ieee.es
Instituto Español de Estudios Estratégicos

Documento
Informativo

13/2013 24 abril de 2013

Mª José Caro Bejarano

ALGUNAS REFLEXIONES SOBRE LA CIBERGUERRA

ALGUNAS REFLEXIONES SOBRE LA CIBERGUERRA

Resumen:

Los últimos ciberataques sobre Corea del Sur sirven de base para reflexionar sobre la posibilidad de enfrentarnos a una ciberguerra o si simplemente el ciberconflicto se emplea como un mecanismo adicional al conflicto convencional. Ante el ciberconflicto se necesita la colaboración público-privada, ya que muchos de los recursos objeto de ataque son propiedad o gestionados por el sector privado.

Abstract:

The recent cyber attacks on South Korea are the basis for considering the possibility of facing a cyberwar or whether cyberconflict is simply used as an additional mechanism to conventional conflict. Public-private collaboration is needed to face cyberconflict, as many of the targeted resources are owned or managed by the private sector.

Palabras clave:

Ciberguerra, ciberataque, ciberconflicto.

Keywords:

Cyberwar, cyberattack, cyberconflict.

ALGUNAS REFLEXIONES SOBRE LA CIBERGUERRA

Uno de los casos de riesgo planteados en la octava edición del Informe de Riesgos Mundiales (Global Risks 2013) presentado el pasado mes de enero por el Foro Económico Mundial (WEF[1]) se sitúa en el centro de una constelación de riesgos tecnológicos y geopolíticos que varían desde el terrorismo a los ciberataques y el fallo de la gobernanza global. Este caso se denomina "Incendio digital incontrolado en un mundo hiperconectado" sobre la desinformación masiva que se extiende vía Internet. Este riesgo examina cómo la hiperconectividad podría permitir un incendio digital que sembraría el caos en el mundo real. Este caso considera el desafío presentado por el uso equivocado de un sistema abierto y fácilmente accesible como Internet y el peligro mayor de los intentos equivocados de evitar tales resultados.

La semana pasada el presidente Barack Obama convocó a 15 de los principales líderes financieros de Estados Unidos a la Casa Blanca para discutir lo que su gobierno considera las amenazas que son más penetrantes, más persistentes y menos manejables - los ciber-riesgos.

Al contrario que con la amenaza nuclear, donde realmente unos gobiernos se enfrentaban a otros gobiernos, ahora "el sector financiero, las empresas y su conocimiento es un nuevo campo de batalla".

En este nuevo mundo, los ciberconflictos son una realidad, pero nadie ha escrito las reglas de cómo se debe gestionar la responsabilidad entre el gobierno y el sector privado.

A diferencia de las típicas crisis de seguridad nacional, el sector privado controla la mayor parte de los recursos que pueden resolver con decisión los ciberconflictos. El Gobierno mantiene la responsabilidad general de la ciberdefensa nacional, sin embargo, no ha desarrollado doctrinas de respuesta. Existe cierta limitación en la administración pública debido a sus procesos internos, intereses en competencia y la falta de experiencia en la solución de problemas de seguridad nacional, en colaboración con el sector privado.

Un grupo de destacados ciberestrategas realizó una simulación que ilustra la rapidez con que un ciberconflicto podría escalar desde unas tensiones iniciales hacia algo más serio. La reunión[2] demostró como a menudo la administración del gobierno y el sector privado no logran comunicarse de manera efectiva, o actuar en colaboración para hacer frente a una amenaza a la seguridad nacional que sólo se puede dominar juntos.

[1] Véase www.weforum.org. Global Risks 2013, eigth edition.
[2] La simulación fue convocada por el Atlantic Council y la empresa privada SAIC.

La simulación consistió en una DDoS o denegación de servicio distribuida sobre las instituciones financieras de Estados Unidos lanzada a principios de este año. Esos ataques siguieron el esquema de los ataques producidos el verano pasado que utilizó un código dañino para borrar los datos de unos 30.000 ordenadores de la empresa Saudi Aramco.

Esta cibersimulación permitió recoger, siguiendo el desarrollo de una situación ficticia, una serie de conclusiones y recomendaciones para reaccionar ante una situación de este tipo.

