CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

HACIA UNA NORMA INTERNACIONAL CONTRA LA MANIPULACIÓN DE LA INTEGRIDAD DE LOS DATOS FINANCIEROS

TIM MAURER, ARIEL LEVITE, Y GEORGE PERKOVICH | MARZO 27, 2017

INTRODUCCIÓN

El 18 de marzo de 2017, los ministros de Finanzas y los gobernadores de los bancos centrales de las veinte principales economías del mundo —G20— emitieron un comunicado en el que destacaron lo siguiente:

> El uso malicioso de Tecnologías de la Información y la Comunicación (TIC) podría afectar servicios financieros que son esenciales tanto para los sistemas financieros nacionales como internacionales, mellar la seguridad y la confianza, y poner en peligro la estabilidad financiera. Nos proponemos promover la resiliencia de las instituciones y los servicios financieros en las jurisdicciones de los países del G20 frente al uso malicioso de las TIC, incluso cuando estas acciones provengan de países que no forman parte del G20. Como primer paso, y a fin de mejorar nuestra cooperación trasnacional, le solicitamos al Consejo de Estabilidad Financiera (*Financial Stability Board*, FSB) que realice un relevamiento de las regulaciones pertinentes que se hayan emitido y de las prácticas en materia de supervisión que existen en nuestras jurisdicciones, así como de las directrices internacionales. Esa actividad incluirá la identificación de prácticas efectivas. El FSB debería informar sobre los avances en esta tarea durante la Cumbre de Líderes que se llevará a cabo en julio de 2017 y presentar un informe de relevamiento en octubre de ese mismo año[1].

Es positivo que los ministros de Finanzas y gobernadores de los bancos centrales del G20 hayan instado a mejorar la resiliencia del sistema financiero mundial. Sin embargo, los gobiernos no deberían limitarse a pedirle al sector privado que haga más, pues ellos mismos pueden contribuir a reducir el riesgo en el sector financiero. Los jefes de Estado que forman parte del G20 podrían asumir explícitamente, en nombre de sus países, el compromiso de no utilizar herramientas cibernéticas ofensivas que corrompan la integridad de los datos del sistema financiero y de prestar su colaboración ante ese tipo de ataques.

La crisis financiera que se desató en 2007 puso de manifiesto, por un lado, cuán importante es la confianza para el sistema global y, por el otro, la fragilidad de ese sistema. El incidente cibernético que afectó al Banco Central de Bangladés en 2016 expuso una nueva amenaza contra la estabilidad financiera y la magnitud inédita del riesgo que representan los actores cibernéticos maliciosos para las instituciones financieras[2]. Más allá de fines más comunes como el robo, las operaciones cibernéticas se utilizan para manipular la integridad de los datos, y es sobre todo en este sentido que plantean un conjunto diferenciado y más amplio de riesgos sistémicos que otras formas de coerción financiera. Debido a la naturaleza compleja e interdependiente del sistema financiero y a que

ACERCA DE LOS AUTORES

Tim Maurer *es codirector de la Iniciativa sobre Ciberpolíticas del Fondo Carnegie para la Paz Internacional (Carnegie Endowment for International Peace). Sus investigaciones se centran principalmente en el ciberespacio y en asuntos internacionales, como ciberseguridad, derechos humanos en línea y gobernanza de Internet.*

Ariel (Eli) Levite *es investigador sénior invitado del Programa de Políticas Nucleares del Carnegie Endowment. Entre 2002 y 2007 se desempeñó como subdirector general principal en materia de políticas en la Comisión Israelí de Energía Atómica.*

George Perkovich *es vicepresidente de estudios en el Carnegie Endowment for International Peace. Sus investigaciones abordan principalmente temas de estrategia nuclear y no proliferación, y se enfocan en Asia Meridional, Irán y el problema de la justicia en la economía política internacional.*

este trasciende fronteras físicas y nacionales, la manipulación de la integridad de los datos de las instituciones financieras puede, de manera deliberada o no, poner en jaque la estabilidad financiera y la del sistema internacional. Es importante señalar que, a diferencia de lo que ocurrió en la crisis mundial de 2007–2008, este riesgo existe con independencia de las variables económicas subyacentes y se acentuará a medida que más gobiernos asuman como objetivo explícito tener una economía que funcione sin efectivo[3].

