¿Es posible un Pearl Harbor cibernético?

Iván Giménez Chueca

La ciberguerra está en boca de todo el mundo, para algunos será la causa de devastadores ataques en el futuro, mientras que para otros, supone una amenaza muy matizable.

En octubre de 2012 los principales medios de comunicación internacionales recogían unas palabras del entonces Secretario de Defensa de EE UU, Leon Panetta, donde alertaba de que el país afrontaba la amenaza de un Pearl Harbor cibernético, es decir, que un enemigo lanzará ciberataques contra infraestructuras críticas que causaran importantes pérdidas humanas, paralizara al país y creara sensación de vulnerabilidad y de inseguridad en la Red.

Más allá de las palabras de Panetta (quien no fue el primero en acuñar el término ya que se remonta a los 90), este pasado verano se produjo un ciberataque que supuso el robo de información sobre millones de trabajadores del Gobierno federal estadounidense. Una vez más, las sospechas recayeron sobre *hackers* chinos; y en los medios de EE UU se inició un debate sobre si se estaba ante el temido ciber Pearl Harbor. Cabeceras como *Los Angeles Times* o *USA Today*,

se mostraron a favor, considerando que la sustracción de los datos de los trabajadores públicos era un auténtico desastre. Mientras que *Washington Post* se mostró rotundamente en contra, y lo consideraba algo más propio de una operación de espionaje que de un acto de guerra.

Estas dos posturas reflejan el debate entre especialistas sobre hasta qué punto es posible que una acción desde Internet pueda causar daños realmente graves a infraestructuras sensibles en un país. En realidad, se puede considerar una faceta más de la discusión entre optimistas y pesimistas respecto al rol que tiene Internet en el mundo actual.

Los más alarmistas consideran que es cuestión de tiempo que se pueda desarrollar este tipo de gran ciberataque. Entre los partidarios de estos argumentos está Joseph Nye, politólogo neoliberal estadounidense, que defiende que la creciente dependencia de los países más avanzados en sistemas digitales complejos para sus actividades económicas y militares crea nuevas vulnerabilidades que pueden ser fácilmente explotadas en un escenario de ciberguerra.

Nye también apunta que en la Sociedad de la Información el poder se ha difuminado, y que Internet ofrece un territorio donde la hegemonía de los Estados tradicionales se ve cada vez más contestada por las organizaciones no estatales. En esta línea de pensamiento, se inscriben todas esas advertencias de que las operaciones de ciberguerra son mucho menos costosas que las acciones convencionales, lo que posibilita que estén al alcance de *Estados canallas* y de grupos armados.

Otra de las voces destacadas que advierten de los peligros de la guerra en Internet es Richard A. Clarke, responsable de contraterrorismo en las Administraciones de Bill Clinton y George W. Bush. En su libro de 2009 *Guerra en la Red* (escrito conjuntamente con Robert K. Knake, experto en ciberseguridad del Council on Foreign Relations) muestra el hipotético escenario de un ataque desde Internet que dañe infraestructuras claves de EE UU, y que ocasiona explosiones en refinerías y plantas químicas, accidentes en transportes y el colapso del sistema financiero. El resultado son miles de muertos, un país en *shock* y sin la posibilidad de determinar claramente quien es el responsable.

Escenarios de este perfil tan catastrófico lo suelen utilizar como advertencia los defensores de que es posible un ciber Pearl Harbor o un ciber 11-S, dependiendo de si la autoría es una potencia enemiga o un grupo terrorista. Pero tal y como reconocen Clarke y Knake en su libro, estas capacidades aún no están plenamente desarrolladas. Aunque, en la línea de Nye, también insisten en que países como Estados Unidos son muy vulnerables porque dependen en exceso del ciberespacio, tanto sus entidades públicas como privadas.

Por otro lado, hay otra línea de pensamiento entre expertos que considera que las capacidades

actuales de los países y de los grupos armados son muy limitadas para lanzar un ciberataque tan devastador. Uno de los autores que más matizan los efectos de esta forma de guerrear es Thomas Rid, profesor del Departamento de Estudios de la Guerra en el King College de Londres. En uno de sus trabajos más destacados, *Cyber War Will Not Take Place,* analiza los actos de ciberguerra siguiendo el pensamiento de Von Clausewitz, quien considera que un acto bélico debe ser violento (causar daño humano y/o material), instrumental (debe tener medios y un fin) y tener naturaleza política.

