



:: [portada](#) :: [Conocimiento Libre](#) ::

02-10-2013

Policías y piratas

Liberticidas en el ciberespacio

Higinio Polo

Rebelión

P { margin-bottom: 0.21cm; }

En diciembre de 2011, el gobierno norteamericano filtró a *The Wall Street Journal* que el Ejército chino estaba detrás de la mayoría de los piratas informáticos que se dedican al espionaje y que atacan las redes estadounidenses. Según esa información, repetida de inmediato por toda la prensa internacional, los piratas chinos habían robado información secreta en organismos gubernamentales norteamericanos y en entidades relacionadas con el Departamento de Defensa. Asesores del gobierno Obama, como James Andrew Lewis, del CSIS (*Center for Strategic and International Studies*, de Washington), basándose en informaciones de la NSA, llegaron a hablar del "trabajo sucio" realizado por esos piratas para el Ejército chino. Un mes antes, el responsable del *National Counterintelligence Executive* (NCIX) acusaba abiertamente a China y Rusia, en un informe presentado al Congreso norteamericano, de estar detrás del espionaje cibernético y de los *hackers* informáticos.

Esas denuncias se fueron repitiendo en los meses siguientes. En febrero de 2013, la empresa de seguridad *Mandiant* acusaba a una "unidad secreta" del Ejército chino de dirigir centenares de ataques informáticos a "organismos y empresas" norteamericanas. El informe, que había sido encargado por *The New York Times*, entre otros, revelaba que, desde el barrio de Pudong, en un "edificio de doce plantas de Datong Road", en Shanghái, la "Unidad 61398 del Ejército Popular de Liberación" chino, que dispone de miles de empleados expertos en gestión de redes informáticas y que dominan el inglés, había asaltado y robado enormes cantidades de información en los Estados Unidos, penetrando en numerosos organismos e instituciones; entre ellas, infraestructuras estratégicas como la red de energía eléctrica. También se acusaba a esa supuesta unidad secreta del ejército chino de haber atacado al *New York Times* y al *Wall Street Journal*, además de a Twitter. Para hacer más contundente y creíble la denuncia, el *New York Times* aseguraba que los piratas habían penetrado en los ordenadores de cincuenta y tres empleados suyos, y robado información y claves... después de que el periódico publicase informaciones sobre la supuesta fortuna de la familia del anterior primer ministro chino, Wen Jiabao. Entre la maraña de noticias alarmistas, la agencia Reuters concluía afirmando que la amenaza informática "se ha originado en China".

Unos meses antes, un informe del Congreso norteamericano calificaba a China como "la mayor amenaza del ciberespacio", mientras se divulgaban acusaciones al gobierno de Pekín sobre supuestos ataques informáticos realizados contra la empresa de armamento y aeroespacial *Lockheed Martin*, el Pentágono e incluso compañías como Coca-Cola y Google, y el propio Obama anunció, con preocupación, que "países extranjeros" estaban atacando secretos industriales norteamericanos. La insinuación sobre la responsabilidad china fue lanzada al mundo y convertida en una acusación en toda regla contra Pekín. En esos días, portavoces del gobierno chino fueron interpelados por la prensa internacional sobre la noticia de que China también había lanzado ataques cibernéticos a Alemania, y, poco después, circularon informaciones sobre otros asaltos informáticos chinos a miles de ordenadores, así como cadenas de televisión y bancos en Corea del Sur.



De nada sirvió que Pekín negase las acusaciones, y que un portavoz oficial del gobierno chino manifestase que, contrariamente a las noticias difundidas, su país era una víctima de esa piratería y que, precisamente, la gran mayoría de esos ataques procedían de Estados Unidos. En febrero de 2013, el secretario de prensa de la Casa Blanca, Jay Carney, informó de los "reiterados ataques cibernéticos" (sin acusar directamente a China, pero dando por sobrentendida su responsabilidad), así como de la aprobación de un decreto que otorga poderes especiales a Obama "para responder a los ciberataques". En su comparecencia, Carney, siempre sin realizar acusaciones directas, se hizo eco de la alarma ante posibles sabotajes chinos a la red eléctrica norteamericana, al tráfico aéreo, a la distribución de agua, a empresas estratégicas y entidades financieras, y de la imprescindible protección de los secretos nucleares, como había hecho Obama. La exigencia de que China respetase la "legalidad internacional" fue lanzada de nuevo al mundo. Para remachar el clavo, un informe del Pentágono sobre la capacidad militar china, presentado al Congreso en mayo de 2013, indicaba que los ataques cibernéticos contra Estados Unidos "parecen provenir del gobierno y el ejército chino", al tiempo que acusaba a Pekín de espionaje industrial y de atacar las redes informáticas militares norteamericanas.