En 2015, el Grupo de Expertos Gubernamentales de la ONU (*UN Group of Governmental Experts*, UNGGE) y el G20 ya habían propuesto que se adoptaran normas amplias contra los ataques a infraestructuras civiles críticas en tiempos de paz. En esta oportunidad, los ministros de Finanzas y gobernadores de bancos centrales del G20 han hecho hincapié, en especial, en el riesgo para la estabilidad financiera. Por lo tanto, en este documento proponemos que los Estados tomen como base estas recomendaciones existentes y que adopten medidas más amplias, asumiendo el compromiso expreso de no vulnerar la integridad de los datos y algoritmos de las instituciones financieras en tiempo de paz o de guerra[4], ni permitir que sus ciudadanos lo hagan[5].

Proponemos la siguiente redacción para ese tipo de acuerdo; y por cierto se insta a que sea debatida y a que se sugieran mejoras:

> Un Estado no deberá realizar ni apoyar a sabiendas una actividad que, de modo intencional, manipule la integridad de los datos y algoritmos de las instituciones financieras, cualquiera sea el lugar donde se encuentren almacenados o cuando se encuentren en tránsito.
>
> En la medida que la ley lo permita, un Estado deberá responder con prontitud a las solicitudes pertinentes que otro Estado formule de mitigar actividades que manipulen la integridad de los datos y algoritmos de las instituciones financieras, cuando esas actividades pasen a través de su territorio o emanen de él, o sean realizadas por sus ciudadanos.

Los Estados ya han mostrado suma cautela en lo que respecta el uso de medios cibernéticos contra la integridad de los datos de instituciones financieras. Por lo tanto, el tipo de acuerdo que venimos analizando haría explícito lo que hasta el momento podría considerarse una práctica estatal emergente. Explicitarlo posibilitaría lo siguiente:

- enviaría el mensaje claro de que la estabilidad del sistema financiero mundial depende de que se preserve la integridad de los datos financieros en tiempos de paz y de guerra, y de que la comunidad internacional considera inaceptable la manipulación de la integridad de esos datos;
- generaría confianza entre los Estados que ya actúan con prudencia en este ámbito y, de ese modo, aumentaría su capacidad de movilizar a la comunidad internacional si la norma fuera violada;
- generaría una oportunidad política de lograr una mayor colaboración para actuar contra los agentes no estatales que atacan a instituciones financieras empleando medios cibernéticos; y
- complementaría y mejoraría los actuales acuerdos e iniciativas, como la declaración del G20 de 2015, el informe del UNGGE de 2015 y las pautas en materia cibernética ('Cyber Guidance') del Comité de Pagos e Infraestructuras del Mercado (*Committee on Payments and Market Infrastructures*, CPMI) y de la Organización Internacional de Comisiones de Valores (OICV) de 2016.

Si bien en el comunicado de los ministros de Finanzas y gobernadores de bancos centrales de los países del G20 emitido el 18 de marzo no se define la frase "uso malintencionado de las TIC", es razonable suponer que se refiere, sobre todo, a la integridad y disponibilidad de datos financieros. Pues es inevitable, y no necesariamente malintencionado, que en ocasiones los organismos de orden público y de inteligencia violen la confidencialidad de los datos en poder de bancos y otras instituciones financieras con el objetivo de combatir el terrorismo, la proliferación de armas y la delincuencia. Por lo tanto, en este trabajo se describe por qué es fundamental, por un lado, prohibir la corrupción de datos en el sistema financiero mundial para lograr la estabilidad del sistema internacional y, por otro, consolidar una norma integral en este sentido.

Se esperaría que los Estados cumplan estos compromisos observando las limitaciones y los requisitos de las normas nacionales e internacionales, que posteriormente tal vez haya que ajustar para reflejar los compromisos aquí sugeridos. También se esperaría que implementen las directrices y mejores prácticas existentes, como las delineadas en las pautas en materia cibernética del CPMI y la OICV de 2016[6].

Los jefes de Estado que forman parte del G20 tienen ahora la oportunidad de adoptar ese compromiso y de pedir al Consejo de Estabilidad Financiera que lo ponga en práctica, junto con los organismos normativos pertinentes, el sector privado, las autoridades de aplicación de la ley y el equipo de respuesta a emergencias cibernéticas (*Computer Emergency Response Team*, CERT). Se basaría en el precedente sentado en 2015, cuando el G20 decidió incluir el tema de la ciberseguridad en el comunicado de los jefes de Estado, y en el precedente de las medidas tomadas por el G20 tras la crisis financiera de 2007, así como en el comunicado de los ministros de Finanzas y gobernadores de los bancos centrales del G20.

ANTECEDENTES

En 2015, el UNGGE, del que formaban parte representantes de los cinco miembros permanentes del Consejo de Seguridad de la ONU, acordaron lo siguiente en su informe de consenso: "Un Estado no debería realizar ni apoyar de forma deliberada actividades en la esfera de las TIC contrarias a las obligaciones que le incumben en virtud del derecho internacional que puedan dañar intencionadamente infraestructuras fundamentales que prestan servicios al público o dificulten de otro modo su utilización y funcionamiento"[7].