Entre las conclusiones destaca que, aunque con demasiada frecuencia, el gobierno quiere resolver los ciberconflictos por sí mismo, como hace en la mayoría de las crisis de seguridad nacional, en este tipo de escenario es imprescindible la colaboración con el sector privado. De hecho, son pocos los ciberconflictos en los últimos 25 años que se han resuelto de manera decisiva por los gobiernos, según expresa Jason Healey, el director de la Cyberstatecraft Initiative del Consejo Atlántico.

Para resolver la mayoría de las cibercrisis hay que combinar la agilidad y la experiencia del sector privado, el cual además, también por lo general, tiene acceso a los medios para hacerlo. El gobierno carece de estas virtudes, aunque conoce el contexto general del ataque y tiene enormes recursos de espionaje y de financiación, y controla los resortes del poder económico, diplomático y militar tradicional.

Estos últimos meses han demostrado que tales discusiones no son teóricas. El mensaje de Obama para el sector financiero fue claro: *Antes de que las cosas se pongan aún más serias, el gobierno y las empresas privadas en conjunto deben hacer más para prepararse para los inevitables ciberconflictos del futuro*.[3]

Por otra parte, el estudio de los recientes ciberataques a Corea del Sur destaca cuatro verdades sobre los ciberconflictos, una vez analizados. Las implicaciones de tres de ellas son obvias, la cuarta todavía no es así: 1) los ciberconflictos son perjudiciales, 2) pero están lejos de la guerra, 3) los ciberconflictos son cada vez más fáciles de predecir y la nación responsable a menudo es perfectamente obvia, 4) sin embargo, para detener este tipo de ataques asimétricos, a veces hay que utilizar un enfoque tradicional.

Los ciberconflictos analizados son los producidos en marzo de 2013, en esa ocasión los equipos de Corea del Sur de los sectores financieros, energéticos y de medios de comunicación sufrieron un ataque sofisticado que afectó a cajeros automáticos y sitios web fuera de línea.

[3] Para más información consultar el artículo *Seeking to Avert Cyber War* de Frederick Kempe, presidente y CEO del Consejo del Atlántico.

Inicialmente los ataques parecían ser una típica negación de servicio, en el que simplemente las redes se vieron inundadas por el tráfico, que las tornó fuera de servicio.

En un principio, incluso los grandes ataques de DDoS son fáciles de lanzar, ya que los grupos delictivos pueden conseguir la capacidad necesaria simplemente alquilándola por horas, y por tanto, no se necesitan los llamados ciberguerreros. En un segundo momento, se observó que los ataques tenían un componente más interesante y peligroso, ya que se destruyó los datos de los ordenadores atacados con un borrado de sus discos duros.

A pesar de ello, esta interrupción no era de larga duración ni, en última instancia, de carácter letal, los sistemas se recuperaron en días e incluso horas. Y ésta es, de hecho, la regla de los ciberconflictos, no la excepción.

El estudio realizado por el Atlantic Council y la Cyber Conflict Studies Association sobre la historia del ciberconflicto, no ha encontrado un solo caso en el que alguien haya muerto por un ciberconflicto. Los ciberconflictos pueden ser relativamente fáciles de poner en marcha, pero también es bastante fácil recuperarse de ellos. Los recursos afectados se pueden reemplazar rápidamente. Son indudables las molestias. Como tal, los ciberconflictos conllevan bastantes molestias pero casi nunca se pueden considerar terrorismo y mucho menos guerra.

La segunda verdad contradice la idea de que los ciberataques son imprevisibles. Los ataques a Corea del Sur son sólo el último de una serie que se remonta a 2009, una tendencia que se hizo no sólo totalmente previsible, sino predecible.

En la historia del ciberconflicto hay un fuerte vínculo entre las crisis geopolíticas en el mundo real y los ciberataques posteriores. Por ejemplo, cada vez que hay una refriega entre los barcos de pesca de China y otro reclamante de las islas en disputa, se espera que haya hacking o piratería patriótica procedente de China. En consecuencia, tan pronto como Corea del Norte renunció el armisticio con Corea del Sur a mediados de marzo, algunos ya dieron la alarma sobre la probabilidad de los ciberataques.