A principios de mayo, noticias difundidas por la agencia *Bloomberg*, y reproducidas por la prensa internacional, daban cuenta de que piratas informáticos chinos habían conseguido "robar secretos militares vitales" en Estados Unidos. A mediados del mismo mes, de nuevo *The New York Times* publicaba una destacada noticia, basada en "fuentes del gobierno" norteamericano y en "expertos en seguridad", según la cual la sección secreta del ejército chino (*Unidad 61398*) a quien, meses atrás, se había hecho responsable del espionaje, había vuelto a "atacar empresas estadounidenses". En un alarde de honradez y virtud, responsables del gobierno norteamericano declararon que, si bien esperaban que la denuncia pública de la piratería china hecha en febrero avergonzase al gobierno de Pekín, y llevase al desmantelamiento de la unidad 61398, el hecho de que ésta hubiese recuperado su actividad "no les había sorprendido". La maldad y falsedad chinas se daban por supuestas: el mundo se enfrentaba al peligro de los piratas orientales.

Pese a la gravedad de las denuncias, la presión no había terminado. A finales de mayo, *The Washington Post* informaba de que piratas chinos habían conseguido documentos de los *escudos antimisiles* norteamericanos previstos para Asia, Oriente Medio y Europa. Según el diario, un informe del *Defence Science Board* (DSB, un comité de expertos civiles que asesora al Departamento de Defensa) revelaba que, además, los piratas se habían apoderado de información vital del más moderno y costoso armamento norteamericano, como el caza F-35. El informe concluía que el Pentágono tenía serias deficiencias para hacer frente a esos ataques cibernéticos y para responder a un conflicto global. La mezcla de informaciones alarmistas, acusaciones veladas a China, filtraciones periodísticas calculadas y medias verdades, configuraba un preocupante escenario para Estados Unidos, que, así, debía hacer frente al habitual juego sucio de Moscú, y, sobre todo, de Pekín.

De nada había servido que, en febrero de 2013, el gobierno de Pekín hiciese público que miles de sitios chinos habían recibido ataques, entre ellos instituciones del gobierno, centros militares y empresas estratégicas, como, de hecho, les constaba a los servicios secretos norteamericanos y a la propia Casa Blanca; y, tampoco, que se hubiera conocido que Estados Unidos era el responsable del ataque al programa nuclear de Irán con el virus *Stuxnet*, en una operación ordenada personalmente por Obama en el verano de 2010. La central nuclear iraní de Natanz fue atacada con el virus, dejando inactivas a centenares de centrifugadoras. Fuentes de los servicios secretos norteamericanos consideraron que el programa nuclear iraní había sido retrasado dos años.



En ese momento, para desesperación de los servicios secretos norteamericanos, es cuando estalla la bomba activada por un desconocido, Edward Snowden. *The Guardian* y *The Washington Post* publican, el 7 de junio de 2013, informaciones que demuestran que Estados Unidos dispone de un vasto programa de espionaje informático en todo el mundo, PRISM, que había robado millones de mensajes y conversaciones telefónicas en China, y penetrado en los ordenadores de *Pacnet*, una empresa de Singapur y Hong-Kong propietaria de cables submarinos de fibra óptica en Asia. Igual había hecho en otras partes del mundo: en Rusia, Brasil, Oriente Medio, incluso en la Unión Europea, que había sido espiada con la instalación de micrófonos ocultos en sus sedes y con la infiltración en las redes informáticas. Los agentes de la NSA, *National Security Agency*, llegaron a utilizar las instalaciones de la OTAN en Bruselas para espiar a sus propios aliados. Las revelaciones mostraban que todos los ciudadanos, en cualquier lugar del mundo, estaban expuestos a la intromisión de un silencioso y siniestro fiscalizador que podía llegar a los rincones más privados de sus vidas. Pese a las tímidas protestas de algunos gobernantes europeos, la mayor parte de los analistas independientes subrayaron su convicción de que los gobiernos europeos, tanto en Alemania como en otros países, habían facilitado el trabajo de la NSA: la petición de explicaciones de la Comisión Europea apenas fue el cumplimiento de una penosa obligación sin mayores consecuencias. Europa daba la exacta dimensión de su vasallaje ante Washington.