Posteriormente, adhirieron a esta declaración los jefes de Estado en la cumbre del G20 de 2015[8]. Sin duda, estos compromisos políticos generales resultan loables. Sin embargo, la historia sugiere que, a menudo, los Estados prometen demasiado pero cumplen poco al momento de hacer efectivas este tipo de declaraciones normativas tan amplias. Un problema es la ambigüedad, pues a veces los Estados definen de distinta manera cuáles son las infraestructuras críticas. Asimismo, cada vez son más los expertos que se manifiestan escépticos con respecto a la efectividad del proceso del UNGGE[9]. Por otra parte, el lenguaje utilizado por el UNGGE se centra en los efectos de las ciberoperaciones, y esto deja un vacío en el contexto específico del sistema financiero global, que es sumamente interdependiente. Por lo tanto, vale la pena intentar alcanzar un acuerdo más detallado que tome ese texto como base y lo aclare en relación con determinadas operaciones que podrían ser particularmente perjudiciales para el sistema internacional.

El sistema financiero es un área especialmente prometedora, pues hay intereses comunes entre la mayoría de los Estados. Se diferencia de casi todos los demás tipos de infraestructura crítica, como el transporte o la red eléctrica, porque es globalmente interdependiente. Las principales potencias, a pesar de las diferencias fundamentales que mantienen, han reconocido esto tanto en la teoría como en la práctica. El gobierno de EE. UU. se habría abstenido de llevar adelante ciberoperaciones ofensivas contra los sistemas financieros de Saddam Hussein, así como en ejercicios de simulacro de conflicto con China[10]. El texto de proyecto del Convenio *Internacional sobre Seguridad Informática* de 2011 propuesta por Rusia sugiere de manera explícita que "cada Estado Parte adopte las medidas necesarias para garantizar que la actividad de los sistemas de información internacionales de gestión del flujo de. . . las finanzas… continúe sin interferencias"[11]. También China tiene intereses concretos en el sistema, lo cual se refleja, entre otras cosas, en su exitosa iniciativa de incorporar el renminbi a la canasta de monedas de reserva mundial del FMI[12]. Mientras tanto, países en todo el mundo establecen o consolidan CERT específicos para el sector financiero, como, por ejemplo, lo hizo la India en febrero de 2017[13].

Dado que el sector financiero es globalmente interdependiente, resulta más vulnerable que otras infraestructuras críticas y existen más probabilidades de que los Estados valoren, en pro del interés común, la necesidad de protegerlo. Los efectos nocivos de una intrusión en la red eléctrica o en el sector del petróleo y el gas se limitarán, mayormente, al territorio de un solo país o de sus vecinos contiguos. Sin embargo, los efectos de un incidente que apunta la integridad de los datos de una

institución financiera no necesariamente están limitados por la geografía. Sería muy difícil comprender esos efectos y, por lo tanto, no sería fácil adecuarse a ellos y anticiparlos. Una operación que ataque un sistema de procesamiento de pagos podría corromper en forma directa las transacciones que se realizan por medio de ese sistema. De manera indirecta, la manipulación de la integridad de los datos de una institución podría causar su quiebra y esto, a su vez, podría perturbar todo el sistema internacional. Por ejemplo, el colapso de Lehman Brothers en 2008 puso de relieve el efecto contagio imprevisto que puede tener incluso la quiebra de una sola institución. De manera parecida, la crisis financiera asiática de 1997 se desencadenó por la estrepitosa caída de la moneda tailandesa y por el efecto contagio imprevisto que sufrió toda la región. Es difícil prever esos efectos secundarios. Asimismo, es posible que el atacante no los tenga en cuenta al momento de evaluar los daños que pretende causar.

Sobre este punto, puede ser útil la experiencia internacional sobre la prohibición de falsificar moneda. Los Estados han adherido y contribuido a aplicar tal prohibición porque todos son vulnerables a los efectos de la falsificación. Dado que esta limitación goza de amplia aceptación, es muy probable que los Estados que la transgredan enfrenten sanciones. Queda claro que los agentes no estatales continúan realizando falsificaciones, al igual que también lo hacen Corea del Norte y algunos otros Estados, pero la práctica está suficientemente controlada como para no representar una amenaza a la estabilidad del sistema financiero internacional[14].

