ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

37/2012 23 abril de 2013

*Miguel A. Benedicto Solsona**

EEUU ANTE EL RETO DE LOS CIBERATAQUES

EEUU ANTE EL RETO DE LOS CIBERATAQUES

Resumen:

El ciberespacio es como el salvaje Oeste donde no hay reglas ni fronteras y es fácil cometer delitos y huir. Los gobiernos y empresas sufrieron en 2012 alrededor de 30.000 ataques. El supuesto apoyo del Ejército chino a un centenar de ciberataques frente a EEUU supone un grave desafío para la seguridad y la economía del país además de abrir una guerra fría entre ambas potencias. Obama no ha dudado en actuar mediante decreto para poner coto al ciberespionaje de la propiedad intelectual y evitar ataques frente a las infraestructuras vitales de EEUU. La ciberguerra se ha convertido en una de las claves de la bóveda defensiva norteamericana.

Abstract:

Cyberspace is like the Wild West where there are no rules or boundaries and it is easy to commit crimes and flee. Governments and businesses suffered in 2012 about 30,000 attacks. The Army alleged support a hundred Chinese cyberattacks against U.S. poses a serious challenge to the security and economy of the country as well as opening a Cold War between the two powers. Obama has not hesitated to act by decree to curb cyberespionage on intellectual property and avoid attacks against U.S. critical infrastructure. Cyberwar has become a key of U.S. defensive dome.

Palabras clave:

Estados Unidos, ciberguerra, China, Irán, Stuxnet, Flame, ataque cibernético, Obama, hacker, Zero Day, Rusia.

Keywords: U.S. cyberwar, China, Iran, Stuxnet, Flame, cyber attack, Obama, hacker, Zero Day, Russia.

INTRODUCCIÓN

Los supuestos ataques cibernéticos desde China con apoyo de una unidad secreta del Ejército Popular de Liberación han activado todas las alarmas en los EEUU.

La empresa Mandiant denunció el pasado 19 de febrero que *hackers* chinos, que acosan los sistemas informáticos de países occidentales, están vinculados a las fuerzas armadas del gigante asiático. En su informe aseguraba que los *hackers* de la Unidad 61398 han robado proyectos tecnológicos, estrategias de negociación y procesos industriales de más de un centenar de empresas durante los últimos 6 años.

Los *hackers* también accedieron a los sistemas de una empresa de defensa de EE UU y penetraron en una compañía que ayuda a gestionar la red eléctrica y los oleoductos de Norteamérica.

Estos ataques, según el gobierno de EEUU, suponen un grave desafío para la seguridad y para la economía del país. Además se producen en un momento de intento de cooperación entre las dos grandes economías del mundo por su interdependencia mutua.

La Casa Blanca anunció que tomará las medidas necesarias frente a ese desafío y pidió al Congreso una legislación más eficaz para hacer frente al peligro de la ciberguerra. Por su parte, el presidente Obama anunció, antes de pronunciar el discurso del Estado de la Unión, un decreto que le otorga poderes para responder a los ciberataques si lo cree necesario.

LA CIBERGUERRA

Se puede considerar a la ciberguerra como el conjunto de acciones que se realizan para producir alteraciones en la información y los sistemas del enemigo, a la vez que se protege la información y los sistemas del atacante. También se la puede denominar como guerra encubierta. En principio, los ataques informáticos no son considerados como ataques armados.[1] Sin embargo, Estados Unidos estudia una dura legislación que podría incluir los ciberataques en el listado de acciones consideradas como un acto de guerra, quizá con la vista puesta en sus infraestructuras críticas para la seguridad nacional. El ciberespionaje puede dañar a las empresas pero los riesgos del cibersabotaje pueden ser peores. Por ejemplo, los sistemas de control industrial son en gran parte controlados por ordenador. Organizaciones terroristas podrían causar un daño físico y económico importante a refinerías, plantas de energía, sistemas de agua, tuberías y otros sin dejar un rastro muy marcado.

