35] Ibídem, p. 11.
[36] Ibídem, p. 36.
[37] Ibídem, p. 36.
[38] The Washington Post, 28-05-2013. Disponible en 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. Fecha de la consulta 07-06-2013.

proyectos armamentísticos, y que ahora estarían en posesión del Gobierno chino. Algunas de ellas constituían la columna vertebral de la defensa regional de misiles prevista para Asia, Europa y el Golfo Pérsico. Los diseños incluyen el sistema avanzado de misiles Patriot, conocido como PAC-3; un sistema para derribar misiles balísticos conocido como THAAD; o el sistema de defensa de misiles balísticos Aegis de la Armada. El rotativo concluye que los hackers chinos se habrían apoderado también del sistema de armas más caro jamás construido: el F-35 Joint Strike Fighter, cuyo coste rondaría aproximadamente los 1,4 billones de dólares, y cuyo proyecto ya había sido objeto de otro ciberataque en el 2007.

El documento del Pentágono advierte que estas capacidades informáticas podrían ser utilizadas por China en tres áreas estratégicas:

- Primero, para obtener datos de interés para inteligencia y con el propósito de poder llevar a cabo ataques a redes informáticas.
- Segundo, pueden ser empleadas para restringir las acciones de un adversario o ralentizar su tiempo de respuesta al atacar las redes logísticas, de comunicaciones y actividades comerciales.
- Tercero, pueden servir como un multiplicador de fuerza, cuando se combinan con ataques cinéticos en tiempos de crisis o de conflicto.

El desarrollo de cibercapacidades para una Guerra es ampliamente documentado por escritos autorizados del PLA, entre los que citan Science of Strategy y Science of Campaigns, dos documentos militares que identifican la guerra de la información como "esencial para lograr la superioridad de la información y un medio eficaz para luchar contra un enemigo más fuerte"[39]. Aunque ninguno de los dos documentos citados identifica criterios específicos para utilizar los ataques en la red contra un enemigo, ambos defienden el desarrollo de capacidades para combatir en este campo. Como *Science of Strategy* explica, "En la Guerra de la Información, los sistemas de mando y control son el corazón de la obtención de datos, el control y su aplicación en el campo de batalla. Es también, el nervio central de todo el campo de batalla"[40].

El informe de defensa remarcaba que China ha incrementado sus acuerdos diplomáticos y apoyos en aquellos foros multilaterales e internacionales donde se discuten cuestiones sobre la ciberdefensa. A la par, resalta que "la agenda de Beijing esta frecuentemente en concordancia con los esfuerzos de Rusia para promover más control internacional sobre ciberactividades"[41].

[39] Departamento de Defensa de los EE.UU, op. cit. p. 36.
[40] Ibídem, p. 37.
[41] Ibídem, p. 37.

En este sentido recuerda el interés de ambos países por promover un Código de Conducta sobre la Seguridad de la Información, que daría a los gobiernos un control absoluto sobre el flujo de la información y los contenidos del ciberespacio. Código de Conducta, presentado en 2011 ante la Asamblea General de Naciones Unidas, a la vez que acusa a ambos gobiernos de jugar un papel disruptivo frente al marco de organizaciones internacionales que pretenden instaurar una medida en base a la transparencia y la confianza.

INCREMENTO DE CAPACIDADES

El Pentágono afirma que el Ejército Popular de Liberación Chino dedica la nomenclatura EW para identificar la Guerra Electrónica, "como una forma de eliminar o reducir los avances tecnológicos de Estados Unidos". El informe concluye que para China es una Cuarta dimensión vital para el combate y que sería considerada al mismo nivel que las fuerzas tradicionales de tierra, mar y aire. En efecto, los objetivos de esta ofensiva estarían focalizados en la radio, radares, frecuencias de onda corta, así como ordenadores y sistema de información[42].