Otra analogía histórica muestra por qué las principales potencias económicas como las que conforman el G20 tendrían, por lo menos, interés en avalar y respaldar una norma específica contra la manipulación de datos financieros en tiempos de paz y de guerra: en 1914, el Gobierno británico, usando su posición dominante en el sistema comercial y financiero mundial, llevó adelante una guerra económica contra Alemania. Aunque la estrategia logró desestabilizar la economía mundial, apenas tres meses después el Gobierno británico desistió. La reacción negativa fue mucho más intensa y súbita de lo previsto, e incluyó a empresas, trabajadores y figuras políticas del Reino Unido que hicieron sentir su voz de protesta, así como la presión de los aliados[15]. Dado que la economía global se encontraba en ese momento sumamente integrada, resultó imposible contener los efectos no deseados e imprevistos de un ataque económico.

Es evidente que, en el siglo XXI, algunos Estados que están relativamente apartados de la economía global y agentes no estatales que pueden o no estar vinculados con los primeros tienen la capacidad de lanzar ciberataques contra instituciones financieras. No cabría esperar que fueran esos agentes hostiles los que adhieran al compromiso propuesto. Aun así, los Estados que sí respalden esa norma de manera explícita estarían más unidos y tendrían un interés y un fundamento más claro para exigir y tomar represalias contra quienes violen la norma, sean Estados, terroristas o ciberdelincuentes. Es decir, el acuerdo explícito propuesto podría servir de base para definir medidas colectivas contra todo tipo de infractores. (Algunos Estados que declararan su adhesión a la propuesta podrían verse tentados a tolerar o utilizar "corsarios" u otros intermediarios para atacar instituciones financieras. Sin embargo, también en este caso, la existencia del acuerdo permitiría contar con más herramientas que las que existen en la actualidad para ejercer presión sobre los Estados con malas intenciones).

APROVECHAR LAS NORMAS Y EL DERECHO INTERNACIONAL EXISTENTES

Un acuerdo explícito contra la manipulación de la integridad de los datos de las instituciones financieras partiría de las iniciativas internacionales recientes como base para elaborar normas aplicables al ciberespacio, así como las disposiciones básicas del derecho internacional contra la falsificación de moneda. Asimismo, un compromiso de ese tipo abordaría una laguna en el Derecho de los Conflictos Armados (también conocido como derecho internacional humanitario).

A la fecha, la iniciativa más importante de la comunidad internacional para elaborar normas de circulación en el ciberespacio es el proceso relativo al Grupo de Expertos Gubernamentales de la ONU, cuyo trabajo recibió el respaldo del G20 en 2015.

Aún así, en primer lugar, hasta el momento la declaración emitida en 2015 por el grupo y el respaldo del G20 carecen de precisiones suficientes y no estipulan pasos concretos para convertirlas en regímenes de seguridad efectivos y sólidos. En segundo lugar, la redacción deseada de las normas del UNGGE se aplica a tiempos de paz y no hace referencia a los comportamientos durante un conflicto armado, ni aborda los vacíos que existen en el derecho internacional humanitario. Asimismo, hay una brecha en el contexto específico de las ciberoperaciones contra instituciones financieras.

La manipulación de la integridad de los datos financieros comparte, en varios sentidos, similitudes con la falsificación de moneda. Con respecto a este punto, el Convenio Internacional para la Represión de la Falsificación de Moneda de 1929 puede proporcionar un fundamento legal que sirva de base[16]. Como lo resumió en 2004 el entonces consejero jurídico del Fondo Monetario Internacional, François Gianviti: "El derecho de un Estado de emitir su moneda está protegido contra la injerencia de Estados extranjeros. Por lo tanto, un Estado extranjero no puede falsificar la moneda de otro Estado (derecho internacional consuetudinario y Convenio de Ginebra del 20 de abril de 1929 para la Represión de la Falsificación de Moneda)"[17]. Fueron pocas las oportunidades en que se violó esta prohibición, lo cual demuestra que la norma ha sido muy sólida a lo largo de varias décadas[18]. Esto refleja que los Estados reconocen que la falsificación de moneda socava la integridad del sistema financiero en general y la confianza en él, del cual muchos, si no todos, dependen.

Sin embargo, los Estados aún no han debatido ni decidido si las prohibiciones contra la falsificación podrían y deberían extenderse a la era digital, ni cómo hacerlo. Es decir, ¿puede y debe aplicarse el Convenio para la Represión de la Falsificación de Moneda a la moneda digital o a los datos financieros? Si en el siglo XXI es tan importante preservar la integridad de los datos financieros como la de la moneda, entonces plasmar esto expresamente en un nuevo acuerdo específico sería una medida beneficiosa para los intereses mundiales. El antecedente del régimen contra la falsificación podría hacer que se entienda este interés y se confíe en que es viable prohibir la manipulación de los datos financieros.