Para este académico, los ciberataques que se han registrado hasta la fecha no reúnen estos tres criterios, y deben verse como acciones más propias del ámbito del espionaje o del sabotaje, y no de un auténtico conflicto bélico, cita los ejemplos de las acciones en la Red contra Estonia y Georgia en 2007 y 2008 respectivamente, atribuidos a *hackers* rusos y con unos efectos limitados al robo o bloqueo de información en la Red.

En un línea similar se manifiesta otro experto como Peter W. Singer, investigador de Brookings Institution, y conocido por sus trabajos sobre los campos de batalla del futuro. Este verano ha publicado la novela *Ghost Fleet* junto a August Cole, investigador de Atlantic Council. El libro narra cómo China y Rusia lanzan un ataque sorpresa contra Estados Unidos combinando fuerzas convencionales con tácticas de ciberguerra.

Singer también se muestra muy crítico con quien habla alegremente de ciberguerra, y de un Pearl Harbor cibernético. En un artículo en Politico, apuntó que estos términos deberían ajustarse a acciones que implicasen una violencia masiva y con objetivos políticos de alto nivel, y no para acciones que supusieran el mero robo de información, o el bloqueo de algunas páginas web de manera temporal.

También cree que, a día de hoy, las armas y acciones propias de una ciberguerra tienen verdadera efectividad si se emplean en apoyo de acciones bélicas convencionales, como en su novela. En el citado artículo en Politico, pone el ejemplo de la Operación Orchard, cuando Israel bombardeó una planta atómica siria en 2007 para poner fin a un presunto e incipiente programa nuclear de Bachar al Assad. Los cazabombarderos hebreos pudieron violar el espacio aéreo del país árabe sin oposición porque la inteligencia israelí habrían conseguido *hackear* los sistemas de radar y antiaéreos del régimen de Damasco.

Tanto Rid como Singer también creen que para el desarrollo de unas capacidades realmente efectivas de ciberguerra hace falta disponer de los recursos de un Estado poderoso. Ambos analizan el caso de Stuxnet (el virus informático utilizado para sabotear la central nuclear iraní de Natanz, parte clave del programa atómico de Teherán), y consideran que esta operación no se habría podido llevar a cabo sin los recursos humanos y materiales de los que disponen Israel

y Estados Unidos, presuntos promotores del ataque. De igual manera, la propia debilidad militar del régimen de los ayatolás respecto a estos dos países le imposibilitó llevar a cabo una acción de represalia.

La respuesta a un ciber Pearl Harbor

Hasta ahora, otro punto que han esgrimido con frecuencia los más pesimistas es que si finalmente se produce un ciberataque de consecuencias devastadoras, sería muy difícil determinar la autoría del mismo. Además, consideran que la dificultad para identificar a la fuente agresora hace que la disuasión sea muy difícil de conseguir en la ciberguerra. Contrariamente, a lo que ha sucedido con el armamento nuclear, donde el temor a la destrucción mutua asegurada disuade a los posibles agresores.

Pero en abril de 2015, Estados Unidos presentó su nueva estrategia de ciberdefensa, donde por primera vez se hablaba claramente de establecer una disuasión, ya que el Pentágono asegura que cuenta con la capacidad para determinar la autoría de cualquier agresión que provenga de Internet, y establecer las represalias oportunas. Además, estima que para 2018 tendrá desplegados 133 equipos especializados en la guerra en la Red.

Además, esta línea de actuación también considera que es posible la “disuasión por negación”, es decir, crear unos sistemas defensivos que frustren *a priori* cualquier intento de agresión. En cuanto a las acciones ofensivas, se contempla desarrollar una capacidad para llevarlas a cabo, siempre y cuando se haga para “proteger los intereses de Estados Unidos”.

Esta nueva estrategia de ciberdefensa de Estados Unidos también aleja el riesgo del ciber Pearl Harbor. El Departamento de Defensa considera poco probable que haya un único ataque muy devastador, y sitúa el principal riesgo en las agresiones de bajo perfil pero continuas, y que realmente representan una amenaza de cara a la protección de información sensible.

Fecha de creación
7 diciembre, 2015