Las revelaciones de Snowden, que había huido a Hong-Kong, eran de una gravedad inusitada, y, aunque el responsable de la NSA, el general Keith Alexander, justificó el programa de espionaje norteamericano afirmando que se habían evitado múltiples ataques terroristas, la denuncia mostraba al mundo la sistemática violación por parte de Estados Unidos de su propia Constitución (el ex analista de la CIA hizo referencia a la cuarta y quinta enmiendas), de la Carta de las Naciones Unidas y de la Declaración Universal de Derechos Humanos, además de numerosos acuerdos internacionales, organizando un oscuro poder ajeno a cualquier control democrático: la distopía de Orwell, tantas veces utilizada en el pasado contra la Unión Soviética y ahora contra China, llegaba de la mano de los hipócritas defensores de los derechos humanos radicados en Washington. Snowden reveló también que la NSA había pirateado ordenadores en China desde 2009, tanto en organismos gubernamentales, como en empresas y universidades. Para añadir gravedad a la denuncia, se constató la complicidad de las grandes compañías de Internet (Microsoft, HP, Apple, Google, Facebook, Twitter, Yahoo!, servicios de Skype, You Tube, etc) con el programa de espionaje norteamericano, que puede acceder a los servidores de esas empresas: la información de las redes sociales, las comunicaciones privadas de los ciudadanos, las claves de sus cuentas, sus actividades, incluso sus recorridos urbanos más anodinos podían ser espiados y fiscalizados a través de las compañías de Internet y de las empresas de telefonía. El gobierno estadounidense se había reservado, además, los mecanismos necesarios para obligar a cualquier empresa a entregar información privada de sus clientes. De esa forma, centros de escucha, procesamiento y espionaje como el situado en la estación de la RAF en Menwith Hill, Yorkshire, y los situados en Bude, en la península británica de Cornwall; en Cheltenham, también en Gran Bretaña, así como en Chipre y en la isla británica de Ascensión, en el océano Atlántico, y otros, almacenan millones de llamadas, mensajes y comunicaciones de todo tipo.

Como si fuera una ironía de la historia, el mismo día en que se publica la denuncia de Snowden, Obama se reúne con Xi Jinping en la residencia de Sunnylands, California. Durante la entrevista, el presidente norteamericano, en un escalofriante ejercicio de hipocresía, avisa a su homólogo chino de que las relaciones entre los dos países peligraban si China "no detenía sus ciberataques". La advertencia de Obama fue comunicada a la prensa por el consejero de seguridad nacional, Tom Donilon, cuando aún no había llegado la onda expansiva de la desertión de Snowden y de la enorme gravedad de sus revelaciones. La huida de Snowden a Hong-Kong, primero, y a Moscú, después, crea una complicada situación estratégica donde Estados Unidos intenta por todos los medios detener al antiguo analista de la CIA y la NSA, mientras consigue calmar a sus aliados



Europeos, mezclando persuasión, chantaje y forzada solidaridad entre los socios atlánticos, e intenta detener el golpe y gobernar la difícil situación creada en sus relaciones con Pekín y Moscú. Pese a la evidencia de la hipocresía de Estados Unidos, su gobierno no renuncia a poner el foco en Snowden: es un desertor, un delincuente, y debe someterse a la ley. Con su habitual altanería, Washington exige la entrega del traidor, y amenaza a los países que pretendan acoger a Snowden.

Mientras tanto, la maquinaria propagandística estadounidense se esfuerza por fabricar una explicación favorable a sus intereses, que haga olvidar, una vez más, su responsabilidad. En Washington creen que, si las mentiras sobre las "armas de destrucción masiva" en poder de Iraq habían sido casi olvidadas, pese a haber sido la excusa para declarar una guerra que ha causado centenares de miles de muertos, también la bomba de Snowden podía ser desactivada, con una mezcla de información adecuada, presión diplomática, mentiras, amenazas y chantajes, y, al mismo tiempo, jugando con las necesidades estratégicas de Pekín y Moscú, cuyos intereses no pasan hoy por un enfrentamiento directo con Estados Unidos. Así, Dick Cheney, vicepresidente con Bush, acusó a Snowden de "espionar para China", imputación que fue rechazada por el ex analista negando que hubiese compartido información con Pekín ni con Moscú. Pese a ello, los responsables norteamericanos filtraban a la prensa internacional sus sospechas acerca de la curiosa coincidencia de la denuncia de Snowden y el encuentro entre Obama y Xi Jinping, que habría servido para desactivar las acusaciones norteamericanas a China. Las sospechas recaían sobre Snowden, el foco de la atención mundial no debía ser el escandaloso espionaje norteamericano, sino la traición de un desertor, que debía ser entregado a la justicia de su país.