Por su parte, en el Derecho de los Conflictos Armados tampoco se explica la índole y la importancia de los datos. Hay, por lo menos, dos temas importantes sobre este punto. Uno se relaciona con la *ius ad bellum* (la causa justa para la guerra). Las opiniones entre los expertos del derecho están divididas respecto de si un ataque contra datos financieros (por muy extraordinarios y masivos que sean sus potenciales efectos) califica o no como uso de fuerza. El artículo 2(4) de la Carta de la ONU solo prohíbe el uso de la fuerza armada, pero no la coerción política o económica[19]. En términos más amplios, ante el surgimiento de guerras híbridas y de la guerra de información, ahora la comunidad internacional se enfrenta al desafío de decidir si hay alguna manera de abordar legalmente los actos de coerción que no comportan uso de la fuerza y cómo hacerlo. El *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Manual Tallin 2.0 sobre el derecho internacional aplicable a las ciberoperaciones)* de 2017 se centra en esta cuestión.

Resulta más pertinente determinar si la *ius in bello* (la conducta justa durante la guerra) exige o admite que haya datos que se consideren que no pueden afectarse. Una vez más, las opiniones de los expertos jurídicos están divididas sobre este punto. Por ejemplo, el grupo de expertos legales que compiló el *Manual Tallinn* de 2013 sostuvo que los datos no son un objeto y, por ende, las ciberoperaciones ofensivas que atacan la integridad de los datos financieros están fuera del alcance, de los principios y de las salvaguardas del actual derecho internacional humanitario[20]. En consecuencia, la condición de los datos financieros conforme al derecho internacional es objeto de debate.

Asimismo, si las instituciones financieras se consideran objetos civiles o militares depende de si un país define "objeto militar" en un sentido estricto que solo incluya las capacidades de combatir en una guerra o si, como para Estados Unidos, ese término se define de manera más amplia para incluir las

"capacidades de combate bélico y de sostenimiento bélico"[21]. En el último caso, las instituciones financieras y sus datos podrían verse como objetivos militares legítimos durante un conflicto armado (aunque, como señalamos antes, Estados Unidos parece haber evitado hasta el momento tales ataques)[22].

Por eso, un acuerdo explícito de no manipular la integridad de los datos financieros podría indicar, por lo menos en este contexto limitado, hacia dónde pretenden los estados adherentes que evolucione el derecho internacional.

EL ACUERDO PROPUESTO

Las actuales tendencias observadas en el ámbito internacional sugieren que es más probable que las ciberamenazas se produzcan en la zona gris comprendida entre los períodos de paz y un conflicto armado[23]. Un acuerdo que proteja únicamente la integridad de los datos financieros en tiempos de paz sería insuficiente, dada la importancia que el sistema financiero tiene para la estabilidad y el bienestar de todos los Estados y sociedades. Las posibles consecuencias negativas no deseadas de un ataque sobre la integridad de los datos, incluidos los efectos imprevistos, exceden cualquier beneficio. Además, en caso de conflicto armado, se necesitará dinero para reconstruir y solventar eventuales reparaciones. Por lo tanto, es deseable y posible que los Estados se comprometan a no manipular la integridad de los datos financieros en ninguna circunstancia.

Concentrarse en la integridad de los datos no le resta importancia a proteger su disponibilidad y confidencialidad. Sin embargo, puede alegarse que las consecuencias nacionales e internacionales de manipular datos son más significativas que las violaciones de confidencialidad y que, desde el punto de vista técnico, resulta más difícil abordarlas en comparación con la interrupción de la disponibilidad. Corromper la integridad de los datos puede plantear serios obstáculos a su recuperación. Además de los obstáculos técnicos, algunas disposiciones legales específicas del sistema financiero plantean escollos adicionales, como la firmeza de la liquidación. Por estos y otros motivos, la manipulación de la integridad de los datos es un problema de mucha mayor envergadura que la actividad maliciosa que menoscaba la disponibilidad de datos.

Por último, si bien es posible que haya discrepancias entre los expertos con respecto a qué constituye "riesgo sistémico" para el sistema financiero, existe un consenso generalizado de que la integridad de los datos es el riesgo más preocupante.