En este sentido sostiene, que Unidades de EW de Ejército Popular de Liberación Chino han llevado a cabo operaciones de jamming y anti-jamming, poniendo a prueba el grado de comprensión que tienen las fuerzas armadas sobre armas de EW, su equipamiento y rendimiento, hechos que han ayudado a aumentar su confianza en la ejecución de operaciones de enfrentamiento directo, con equipo real en ambientes de simulación de guerra electrónica. Los avances en la investigación y el despliegue de armas de guerra electrónica se están probando en estos ejercicios y han demostrado su eficacia. Estas armas incluyen equipos jamming contra múltiples sistemas de comunicaciones y de radar y sistemas de satélite GPS", aseveran.[43]

La portavoz del Ministerio de Relaciones Exteriores Chino, Hua Chunying, calificaba de "indiscretos" los comentarios vertidos por el Departamento de Defensa Norteamericano sobre "la construcción legítima y normal de la defensa nacional de China y difundiendo la teoría de la llamada amenaza militar de China, lo que no es propicio para la confianza mutua y la cooperación entre ambas partes. Nos oponemos firmemente a ello y hemos hecho gestiones con la parte norteamericana"[44].

[42] Ibídem, p. 37.
[43] Ibídem, p. 37
[44] Conferencia de Prensa de la Portavoz del Ministerio de Relaciones Exteriores, 07-05-2013. Disponible en http://www.embajadachina.es/esp/fyrth/t1038739.htm. Fecha de la consulta 10-06-2013.

Chunying afirmaba que "la seguridad en la red atañe a los gobiernos, a los secretos comerciales y a la intimidad personal", a la vez que afirmaba que el gobierno, personas e instituciones de su país otorgaban la misma importancia que sus homólogos norteamericanos a la importancia de la misma a la vez que mostraba su oposición a las actividades de los hackers.

"China sigue invariablemente el camino de desarrollo pacífico, aplica una política defensiva y constituye una fuerza firme para la salvaguardia de la paz y la estabilidad en la región de Asia-Pacífico y en el mundo. Partiendo de sus propias circunstancias, China realiza la necesaria y moderada construcción de defensa nacional sólo para salvaguardar la independencia nacional, la soberanía y la integridad territorial. Eso también es un legítimo derecho de un Estado soberano", afirmaba la portavoz China.

Por otra parte, el portavoz del Ministerio de Defensa Chino Geng Yanshseng rebatía el compendio de acusaciones formuladas por el Washington Post. "El reportaje subestima la capacidad de seguridad del Pentágono y la inteligencia del pueblo Chino. China tiene ya la habilidad de construir las armas necesarias para la seguridad nacional, como la construcción de portaaviones, aviones de combate, grandes aviones de transporte y el sistema de navegación por satélite Beidou, claramente han demostrado"[45].

En este clima, los máximos dirigentes de ambos países mantuvieron a principios de junio un encuentro en California, en el que las acentuadas acusaciones mutuas sobre ciberataques tuvieron una importancia fundamental, y que, una vez más, fueron atenuadas por las habilidades diplomáticas de ambos gobiernos. Tanto Obama como Xi Jinping, consideraron que los ataques a sus sistemas informáticos no era el principal escollo a resolver entre sus gobiernos. Asimismo, reafirmaron su voluntad "para construir sistemas de defensa y protección, tanto en el sector público como privado, a la vez que negociar con otros países para construir normas comunes"[46].

Hasta que ese momento llegue, ambas potencias han dado un paso adelante en la preparación de su defensa contra intrusiones en el espacio virtual.

El 23 de julio de 2009, el secretario de Defensa de Estados Unidos ordenó al jefe del Mando Estratégico de EEUU (USSTRATCOM) la creación del "United States Cyber Command"

[45] Ministerio de Defensa Chino, 30-05-2013. Disponible en http://eng.mod.gov.cn/Press/2013-05/31/content_4453733.htm. Fecha de la consulta 12-06-2013.

[46] The New York Times, 08-06-2013. Disponible en http://www.nytimes.com/2013/06/09/world/asia/obama-and-xi-try-building-a-new-model-for-china-us-ties.html?pagewanted=all&_r=0 . Fecha de la consulta 09-06-2013.