1 Argumosa, Jesús. La Ciberguerra: Guerra Fría en el S. XXI. 27 febrero 2013. Atenea Digital.

Europa, por su parte, ultima una estrategia común a través de la Comisión Europea para protegerse, mientras Alemania y Francia se plantean aprobar leyes que obliguen a las empresas atacadas a informar a las autoridades.[2]

El Zero Day

La ciberseguridad ha sido un problema para la seguridad nacional de EEUU desde la década de 1990, pero la respuesta ha sido ad hoc y reactiva, marcada por la incertidumbre sobre cómo hacer frente a un problema nuevo e importante para la seguridad internacional. Hasta que llega un Día Cero que infunde miedo en la inteligencia militar y en las grandes empresas. El término es utilizado por los piratas informáticos y especialistas en seguridad para describir un defecto descubierto por primera vez por un hacker que puede ser explotado para entrar en un sistema e infectarlo.

Los impulsos electrónicos que llevan los datos se mueven a la velocidad del rayo. Una ida y vuelta entre Washington y Pekín a través de la red se produce en un tiempo mínimo. No importa donde se encuentren los hackers físicamente. En el ciberespacio, piratas, terroristas y ciberguerreros pueden operar prácticamente al lado de la gente común y navegar por la World Wide Web, enviar correos electrónicos o mensajes telefónicos.

Las empresas son muy frágiles, buscan el beneficio y se paran a pensar como hacer su software perfecto. Muchas de estas vulnerabilidades están relacionadas con errores en el código diseñado para analizar, clasificar, o archivos de datos enviados a través de Internet.[3]

Los organismos gubernamentales que participan en operaciones secretas de hacking, junto con algunos fabricantes de software afectados, compran información sobre Zero Days en el mercado negro, según los especialistas en seguridad[4].

En 2005, una empresa de seguridad llamada TippingPoint comenzó a ofrecer recompensas a los investigadores. Desde entonces, más de 1.600 personas han sido remuneradas por informar de casi 5.000 días cero. Un *hacker* de Shanghai, llamado Wu Shi, ganó cerca de 300.000 dólares por advertir de más de 100 errores en los navegadores Web. El sistema parecía ideal, excepto por una cosa: los fabricantes de software a menudo no suelen hacer caso a las advertencias.

2Araújo, Heriberto y Cardenal, Juan Pablo. Avanzadilla china en la ciberguerra. El País. 23 febrero 2013

3Hype and fear. The Economist. 8 diciembre 2012

4***O'Harrow Jr., Robert.*** **Understanding cyberspace is key to defending against digital attacks.** Washington Post. **3 junio2012**

Infraestructuras vitales

El comité de Asuntos de Espionaje de la Cámara de Representantes de EEUU ha calculado que los robos en Internet de secretos comerciales y propiedades intelectuales, en su gran mayoría dirigidos por China, le han costado a EEUU más de 300.000 millones de dólares en 2012.

Pero esta ciberguerra tiene otro flanco, que Obama recordó en su discurso sobre el Estado de la Unión y que afecta a la seguridad del país y de los ciudadanos: el riesgo de penetración en sistemas como los de la energía eléctrica, el agua potable o el tráfico aéreo, entre otros cuya interferencia podría generar pánico y caos. La Casa Blanca quiere regular la actividad en el ciberespacio para proteger ciertos puntos vitales de la infraestructura de EE UU.

Los temores sobre la vulnerabilidad de las sociedades occidentales a los cibertaques han crecido. Los líderes políticos y militares no pierden ninguna oportunidad para declarar que la ciberguerra ya está sobre nosotros. El ex secretario de Defensa de EEUU, Leon Panetta, habló de una "ciber-Pearl Harbour". Un alto funcionario dijo en privado que un ciberataque contra Estados Unidos podría ser peor que el 11-S con la explosión de refinerías de combustible, redes eléctricas o el caos del tráfico aéreo.

La realidad actual es un sin número de ataques anónimos a los gobiernos y las empresas con el fin de robar extensiones de valiosos datos comerciales o de seguridad. Algunos expertos creen que tales robos han costado cientos de miles de millones de dólares en I+D. Muchos de estos ataques son puramente criminales, pero en los más sofisticados suele haber Estados detrás aunque es muy difícil demostrarlo.

