# El mundo ya no se burla del poderío cibernético de Corea del Norte.

**Por: David E. Sanger , David D. Kirkpatrick / Nicole Perlroth. The New York Times. 11/11/2017**

Cuando el año pasado los *hackers* norcoreanos intentaron robar 1000 millones de dólares de la Reserva Federal de Nueva York, solo los detuvo un error ortográfico. Estaban realizando un saqueo digital de una cuenta del Banco Central de Bangladés, cuando los banqueros comenzaron a sospechar de una solicitud de retiro en la que decía “fandation” en vez de “foundation” (fundación).

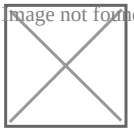
A pesar de todo, los secuaces de Kim Jong-un obtuvieron 81 millones de dólares en el golpe. Su trayectoria es una mezcla de fracasos y éxitos, pero el ejército de más de 6000 *hackers* que tiene Corea del Norte es persistente, y desde luego que va mejorando, aseguraron funcionarios de seguridad de Estados Unidos y Reino Unido, quienes han encontrado que el origen de estos ataques y algunos otros es Corea del Norte.

Entre toda la atención que genera el progreso de Pyongyang para desarrollar un arma nuclear capaz de impactar a Estados Unidos, los norcoreanos también han desarrollado sigilosamente un ciberprograma que está robando cientos de millones de dólares y está demostrando que puede desatar el caos a nivel mundial.

A diferencia de las pruebas de armas, las cuales han acarreado sanciones internacionales, prácticamente no se han hecho retroceder ni se han castigado los ciberataques de Corea del Norte, a pesar de que el régimen está utilizando sus capacidades de *hackeo* con el fin de ejecutar verdaderos ataques en contra de sus adversarios.

Del mismo modo en que los analistas de Occidente alguna vez se burlaron del potencial que tenía el programa nuclear de Corea del Norte, los expertos también desestimaron su potencial cibernético, pero ahora reconocen que el *hackeo* es un arma casi perfecta para Pyongyang, pues Corea del Norte está aislada y tiene poco que perder.

Image not found or type unknown



Retratos de los antiguos líderes de Corea del Norte, Kim Il-sung y Kim Jong-il, en un edificio de PyongyangCreditEd Jones/Agence France-Presse — Getty Images

La infraestructura primitiva del país es mucho menos vulnerable a una represalia cibernética, además los *hackers* de Corea del Norte operan fuera del país. Las sanciones no brindan una respuesta útil, ya que se han impuesto una gran cantidad de ellas. Además, los asesores de Kim están apostando a que nadie responderá a un ciberataque con un ataque militar, por temor a que escale el conflicto entre las dos Coreas.

Y está lejos de ser un conflicto en una sola dirección: según algunos indicadores, Estados Unidos y Corea del Norte llevan años entrelazados en un activo conflicto cibernético.

Tanto Estados Unidos como Corea del Sur también han colocado “implantes” digitales en el Buró de Reconocimiento General, el equivalente norcoreano de la Agencia Central de Inteligencia, según documentos que Edward J. Snowden divulgó hace varios años. Se desplegaron armas cibernéticas y electrónicas de guerra creadas por Estados Unidos con el objetivo de incapacitar los misiles de Corea del Norte, un ataque que fue, en el mejor de los casos, parcialmente exitoso.

De hecho, los dos bandos perciben a la cibernética como una manera de obtener ventaja táctica en su disputa nuclear y de misiles.

Alguna vez, Corea del Norte falsificó de forma burda billetes de 100 dólares para intentar generar dinero en efectivo. En la actualidad, los funcionarios de inteligencia calculan que Corea del Norte cosecha cientos de millones de dólares al año por medio de programas de secuestro, atracos digitales a bancos, *cracking* de

videojuegos en línea y, hace poco, *hackeos* a los mercados de valores de Bitcoin en Corea del Sur.

Un exdirectivo de la inteligencia británica estima que la recaudación de estos ciberatracos podría aportar hasta 1000 millones de dólares al año a Corea del Norte, el equivalente a un tercio del valor de las exportaciones de esa nación.

En 2011, cuando Kim Jong-un asumió el poder heredado de su padre, expandió la misión cibernética para que fuera más que solo un arma de guerra, pues se centró también en el robo, el acoso y el ajuste de cuentas a nivel político.

“La ciberguerra, junto con las armas nucleares y los misiles, es una ‘espada multipropósitos’ que garantiza la capacidad de nuestro ejército para atacar sin misericordia”, supuestamente habría declarado Kim, según un director de la inteligencia surcoreana.

Y el despliegue de sanciones de las Naciones Unidas en contra de Pyongyang solo incentivó el uso de la guerra cibernética por parte de Kim.

“Ya estamos sancionando todo lo que podemos”, afirmó Robert P. Silvers, quien fue secretario adjunto de Ciberpolítica del Departamento de Seguridad Nacional durante el gobierno de Obama. “Ya es la nación más aislada del mundo”.