(USCYBERCOM), cuya capacidad operativa inicial se logró el 21 de mayo de 2010, bajo el mando del general de cuatro estrellas Keith Alexander, que es también el Director de la Agencia de Seguridad Nacional (NSA). Las instalaciones, localizadas en Fort Meade, Maryland, supusieron un costo de 358 millones de dólares.

En su documento fundacional se le define como un mando sub-unificado, subordinado al Mando Estratégico de los EE.UU. que incluye el Ciber Mando del Ejército de Tierra (ARFORCYBER); el Ciber Mando de las Fuerzas Aéreas y el Ciber Mando de los Marines (MARFORCYBER)[47].

Entre las misiones encomendadas, el USCYBERCOM fusiona el espectro completo de operaciones en el ciberespacio del Departamento de Defensa y planifica, coordina, integra, sincroniza y conduce actividades para dirigir la defensa en el día a día y la protección de las redes de Información del Departamento de Defensa. Asimismo se especifica que debe de prepararse para cuando se lo indique, realizar operaciones militares en el ciberespacio de amplio espectro. El Mando se encarga de agrupar los recursos existentes con capacidad para actuar en el ciberespacio, creando sinergias que no existen actualmente y sincronizar los efectos de combate.

Los esfuerzos del USCYBERCOM también apoyarán al conjunto de las Fuerzas Armadas para llevar a cabo con seguridad operaciones efectivas, así como proteger el mando y control los sistemas y la infraestructura del ciberespacio, apoyando a las plataformas de sistemas de armas de interrupciones, intrusiones y ataques.

En esta misma línea, la Agencia de Defensa para Proyectos de Investigación Avanzada (DARPA) ha desarrollado el Ciber Campo (NCR)[48] destinado a proporcionar evaluaciones realistas y cuantificables sobre el desarrollo e investigación de las cibertecnologías, y proteger los sistemas de información crítica nacionales. La finalidad es acelerar la transición tecnológica que permita cumplir con los propósitos recogidos en el "The Comprehensive National Cyber-Security Initiative" (CNCI)[49]. Este campo virtual permite simular ciberataques de potencias extranjeras o de delincuentes informáticos dentro de EEUU.

---

[47] Departamento de Defensa de los Estados Unidos, 25-10-2010. Disponible en http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf . Fecha de la consulta 14-06-2013.

[48] DARPA, The National Cyber Range: A National testbed for Critical Security Research. Disponible en http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf. Fecha de la consulta 14-06-2013.

[49] Consejo de Seguridad Nacional, disponible en http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative. Fecha de la consulta 04-06-2013.

Otro de los pilares fundamentales dentro de la defensa del ciberespacio americano, es la función desarrollada por la Agencia de Seguridad Nacional (NSA) que, bajo el mandato del general Keith Alexander, ya inauguró en 2012 un complejo en Georgia. En breve, la NSA reforzará su actividad defensiva con la inminente puesta en marcha del "Utah Data Center", en el marco de la Iniciativa Nacional Integral de Ciberseguridad de la Comunidad de Inteligencia, y que es considerada como la primera base de datos creada al amparo de "The Comprehensive National Cybersecurity Initiative". Entre las funciones de la nueva instalación, está la de agrupar todos los centros con responsabilidad en el ciberespacio, monitorizando en tiempo real tanto las redes gubernamentales como las privadas[50].

Por su parte, según ha informado la Agencia Oficial Xinhua, el Ejército Popular de Liberación Chino tenía previsto para finales de junio llevar a cabo un ejercicio para probar nuevos tipos de fuerzas de combate, que incluirán unidades que utilizarán tecnología digital, como un esfuerzo para adaptar sus medios a lo que podría considerarse una ciberguerra. La agencia resalta que será la primera vez que las fuerzas de combate chinas realicen unos ejercicios conjuntos en los que se incluyan unidades con capacidad de actuación en el ciberespacio, fuerzas de operaciones especiales, aviación y unidades de guerra electrónica[51].