Snowden, convertido en el refugiado político más célebre del mundo, corre serios riesgos, como le ha ocurrido al soldado Bradley Manning por las revelaciones a *Wikileaks*. Frente a la tesis norteamericana de que Snowden ha incumplido su obligación y se ha convertido en un traidor a su país, lo que justificaría su detención y castigo, se alza la interpretación de los organismos de defensa de los derechos humanos de la propia ONU que mantienen que una persona que ha revelado información que atenta contra los derechos humanos debe ser protegida y asilada en el país que decida acogerlo. Sin embargo, el incidente con el avión presidencial de Evo Morales, desviado y retenido a la fuerza en Viena por las decisiones de Francia, Italia, España y Portugal, tomadas, sin duda, a instancias de Estados Unidos en una clara vulneración del derecho internacional, muestra la difícil situación del antiguo analista de la CIA, y la cacería decretada por Washington. No puede descartarse, incluso, su asesinato extrajudicial, si el gobierno norteamericano considerase que podría asumir el inevitable coste político que supondría. En pocos países del mundo puede estar seguro el ex analista, y Rusia es uno de ellos. Además, Snowden habría entregado a algunos periodistas buena parte de la información en su poder, según afirmó Glenn Greenwald, su contacto con *The Guardian*.

Todos los gobiernos intentan controlar a sus ciudadanos, con groseras intromisiones en la vida privada, pero el peligro del gigantesco programa revelado por Snowden, y la violación del derecho internacional, de los acuerdos entre países, de la propia Constitución norteamericana, es que constata que no se ha detenido la peligrosa deriva totalitaria de Estados Unidos, por más que sus defensores insistan en que ese vértigo no es real. Porque lo cierto es que ningún otro país del mundo ha diseñado y llevado a cabo un programa de espionaje y control semejante. Si a ese



peligroso poder, ajeno a cualquier control democrático, añadimos las iniciativas lanzadas por Washington en los últimos años, como el tribunal secreto (amparado por el FISA, *Foreign Intelligence Surveillance Act*) para autorizar registros y llamadas, las cárceles secretas levantadas en distintos países, los vuelos secretos de la CIA para trasladar a prisioneros políticos, las ejecuciones extrajudiciales ordenadas por el presidente, la letal actividad de los *drones*, los bombardeos selectivos sobre población civil, y los escuadrones de asesinos profesionales del ejército norteamericano preparados para actuar en cualquier lugar del mundo, rasgos todos ellos que sólo Estados Unidos ha desarrollado, no puede más que concluirse que el mundo enfrenta un siniestro Gran Hermano, dueño de la vida y de la muerte.

Pese a la gravedad de la situación, China no quiere iniciar un enfrentamiento abierto con Estados Unidos, aunque no por ello renuncie a forzar acuerdos que limiten el predominio norteamericano en el ciberespacio. Moscú, convertido ahora en refugio de Snowden, tampoco quiere dañar sus relaciones con Washington, lo que explica las palabras de Putin ligando la concesión de asilo al ex analista de la NSA a su compromiso para "no dañar los intereses de Estados Unidos", pero, al mismo tiempo, el gobierno ruso es consciente de que no puede entregar a Snowden, so pena de que Rusia aparezca ante el mundo como un país incapaz de resistir las presiones norteamericanas. Moscú conoce los riesgos que corre: no en vano, el programa de espionaje norteamericano consiguió capturar las conversaciones telefónicas de Putin con ocasión de la cumbre de 2009; sin olvidar que las represalias norteamericanas ya han comenzado: a finales de julio de 2013, el Departamento de Estado hacía público un informe sobre los acuerdos de control de armamentos donde afirmaba que Rusia incumple la *Convención sobre prohibición de armas bacteriológicas*, la *Convención sobre armas químicas*, y el *Tratado sobre fuerzas convencionales en Europa*, FACE, aunque, interesadamente, el informe estadounidense omitía que Washington todavía no ha ratificado el *Tratado para la prohibición de pruebas nucleares*, pese a sus promesas de hacerlo, repetidas durante años. Por su parte, también a finales de julio, el Senado aprobaba una propuesta presentada por Lindsey Graham, un senador republicano de Carolina del sur, estableciendo que si un país otorgaba asilo político a Snowden, el secretario del Departamento de Estado consideraría, junto al Congreso, las represalias que adoptaría el Senado. El mensaje iba dirigido a Moscú.

Rusia y China reclaman una regulación internacional para las comunicaciones en el ciberespacio, pero se niegan a aceptar que esa regulación sea dictada desde Washington: la piratería en el ciberespacio, la capacidad de control de Estados Unidos y la consolidación de un gigantesco poder en la sombra, nos acercan a la distopía orwelliana. Piratas y policías norteamericanos patrullan el ciberespacio y destruyen la libertad: ahora, los ciudadanos saben, sin asomo de dudas, que si la información está en poder de los Estados Unidos, no está precisamente en buenas manos.

Rebelión ha publicado este artículo con el permiso del autor mediante una [licencia de Creative Commons](#), respetando su libertad para publicarlo en otras fuentes.