Los ataques de denegación de servicios distribuidos (*distributed denial of service*, DDoS) son bastante habituales. Tienen carácter temporal y reversible, y existen soluciones técnicas para prevenirlos y mitigar sus efectos. Además, los Estados y la comunidad internacional (a través de las Naciones Unidas) imponen ocasionalmente sanciones a instituciones financieras, algo que, en cierto modo, equivale a negar la disponibilidad de recursos en esas instituciones a sus titulares y usuarios. Podría incluirse la prohibición de realizar operaciones que afecten la disponibilidad de datos cuando la intención o el efecto sea corromper la integridad de las transacciones, como sería, por ejemplo, el caso del *outsider trading*, o tráfico de información privilegiada por parte de personas externas. Lo mismo vale para la disponibilidad de datos en algunos sistemas críticos. Para definir si es posible abordar la manipulación de la disponibilidad de esos datos e incluir esa cuestión en el acuerdo propuesto, así como para determinar de qué manera hacerlo, se debería realizar una consulta más amplia a expertos y obtener su asesoramiento. El G20 debería encargar al Consejo de Estabilidad Financiera que trabaje junto con los organismos y expertos pertinentes en materia de establecimiento de estándares para informar sobre esta cuestión y analizarla mejor.

Con respecto a la confidencialidad, algunos Estados seguirán realizando ciberoperaciones para recabar información de inteligencia de bancos e instituciones financieras. Además de las regulaciones, tales operaciones son fundamentales para llevar un seguimiento de la proliferación de armas y luchar contra el terrorismo, el blanqueo de dinero, el narcotráfico y otras prácticas ilegales. Ni la costumbre ni el derecho internacional prohíben ese tipo de espionaje[24]. Si se intentara incluir la prohibición de actividades de inteligencia en una norma sobre ciberoperaciones contra instituciones financieras, la adopción de esa norma sería inviable o habría muchas dudas sobre su eficacia una vez establecida.

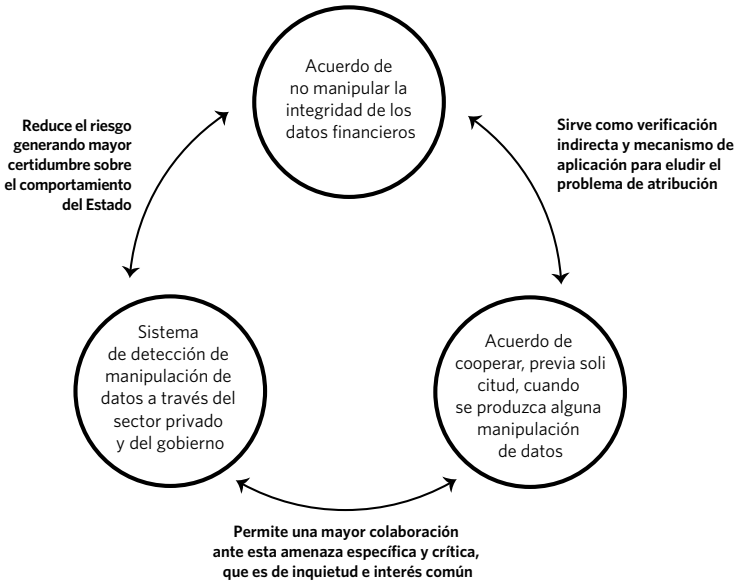
Obviamente, debido a las intrusiones de ciberinteligencia, otros países han comenzado a analizar la posibilidad de establecer limitaciones. Asimismo, deben abordarse cuestiones técnicas para determinar si sería posible distinguir entre intrusiones cibernéticas en sistemas financieros destinadas a recabar información de inteligencia, por un lado, e intrusiones que tienen por objeto la manipulación de datos, por otro. Se prohibiría instalar de manera encubierta cargas que puedan afectar la integridad de los datos financieros.

Teniendo esto en cuenta, el acuerdo propuesto tal como se describe con anterioridad tendría tres elementos relacionados que se refuerzan recíprocamente:

> Un Estado no debe debería realizar ni apoyar de forma deliberada actividades manipulen la integridad de los datos y algoritmos de las instituciones financieras, cualquiera sea el lugar donde se encuentren almacenados o cuando se encuentren en tránsito[25].
>
> En la medida que la ley lo permita, un Estado debería atender con prontitud las solicitudes de asistencia apropiadas de otro Estado para
>
> mitigar actividades que manipulen la integridad de los datos y algoritmos de las instituciones financieras, cuando esas actividades pasen a través de su territorio o emanen de él, o sean realizadas por sus ciudadanos.
>
> Estas disposiciones también se basan en la declaración contenida en el informe 2015 del UNGGE, que señala: "Los Estados no deben recurrir a terceros para cometer actos internacionalmente ilícitos mediante las TIC y deberían procurar garantizar que su territorio no sea utilizado por agentes no estatales para cometer tales actos"[26].