Paralelamente a estas conversaciones entre los dos líderes, The Washington Post hacía público el anuncio del Departamento de Estado en relación a que China había acordado con los Estados Unidos, Rusia y otras naciones la aplicación del derecho internacional ante acciones de los Estados en el ciberespacio. Esto supondría un paso importante para garantizar que algunos sistemas civiles, como las redes de suministro de energía no sean objetivos de ataques cibernéticos[52].

El rotativo afirma que "este acuerdo de salvaguarda de las infraestructuras críticas de China ante las Naciones Unidas, culmina un esfuerzo plurianual de 15 países para reducir las tensiones en el ciberespacio y se produce en medio de la creciente preocupación de los altos funcionarios de Estados Unidos sobre intrusiones informáticas chinas en los registros privados de las corporaciones e instituciones norteamericanas"[53].

[50] Domestic Surveillance Directorate, Utah Data Center. Información disponible en http://nsa.gov1.info/utah-data-center/index.html. Fecha de la consulta 06-06-2013.
[51] Xinhua, 29-05-2013. Información disponible en http://news.xinhuanet.com/english/china/2013-05/29/c_132415053.htm. Fecha de la consulta 15-06-2013.
[52] The Washington Post, 07-06-2013. Información disponible en http://articles.washingtonpost.com/2013-06-07/politics/39823657_1_president-obama-chinese-president-xi-jinping-obama-and-xi . Fecha de la consulta 10-06-2013.
[53] Ibídem.

CONCLUSIONES

Aunque los expertos no parecen ponerse de acuerdo en cuanto al uso del término ciberguerra y lo que puede significar, lo que sí parece claro es que cada vez se dan con mayor frecuencia ciberataques, tras los cuales parecen esconderse motivaciones políticas, y no ser únicamente actividades de organizaciones delictivas.

Una de las definiciones de ciberguerra más difundidas en la actualidad es la de Richard A. Clarke:

"Se denomina ciberguerra cualquier penetración no autorizada por parte de, en nombre de, o en apoyo a, un gobierno en los ordenadores o las redes de otra nación, en la que el propósito es añadir, alterar o falsificar información o causar daños a, o perturbar el adecuado funcionamiento de, un ordenador, un dispositivo de red o los objetos controlados por el sistema informático"[54].

Según esta definición, si fuera posible demostrar que los ciberataques, que tienen por objetivos empresas y organismos estatales de los EEUU y de China, son llevados a cabo por sus respectivos gobiernos, o por lo menos auspiciados por ellos, estaríamos claramente dentro de la definición de ciberguerra que da Clarke. Pero el principal problema que surge con los ciberataques es la atribución, es decir demostrar quien ha sido el atacante. En el caso de China, ni el Pentágono en su informe, ni Mandiant en el suyo, dan pruebas concluyentes de que los ciberataques que mencionan hayan sido llevados a cabo por organismos oficiales chinos.

Lo que sí es demostrable, es que ambos países están enzarzados en una carrera armamentística virtual, con el objetivo de dotarse de capacidades tanto defensivas como ofensivas para su empleo en un hipotético ciberconflicto futuro. La finalidad sería demostrar al posible ciberagresor su poder, y disuadirle de actuar contra él, ante el temor que pudiera suscitar las acciones de represalia que se pudieran llevar a cabo.

Haciendo una analogía, la situación podría considerarse similar a la que tuvo lugar durante la guerra fría, en la cual los EEUU y la Unión Soviética se enzarzaron en una competición para dotarse de mayores arsenales nucleares que su contrincante. En este caso el poder nuclear era del que disponía cada nación era mesurable, ya que hacían ostentación del número de ojivas de las que disponían, y llevaban a cabo pruebas para demostrar sus capacidades al adversario.

[54] Clarke, R. A., Knake R. K. Guerra en la Red. Los Nuevos Campos de Batalla, Barcelona, Ariel, 2011, p. 296.