China, el más activo

China es el transgresor más activo. Emplea a miles de ingenieros de software con talento que se dirigen a las grandes compañías mundiales. En 2009, investigadores canadienses descubrieron una red de espionaje ciberglobal controlada en gran parte por servidores en China. Los objetivos militares y políticos cuyas redes se monitorearon - incluyendo el gobierno tibetano en el exilio y la oficina del Dalai Lama - sugieren un importante papel de China en la operación. Entre los 1.295 ordenadores infectados en 103 países, varios pertenecían a la agencia Associated Press en Londres, según los investigadores del grupo SecDev y el Centro Munk de Estudios Internacionales de la Universidad de Toronto.

En febrero de este año, la empresa Mandiant descubrió que la mayor parte de las poderosas instituciones de Washington han sido penetradas por ciberespías chinos. La lista de los hackeados en los últimos años incluye firmas de abogados, bancos, centros de investigación, medios de comunicación, grupos de derechos humanos, contratistas, oficinas del Congreso, embajadas y agencias federales. Con esa información se puede comprender como funciona y se ejerce el poder en Washington. La única pregunta es si los chinos

tienen los recursos para analizarla.

El Gobierno de Pekín niega toda implicación en unos ataques que pueden ser redirigidos desde cualquier parte del mundo a través de internet, mientras que EEUU ha dado pasos para fortalecer su industria de vanguardia dando a entender sutilmente que China consiente violaciones de su seguridad nacional y de sus empresas.

Según Jeffrey Carr, fundador de la empresa de ciberseguridad Taia Global, está claro que en China se originan un gran número de ataques porque no hay leyes ni una cultura de protección de la propiedad intelectual, pero los chinos no son los únicos. "El informe de Mandiant crea un precedente peligroso. Pese a que China es un claro sospechoso, no se puede acusar sin pruebas definitivas al Ejército Popular, eso implicaría el riesgo de una escalada", asegura Carr,

Uno de los problemas es que este conflicto llega en un pésimo momento político. La llegada al poder en Pekín de Xi Jinping era vista por EEUU como una oportunidad para un periodo de mayor cooperación. Difícilmente ocurrirá eso si Obama plantea de inmediato un asunto tan controvertido como el de los ciberataques. Además, es improbable que el nuevo presidente empiece su mandato con una concesión a EE UU en ese terreno.

Según un informe de 2012 de Symantec y Mcafee, el país que más ataques de malware o virus realiza en el mundo es Estados Unidos, seguido de China y estos dos superpotencias son también las que están a la cabeza de la lista de víctimas.

Pero países como Rusia, Israel o Francia son también muy activos en ciberespionaje tanto industrial como gubernamental. "Tenemos a más de 30 países desarrollados y emergentes aumentando día a día sus unidades militares de ciberespionaje, todas las grandes agencias de inteligencia están implicadas", indica Carr.

Los otros estados que más emplean los ciberatques son Rusia y, recientemente, Irán (que fue la presunta fuente del virus Shamoon que afectó a miles de de ordenadores de Aramco en Arabia Saudita y Qatar RasGas). El gobierno de Teheran también podría estar detrás de los ataques que han sufrido 30 grandes bancos mundiales, en su mayoría estadounidenses, destinados a cerrar sus sitios web. Los hackers intentan sobrecargar el tráfico en internet para frustrar a los clientes a la hora de utilizar los servicios en línea de bancos como JPMorgan Chase, Wells Fargo, Citigroup y PNC.

Por último, Corea del Norte también podría haberse apuntado a esta moda en el supuesto ataque que el pasado mes de marzo paralizó los dos grandes bancos y las cadenas de televisión de su vecino del Sur[5].

5Petersen F.; Cain G. North Korea suspected of mounting cyberattack that shuts down South Korean banks, TV stations. CNN 20 Marzo 20123

El Ciberespacio: nuevo dominio de guerra

El Pentágono ha declarado recientemente el ciberespacio como nuevo dominio de guerra. Las fuerzas de EE.UU. también han puesto en marcha secretamente ataques cibernéticos contra las instalaciones de enriquecimiento nuclear de Irán, para deshabilitar casi 1.000 centrifugadoras de uranio en 2009 y 2010.