La característica importante de esta propuesta es que combina una norma negativa (es decir, los Estados se comprometen a *no hacer* algo) con otra positiva (es decir, los Estados se comprometen *a hacer* algo). También sería deseable que los Estados implementaran los actuales estándares sobre debida diligencia y las mejores prácticas, como las delineadas en las pautas sobre cibernética del CPMI y de la OICV de 2016. Si estos tres elementos se vincularan, la eficacia general de este régimen normativo sería mayor, como se muestra en el gráfico 1. Vincular el acuerdo que rige el comportamiento estatal con las expectativas relativas al sector privado de que se implementen estándares de debida diligencia aborda potenciales problemas de riesgo moral. El compromiso de los Estados de brindar asistencia e información, si estas fueran solicitadas, elude el problema de la atribución al desplazar la carga de la víctima del ataque a los Estados que manifiestan interés en ayudar a responder a los ataques y, en última instancia, a prevenirlos. Se esperaría que los Estados cumplan estas obligaciones ateniéndose a las limitaciones y los requerimientos del derecho nacional e internacional, que quizás haya que ajustar más adelante para reflejar las normas aquí descritas.

Gráfico 1. Tres pilares para un régimen efectivo y que se autoconsolide



Para que el acuerdo logre una adhesión recíproca efectiva y sea aceptado ampliamente entre los Estados Miembros de la ONU, no debería limitarse a una subcategoría de instituciones financieras, por ejemplo, los bancos de importancia sistémica mundial (según los enumera el Consejo de

Estabilidad Financiera) ubicados en una decena de países. Desde la perspectiva de la estabilidad internacional (y teniendo en mira lograr el apoyo de una gran cantidad de Estados), valdría la pena analizar si las garantías deben extenderse a las instituciones financieras de todos los Estados. La idea es que las ciberoperaciones que amenazan la integridad de cualquier institución financiera crearían precedentes e infundirían el temor de que pueden amenazar a todos los Estados.

La prohibición contemplada se aplicaría entre Estados. No se extendería a agentes no estatales (como terroristas) que operen en territorios sobre los cuales el Estado soberano nominal no pueda controlar. Si bien en muchos sentidos sería deseable un alcance más amplio, hay consideraciones prácticas que justifican una aplicación más acotada. Al principio, será difícil persuadir a los Estados de que acepten, sin implicar a agentes no estatales. A partir del momento en que los Estados clave suscriban un instrumento de términos similares a los del acuerdo aquí propuesto, y si eso ocurre, se podrá posteriormente trabajar para intentar ampliar su alcance, en cuanto a los agentes y blancos excluidos.

PROCESO: POSIBLES PRÓXIMOS PASOS PARA CONSOLIDAR LA NORMA

Si el acuerdo propuesto es deseable para los intereses nacionales y mundiales de los Estados clave, cabría preguntarse dónde anclarlo institucionalmente, cómo precisar mejor su aplicación y dónde buscar adherentes. El G20 ha surgido como el foro más prometedor donde los Estados podrían abordar las cuestiones que se analizan en este documento. Uno o más de esos Estados podrían promover esa idea e invitar a otros a perfeccionarla y apoyarla. Asimismo, la propuesta podría someterse a la consideración de diversos foros internacionales y organizaciones multilaterales.

Si el G20 determinara que es conveniente adoptar el acuerdo propuesto, podría:

- Incluir la redacción aquí propuesta (o una mejorada) en el comunicado de la cumbre de jefes de Estado del G20.
- Encargar al Consejo de Estabilidad Financiera
  - que implemente y anuncie el acuerdo ante los organismos de normalización pertinentes y las instituciones del sector privado, incluidos el CPMI, la OICV y el Comité de Basilea (esto incluiría analizar algunas de las cuestiones que se mencionan más abajo, por ejemplo, si la disponibilidad de determinados datos y sistemas debería incluirse y si el acuerdo debería cubrir todos los tipos de datos o algunos tipos de datos específicos, como datos basados en transacciones, datos operativos y datos de libros mayores/titularidad).
  - que elabore, para su presentación en la siguiente cumbre del G20, un informe que dé cuenta de los avances realizados y que incluya una hoja de ruta para su posterior implementación.

A diferencia de las medidas tomadas tras la crisis financiera de 2007–2008, para adoptar e implementar un acuerdo como el aquí propuesto se necesitaría de la participación de los CERT y de las comunidades de seguridad nacional de los distintos países. A la fecha, no hay ningún foro internacional donde puedan desarrollarse tales interacciones. No obstante, el Consejo de Estabilidad Financiera puede actuar como entidad convocante para ese proceso y podría trabajar con otras organizaciones no gubernamentales y recibir el apoyo de estas.