El problema que surge con las "ciberarmas" es que realmente no es de dominio público cuáles son sus capacidades reales, por lo que el efecto de disuasión es más difícil de conseguir, al no poder demostrarse cuál sería su eficacia en caso de emplearse.

En la situación actual, y a pesar de la escalada armamentística virtual, tomando como referencia las tesis del liberalismo de Keohane y Nye[55], la existencia de una densa red de interdependencia económica entre ambos estados, hace que, mientras se mantenga esa situación, a corto plazo un ciberconflicto abierto entre China y los EEUU sea algo poco probable.

*Eguskiñe Lejarza Illaro**
Periodista

[55] Keohane, R.O., Nye, J.S., Power and Interdependence, Nueva York, Harper Collins, 1989.

BIBLIOGRAFÍA

Barack Obama. Discurso sobre el Estado de la Unión 2013 (13-02-2013), http://www.whitehouse.gov/state-of-the-union-2013.

China´s 12th Five-Year Plan: Overview. March 2011, http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Publicationseries/5-years-plan/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf.

Clarke, R. A., Knake R. K. Guerra en la Red. Los Nuevos Campos de Batalla, Barcelona, Ariel, 2011, p. 296.

Conferencia de Prensa de la Portavoz del Ministerio de Relaciones Exteriores, 07-05-2013. http://www.embajadachina.es/esp/fyrth/t1038739.htm.

Consejo de Seguridad Nacional, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

DARPA, The National Cyber Range: A National testbed for Critical Security Research. http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf.

Departamento de Defensa de los EE.UU, "Annual Report to Congress Military and Security Developments Involving the People´s Republic of China 2013". http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf.

Departamento de Defensa de los Estados Unidos, 25-10-2010. http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf .

Domestic Surveillance Directorate, Utah Data Center http://nsa.gov1.info/utah-data-center/index.html.

Keohane, RO, Nye, JS Power and Interdependence: Worlds Politics in Transition, Little, Brown, 1977.

Keohane, R.O., Nye, J.S., Power and Interdependence, Nueva York, Harper Collins, 1989.

MacAfee, En el Punto de Mira. "Las infraestructuras críticas en la era de la ciberguerra".http://resources.mcafee.com/content/EMEA_CIPreport_ES.

MANDIANT, APT1 Exposing One of China's Cyber Espionage Units, 2013, http://intelreport.mandiant.com/.

McAfee, Informe sobre Criminología Virtual 2009. "La era de la ciberguerra, casi una realidad".http://www.mcafee.com/mx/resources/reports/rp-virtual-criminology-report-2009.pdf.

Ministerio de Defensa Chino, 30-05-2013. http://eng.mod.gov.cn/Press/2013-05/31/content_4453733.htm.

Tesoro de los EE.UU, http://www.treasury.gov/resource-center/data-chart-center/tic/Documents/mfh.txt .

The Camberra Times, 10-04-2013. http://www.canberratimes.com.au/it-pro/security-it/cyber-attacks-hurt-chinas-credibility-us-official-20130410-2hkpc.html .
The New York Times, 08-06-2013. http://www.nytimes.com/2013/06/09/world/asia/obama-and-xi-try-building-a-new-model-for-china-us-ties.html?pagewanted=all&_r=0 .
The People´s Bank of China. Enhanced Cooperation for Financial Markets Development between China and Japan (25-12-2011), http://www.pbc.gov.cn/publish/english/955/2011/20111225173248498166576/20111225173248498166576_.html.
The Washington Post, 07-06-2013. http://articles.washingtonpost.com/2013-06-07/politics/39823657_1_president-obama-chinese-president-xi-jinping-obama-and-xi
The Washington Post, 28-05-2013. 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.
The White House, Executive Order-Improving Critical Infrastructure Cybersecurity. February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
Xinhua, 10-03-2013. http://news.xinhuanet.com/english/china/2013-03/10/c_132223206.htm.
Xinhua, 29-05-2013. http://news.xinhuanet.com/english/china/2013-05/29/c_132415053.htm.