Estados Unidos e Israel, según los expertos, estuvieron detrás del virus de Stuxnet, que fue diseñado para paralizar las centrifugadoras nucleares en Natanz y evitar el enriquecimiento de uranio. El ataque alertó al mundo sobre el verdadero potencial de los ataques contra la infraestructura crítica.

El New York Times informó de que Stuxnet fue parte de una operación encubierta de Estados Unidos e Israel contra Irán aprobadas por el presidente Obama. Stuxnet tenía como objetivo un ordenador de control de llamada de un S7 producido por Siemens y utilizada por el gobierno iraní para controlar las centrifugadoras en el proceso de enriquecimiento de uranio. El "gusano" fue lanzado en Internet y se extendió rápidamente en gran parte del mundo, como un virus durante la temporada de gripe. Pero la mayoría de las computadoras y los sistemas infectados se encontraban en Irán. El código del "gusano" fue diseñado para autorreplicarse.

Stuxnet aprovechó cuatro errores de software desconocidos o "días cero", para romper a través de la seguridad una variedad de sistemas informáticos. Los analistas creen que cientos de centrifugadoras fueron dañadas, aunque nadie fuera de la operación lo sabe con seguridad[6].
"Las implicaciones reales de Stuxnet están más allá de cualquier amenaza que hemos visto en el pasado", según los autores de un análisis del virus emitido por la empresa de seguridad informática, Symantec.

Grandes equipos de personas altamente cualificadas son necesarios para producir efectos de tipo Stuxnet, que pueden estar más allá de los grupos terroristas más sofisticados.

Duqu fue otro "gusano" construido en gran parte del mismo código que Stuxnet, pero se concentró en el espionaje en lugar del sabotaje, chupando los datos de los ordenadores que infecta. Y después apareció Flame, una nueva pieza de código malicioso que hace lo mismo que Duqu, pero parece ser aún más sofisticado. Este virus representa una escalada de una guerra cibernética preocupante que se libra entre los estados-nación[7].

Flame fue diseñado para atacar a Irán infectando ordenadores de su ministerio de petróleo y contra objetivos en Cisjordania, Siria y Sudán. Según los investigadores de Kapersky Lab, la

---

6 *O'Harrow Jr., Robert. Cyber Search Engine Shodan Exposes Industrial Control Systems to New Risks*. Washington Post . *June 3, 2012*

7 Flame. The Economist. 29 de mayo 2012

empresa de seguridad que descubrió Flame, el programa ha estado funcionando durante al menos un par de años. La mayoría de los ataques, que la compañía ha puesto al descubierto, se han dirigido contra ordenadores en Irán, aunque también otros países de Oriente Medio han sido blanco de ataques.

Flame parece abrirse camino en las redes a través de puertos USB y de impresoras. A continuación, se pone a transmitir todo, desde capturas de pantalla a los archivos de datos y conversaciones de audio (grabado mediante la activación de las computadoras integradas en los micrófonos) de vuelta a sus hackers.

MEDIDAS CONTRA LOS CIBERATAQUES

La gran mayoría de los virus que han tenido éxito podría haberse evitado con precauciones relativamente sencillas, como la actualización periódica de software. Sin embargo, muchas empresas no se molestan en tomar incluso las medidas más obvias para protegerse contra el robo de datos y las interrupciones del servicio, y mucho menos en equiparse para detener los ataques de alto nivel.

El reto para las autoridades es la manera de resolver ese problema, mientras se refuerzan las defensas de los ciudadanos contra los ataques cibernéticos cada vez más sofisticados.

Las políticas sobre la ciberguerra permanecen confusas y en secreto. El gobierno estadounidense trabaja en nuevas reglas y en una estrategia clara para hacer frente a las ciberamenazas.