Los ataques eran predecibles debido a las reacciones de Corea del Norte, y la comunidad internacional debiera contar con esa nación como el principal responsable de los mismos, a menos que haya pruebas de descargo. Esta conexión no se puede demostrar, pero la verdad es que el ciberconflicto no tiene por qué ser diferente a otros misterios de la seguridad nacional.

Cuando el Cheonan, una corbeta de Corea del Sur, fue hundida en 2010, con la pérdida de 26 marineros, tampoco pudo probarse que Corea del Norte era la responsable, pero la autoría de

la explosión fue lo suficientemente clara. El ataque, como el bombardeo posterior de una isla surcoreana en el que murieron dos infantes de marina y dos civiles, ayuda a alimentar la nueva determinación de China para reprender y, con un poco de suerte, restringir a su rebelde aliado.

Esto apunta a la cuarta verdad. Cuando se trata de evitar que el régimen de Kim Jong Un arremeta con ciberataques, la ruta no debe comenzar en Pyongyang, sino en Pekín.

Esta no es la primera respuesta de la mayoría de la comunidad cibernética, cuyo primer instinto es buscar respuestas técnicas. Los técnicos pueden ayudar a defenderse de futuras interrupciones, pero no ayudarán con el subyacente comportamiento de Corea del Norte.

La comunidad internacional también encontrará algunos nuevos ciber-mecanismos de poder para reducir la intensidad de la crisis. Corea del Norte está simplemente demasiado aislada, con sólo una conexión débil en el ciberespacio. Afortunadamente, no hay necesidad de buscar nuevas soluciones cibernéticas ya que los ciberconflictos no se pueden resolver aislados de la dinámica subyacente de la seguridad nacional.

En realidad, la comunidad internacional no tiene un problema cibernético con Corea del Norte, simplemente tiene un problema con Corea del Norte. Los ciberataques son simplemente una faceta de este dilema mayor. El liderazgo chino está ya cada vez más frustrado públicamente con las pataletas de Kim Jong Un y cada nueva rabieta pone en una situación incómoda, aún más, el liderazgo chino. Según Jason Healey, *director de la Cyber Statecraft Initiative del Atlantic Council*[4], los diplomáticos de Corea del Sur y EE.UU. deben agregar cada nueva interrupción a la lista de los ultrajes de que Beijing tiene que responder y no tratar cada uno como un tema aparte.

Sin embargo, China y otros pueden tratar de desviar la atención al afirmar que no hay pruebas suficientes de la autoría de Corea del Norte. Estados Unidos y Corea del Sur no deberían tratar el tema cibernético como algo diferente y responder de la misma manera que lo hicieron después del hundimiento del Cheonan. Entonces, un grupo de expertos internacionales examinó las pruebas y publicó un informe documentado con la prueba irrefutable que "hacía saber a Corea del Norte y a la comunidad internacional que incluso el ataque más encubierto deja evidencia."

Una comisión, debidamente seleccionada tal vez por las Naciones Unidas o por los gobiernos

[4] Para más información consultar el artículo *To Stop North Korean Cyber Attacks, Start in Beijing* de Jason Healey, director de la Cyber Statecraft Initiative at the Atlantic Council.

involucrados, debería examinar, además, las pruebas forenses y el contexto de seguridad nacional para elaborar conclusiones acerca de qué grupo o nación es responsable. Al igual que con el informe Cheonan, todavía habrá detractores, pero un ajuste de cuentas público y completo traerá la claridad necesaria y ayudará a establecer el punto de referencia para las nuevas normas internacionales.

Los ciberataques norcoreanos aún no han causado víctimas o interrupciones graves. Sin embargo, Corea del Norte ha aprendido a presionar con sus enfrentamientos militares, los ciberataques empeorarán y algún día podrían cruzar los umbrales. La comunidad internacional debería tratar los ciberataques como lo haría con cualquier otro uso de la fuerza por Corea del Norte y presionar al gobierno chino para frenar a su vecino rebelde.

Mª José Caro Bejarano
Analista del IEEE