Kim Jong-un, actual líder de Corea del Norte, inspecciona una fábrica en Pyongyang. CreditKorean Central News Agency

Durante décadas, Irán y Corea del Norte han compartido tecnología de misiles, y las agencias de inteligencia de Estados Unidos llevan mucho tiempo buscando evidencias de esa cooperación secreta en el ámbito nuclear. En el campo de la

cibernética, los iraníes enseñaron algo importante a los norcoreanos: cuando se confronta a un enemigo que tiene bancos, sistemas de comercio, tuberías para petróleo y agua, presas, hospitales y ciudades enteras conectadas a internet, las oportunidades de sembrar el caos son infinitas.

A mediados del verano de 2012, los *hackers* iraníes, quienes apenas se estaban recuperando de un ciberataque que lanzaron Estados Unidos e Israel en contra de sus operaciones de enriquecimiento nuclear, encontraron un blanco sencillo en Saudi Aramco, la firma petrolera propiedad del gobierno de Arabia Saudita y la empresa más valiosa del mundo.

Durante ese agosto, los *hackers* iraníes apagaron un interruptor general exactamente a las 11:08 a. m. y un simple virus llegó a 30.000 computadoras y 10.000 servidores de Aramco, borró su información y la remplazó con una imagen parcial de la bandera estadounidense en llamas. El daño fue tremendo.

Siete meses después, durante los ejercicios militares conjuntos de las fuerzas de Estados Unidos y Corea del Sur, los *hackers* norcoreanos desplegaron una ciberarma muy similar en contra de las redes de computadoras de tres de los principales bancos y dos de las cadenas de televisión más grandes de Corea del Sur, mediante computadoras que se encontraban al interior de China. Como sucedió con Irán y Aramco, para atacar los blancos surcoreanos, los norcoreanos utilizaron un software malicioso que erradicó información y paralizó las operaciones comerciales.

Integrantes de la agencia de seguridad cibernética coreana, en Seúl, monitorean posibles ciberataques.CreditJung Yeon-Je/Agence France-Presse — Getty Images

Más allá del respeto y castigo que quería generar, Corea del Norte buscaba obtener

dinero en efectivo a partir de su ciberprograma.

Entonces, pronto comenzaron los robos digitales bancarios: un ataque en las Filipinas en octubre de 2015; luego el blanco fue el Tien Phong Bank en Vietnam, a finales del mismo año; y después el Banco Central de Bangladés. Los investigadores de Symantec señalaron que fue la primera vez que un Estado había utilizado un ciberataque para fines distintos del espionaje o la guerra, puesto que su objetivo fue financiar las operaciones del país.

En la actualidad, los ataques son cada vez más ingeniosos. En febrero, los expertos en seguridad se percataron de que el sitio web de la autoridad regulatoria financiera de Polonia estaba infectando de forma no intencional a sus visitantes con un software malicioso.

Resulta que los visitantes del sitio polaco recibieron el impacto de un ataque conocido como “watering hole”, en el cual los *hackers*norcoreanos esperaron a que sus víctimas visitaran el sitio y entonces instalaron el software malicioso en sus máquinas. El reporte forense mostró que los *hackers* habían reunido una lista de direcciones de internet de 103 organizaciones, la mayoría de las cuales eran bancos, y diseñaron su software para infectar específicamente a los visitantes de esas instituciones, en lo que los investigadores afirmaron que parecía ser un intento para mover divisas robadas.

Image not found or type unknown

Una pantalla ubicada en una plaza pública en las afueras de Pyongyang, muestra la cobertura noticiosa de las pruebas de un misil norcoreano, en agosto. Credit Kim Won-Jin/Agence France-Presse — Getty Images

Hace poco tiempo, los norcoreanos volvieron a cambiar de rumbo. Los *hackers* dejaron huellas en una serie de intentos de ataques en contra de mercados de valores de criptomoneda en Corea del Sur, y tuvieron éxito en al menos un caso, según los investigadores de FireEye.

Aunque los funcionarios de Estados Unidos y de Corea del Sur suelen expresar indignación por las actividades cibernéticas de Corea del Norte, pocas veces hablan de las suyas… y si estas promueven la carrera armamentística cibernética.

En una reunión reciente de estrategas estadounidenses en la que se juntaron para evaluar las capacidades de Corea del Norte, algunos de los asistentes expresaron su preocupación respecto de que el aumento de la ciberguerra pudiera tentar realmente a Corea del Norte a utilizar muy rápido sus armas —tanto nucleares como cibernéticas— en cualquier tipo de conflicto, por temor a que Estados Unidos pudiera tener métodos secretos para incapacitar al país.

**LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ.**

Fotografía: The new york times

**Fecha de creación**
2017/11/11