La orden ejecutiva de Obama

Pese a que el número de ataques contra empresas de infraestructura crítica, según el Departamento de Seguridad de EE.UU. , creció un 52% en 2012; la legislación destinada a regular los ataques cibernéticos fracasó en el Senado el año pasado. Sobre todo se vio obstaculizado por los grupos empresariales que temían las onerosas regulaciones federales. Esto obligó al presidente Obama a decretar medidas para sofocar el ciberespionaje contra las agencias del gobierno de EE.UU. y empresas estadounidenses. La orden también pretende reforzar las defensas de la infraestructura crítica vulnerables a los ataques cibernéticos.

El presidente aprobó las nuevas directrices para las agencias federales que llevan a cabo las ciberoperaciones. La orden ejecutiva establece cómo deben ayudar a las empresas privadas, particularmente las responsables de la infraestructura nacional crítica, para defenderse contra las ciberamenazas mediante el intercambio de información y el establecimiento de normas.

El decreto es una respuesta al estancamiento de la *ciberley* en el Senado. Los republicanos argumentan que impone una carga excesiva de regulación a la industria, que ya está obligada a revelar cuando sufre un ciberataque. También regula hasta qué punto, organismos como el Departamento de Seguridad Nacional, pueden ir en defensa de las redes nacionales frente a los ataques de *malware*. La orden ejecutiva obliga a dicho Departamento a compartir información clasificada con las empresas acerca de los ataques que se cree que se producen o que están a punto de tener lugar.

Aun así el Congreso necesita hacer más. La Cámara tendría que levantar los límites federales sobre el intercambio de datos y ofrecer nuevas protecciones de privacidad. De momento ha tomado el camino que opone menor resistencia. El año pasado aprobó una ley para eliminar las barreras legales para que las empresas y el gobierno puedan compartir datos sobre hacks.

El decreto del presidente también pide que el Instituto Nacional de Estándares y Tecnología desarrolle un "marco de ciberseguridad práctica" dentro de un año, en torno a las normas de funcionamiento elegidas por la industria privada.

La característica más reseñable de la orden ejecutiva es un requisito para que los reguladores federales de la banca, plantas de energía y otros proveedores de infraestructuras críticas usen el nuevo marco para evaluar y, potencialmente, mejorar las actuales normas de ciberseguridad. Sin embargo, esas empresas son sólo una pequeña porción de los equipos que están en el punto de mira de los hackers. Más compañías deben intensificar sus esfuerzos de seguridad, y le toca al Congreso proporcionar una motivación que el mercado todavía no tiene.

El Pentágono debe estar preparado

La normativa refleja los crecientes temores del gobierno sobre las vulnerabilidades de los equipos que gestionan la infraestructura crítica de la nación. Panetta ya advirtió que podrían paralizar el país y que el Pentágono debe estar preparado. "Si un ciberataque se lanzara en contra de nuestra nación, el pueblo estadounidense debe ser protegido", dijo. "Y si el comandante en jefe da las órdenes de una respuesta, el Departamento de Defensa debe estar dispuesto a obedecer esa orden y actuar.", añadió el ex secretario de Defensa.

Detrás de esos miedos se esconde una realidad inquietante: las redes en los Estados Unidos seguirán siendo vulnerables a los ataques en el futuro inmediato, porque nadie entiende el ciberespacio lo suficiente como para garantizar la seguridad.

En las cuatro décadas desde que Internet comenzó, la mayoría de la investigación que se llevó a cabo sobre la ciberseguridad se hizo sobre la marcha o en el último momento, según los especialistas en seguridad. Ahora, con un mundo que une comunicaciones, infraestructura, ejércitos, bancos, médicos y otros sistemas a un ritmo vertiginoso; la

dinámica del ciberespacio se ha vuelto demasiado compleja y los avances de seguridad sólo están empezando.

Mientras tanto, los atacantes tienen una ventaja enorme. Pueden elegir el momento, lugar y forma de hostigar. En cambio, los agredidos casi siempre tienen que conformarse con reaccionar, haciendo correcciones después de que el daño ya está hecho.

Por eso se crean herramientas como CyberCity[8] que pretende preparar a los piratas informáticos del gobierno para mantener su posición hasta que a largo plazo se pueden encontrar soluciones. CyberCity es un entorno virtual, que recrea una ciudad y su infraestructura crítica, lanzado en los últimos años por los investigadores militares, empresariales y académicos para hacer frente los increíbles retos de seguridad que plantea el ciberespacio, donde millones de ataques o intrusiones ocurren todos los días.

Aun así, la creación de entornos virtuales realistas es extraordinariamente difícil. En el ciberespacio, más de 2.000 millones de personas interactúan con al menos 12.000 millones de computadoras y dispositivos, incluidos los sistemas de posicionamiento global, los teléfonos móviles, satélites, equipos de uso normal y computadoras de control industrial que gestionan las centrales eléctricas o los sistemas de agua.

El Pentágono quiere reforzar al CiberComando con 4.000 empleados más y también trabaja en normas más permisivas de combate ofensivo para la guerra cibernética, por ejemplo, para cerrar un servidor extranjero del que se piense que emana un ataque. El CiberComando y la Agencia de Seguridad Nacional han pedido una mayor flexibilidad para atacar al "enemigo" y se encargarían de la protección de las infraestructuras críticas. La aparición de nuevas doctrinas de ciberguerra en los Estados Unidos está siendo observada de cerca tanto por los aliados como por los potenciales adversarios.

Por lo tanto, aunque abundan las preguntas, las respuestas son pocas. Por ejemplo, no está claro cuánta información sensible sobre amenazas y vulnerabilidades de las agencias del gobierno deben compartir incluso con empresas del sector privado que son cruciales para la seguridad nacional. También es polémico el equilibrio entre la defensa y el ataque. En la guerra cibernética, el atacante tiene la ventaja. Establecer reglas para la ofensiva de la ciberguerra es muy difícil.

El Director de Inteligencia Nacional, James Clapper en su informe anual sobre las amenazas que enfrenta Estados Unidos, presentado al Congreso el pasado mes de marzo, destacó las cibernéticas. "La destrucción puede ser invisible, latente y progresiva", señaló[9] . Según el informe, Internet es cada vez más utilizado como una herramienta tanto por las naciones

8 O'Harrow Jr., Robert. CyberCity allows government hackers to train for attacks. Washington Post. 27 noviembre 2011

9 Carter, Benson and Castillo. Official: Cyberattacks, N. Korea, jihadist groups top U.S. Threats. CNN 13 marzo 2013.

como por los grupos terroristas para lograr sus objetivos. Sin embargo, califica como de "remota posibilidad" un ataque cibernético importante en los Estados Unidos que cause alteraciones generalizadas, como cortes de energía regionales. La mayoría de los países o grupos no tienen la capacidad para llevarlo a cabo, concluye el informe.

Aun así, hay que mejorar la seguridad de la infraestructura crítica nacional, como las redes de energía, el alcantarillado o los sistemas de transporte. Pero estos objetivos no son tan vulnerables como ahora se suele sugerir. Por ejemplo, Stuxnet destruyó quizás una décima parte de las centrifugadoras en Natanz y retrasó algunas de enriquecimiento de uranio durante unos meses, pero fueron reparadas pronto. Su éxito limitado y efímero también ha llevado a Irán a tomar medidas para impedir futuros ataques. Si eso es lo mejor que dos potencias cibernéticas como EEUU e Israel pueden hacer frente a una potencia industrial de tercera categoría; pone en entredicho las predicciones más alarmistas de inminentes ciberataques contra infraestructuras en Occidente[10].

Además, como explica Nigel Inkster del Instituto Internacional de Estudios Estratégicos, pone de relieve el enorme riesgo para el agresor de llevar a cabo un ataque a una infraestructura teniendo en cuenta las consecuencias en caso de que se detecte. Como ya advirtió Leon Panetta los agresores potenciales deben ser conscientes de que los Estados Unidos tiene la capacidad para localizar y exigirles responsabilidades por las acciones que dañan los intereses norteamericanos.
Por eso, como dice el investigador de Rand Corporation, Martin Libicki, es exagerado pensar que las guerras del futuro se llevarán a cabo en gran parte en el ciberespacio. Y es que la ciberguerra sólo puede ser una función de apoyo para otras formas de conflicto.

Una estrategia de ciberseguridad

Aun así no deben desdeñarse sus peligros y hay que tener preparada alguna estrategia como la que propone James Lewis[11] en un informe que identifica seis principios que deben guiar a los Estados Unidos en el desarrollo de un enfoque estratégico:

1. El ciberespacio no es un ambiente único. Los Estados se comportan en este entorno como lo harían en cualquier otro.
2. No podemos "desarmar" en el ciberespacio, y no habrá un "cero global" durante un ciberataque.
3. Se ha entrado en un período de crecimiento sostenido, donde los errores de cálculo y las percepciones erróneas de los adversarios son una fuente de riesgo para los

10 The Economist. Op. Cit.
11Lewis, James Andrew. Conflict and Negotiation in Cyberspace. Center for Strategic and International Studies. 8 febrero de 2013

Estados Unidos.

5. Los intereses de EEUU estarían mejor servidos mediante la incorporación del espionaje y el ciberataque al derecho internacional.
6. El objetivo inmediato de la negociación debe ser el aumento de los riesgos de lanzar un ciberataque o de participar en la actividad cibernética maliciosa para los enemigos estatales y no estatales.
7. Hay un límite en la reducción del riesgo; siempre habrá riesgo. El objetivo de EE.UU. debería ser disminuirlo como parte de sus esfuerzos más amplios para fortalecer la seguridad internacional.

CONCLUSIONES

El desarrollo de ciberarmas ofensivas y defensivas junto a los drones y las operaciones de las fuerzas especiales son la clave de la bóveda de la defensa de la administración Obama pese a los recortes presupuestarios. Los ataques a gobiernos y empresas en 2012 fueron alrededor de 30.000. Las compañías hackeadas sufrieron unas pérdidas entre el 1 y el 5% en el mercado de capitales. El saqueo de la propiedad intelectual que puede ayudar al desarrollo de las capacidades industriales o militares de un estado enemigo es inadmisible. Pero la gran incertidumbre proviene de las consecuencias que podría tener el ciberataque a las infraestructuras críticas del país. De ahí el decreto promulgado por Obama que implica que las agencias reguladoras deben desarrollar unos estándares de seguridad que se apliquen a esas infraestructuras vitales.

Habría que saber qué clase de ciberataque hay que recibir para que el presidente ordene un contraataque. No es lo mismo el robo de propiedad intelectual que cortar el agua potable o la electricidad de una ciudad, igual que no es similar una negociación, una sanción económica o un contraataque del Cibercomando del Ejército de los EEUU.

Washington estudia incluir los ciberataques en el listado de acciones consideradas como un acto de guerra, quizás con la vista puesta en las infraestructuras de carácter crítico para la seguridad nacional y no se descartan ciberataques preventivos sin una declaración de guerra previa.

No sólo la Casa Blanca debe liderar este proceso. Las empresas infravaloran el riesgo que afrontan si son hackeadas. Además es muy difícil de evaluar los daños por el robo de la propiedad intelectual, en algunos casos sólo se ven años después; en otros son inmediatos (tren alta velocidad, automóviles o turbinas de viento). El ciberespionaje o inocular un virus es una tarea fácil pues la mayoría de los casos requiere de técnicas básicas y las herramientas se adquieren fácilmente en internet. Sin embargo, el 90% de los ataques tienen fácil solución y se podrían haber evitado con un mínimo control dentro de las compañías.

Existen cerca de 50 millones de virus en la red y son detectados una media del 20%, algo que también se debe a la escasez de especialistas en ciberseguridad.

El ciberespacio es como el salvaje Oeste donde no hay reglas ni fronteras. Los hackers pueden cruzarlas sin miedo a ser castigados, pues hay países que toleran esas actividades. Sería conveniente llegar a un acuerdo internacional sobre la ciberseguridad, para que la ley impere sobre los tiros en el Ciberoeste, hasta donde sea posible.

[i]

*Miguel A. Benedicto Solsona**

Periodista e investigador del Instituto Franklin-UAH