El Comité de Pagos e Infraestructuras del Mercado y la Organización Internacional de Comisiones de Valores son instituciones relevantes, sobre todo teniendo en cuenta su trabajo reciente. El Fondo Monetario Internacional es otra institución relevante, en el sentido de que es uno de los pocos foros donde se reúnen tanto representantes de ministerios de Finanzas como de los bancos centrales, dos grupos de actores interesados que son clave para esta propuesta. El interés del Foro Económico Mundial y su actuación en el pasado en materia de ciberseguridad presentan una oportunidad para llamar la atención de altos ejecutivos del sector privado sobre este tema. Se debe dar participación a estos ejecutivos, a fin de poder abordar correctamente los detalles técnicos que mejoren la verificabilidad y solidez de la norma. El Instituto de

Finanzas Internacionales (*Institute of International Finance*) es otra institución que podría trabajar en estas cuestiones junto con el sector financiero mundial.

Por último, es claro que existen limitaciones en cuanto al grado de vinculación que los funcionarios de las comunidades de seguridad nacional de cada país pueden tener con los gobiernos y expertos extranjeros en el sector financiero. Teniendo eso en cuenta, podemos prever un escenario donde un acuerdo internacional a través del G20 se complementaría con una serie de declaraciones unilaterales emitidas por cada gobierno o por sus fuerzas militares para reforzar la declaración del G20 y contribuir a la efectividad del acuerdo. Asimismo, los Estados que no forman parte del G20 podrían, sencillamente, realizar declaraciones unilaterales donde expresen que comparten el compromiso de los Estados miembros del G20.

Preguntas que deben abordarse

Hemos elaborado esta propuesta teniendo en cuenta las opiniones y comentarios de funcionarios gubernamentales, organizaciones internacionales relevantes e instituciones financieras de determinados países, entre ellos, Estados Unidos, Rusia, China, el Reino Unido, Singapur e Israel, a fin de evaluar sus propuestas. En general, las opiniones y comentarios han sido positivos; las presunciones básicas reseñadas en este memorando fueron confirmadas o ajustadas en oportunidades posteriores. Para que la norma goce de amplia aceptación y sea de práctica generalizada, las siguientes cuestiones deberían quedar aclaradas y abordarse más exhaustivamente durante el período en que se negocie e implemente. Invitamos a los lectores a analizarlas y a enviar sus respuestas a los autores o a otras partes interesadas.

1. ¿Cuál debería ser el alcance de las instituciones financieras?. ¿Son suficientes las definiciones y el alcance que se indican más abajo, o es necesario acotarlos o ampliarlos?[27]. En la siguiente terminología se incluyen definiciones ya acordadas en el comercio internacional, en especial, las definiciones definitivas negociadas como parte del Acuerdo de Asociación Transpacífico (*Trans-Pacific Partnership*, TPP) y con la comunidad financiera internacional.
   - "cualquier intermediario u otra empresa que esté autorizada para hacer negocios y esté regulada o supervisada como una institución financiera conforme la legislación de la Parte en cuyo territorio se encuentre ubicada" (esta es la definición de "institución financiera" que aparece en el texto definitivo del TPP para servicios financieros);
   - "una institución financiera, incluso una sucursal, ubicada en el territorio de una Parte que sea controlada por personas de otra Parte" (esta es la definición de "institución financiera de otra parte" que aparece en el texto definitivo del TPP para servicios financieros);
   - "cualquier entidad no gubernamental, incluso cualquier bolsa de valores o futuros o mercado, agencia de compensación, u otra organización o asociación, que ejerza autoridad reguladora o de supervisión sobre los prestadores de servicios financieros o instituciones financieras por ley o delegación del gobierno central o regional" (esta es la definición de "organismo regulador autónomo" que aparece en el texto definitivo del TPP para servicios financieros)[28]; y
   - "[s]istema multilateral entre entidades financieras participantes, incluido el operador del sistema, que se utiliza a efectos de compensar, liquidar o registrar pagos, valores, derivados u otras operaciones financieras" (esta es la definición de "infraestructura del mercado financiero" que aparece en BIS/OICV 2012 *Principios aplicables a las infraestructuras del mercado financiero*)[29].
2. Teniendo en cuenta que la falta de disponibilidad de determinados datos y sistemas podría tener un gran impacto en el sistema en su totalidad, ¿cómo podría agregarse disponibilidad y combinarse con el énfasis en la integridad de los datos dentro de un marco y una descripción efectivos? Por otro lado, ¿hay actividades maliciosas contra la disponibilidad que afecte la integridad de las transacciones? En ese caso, ¿de qué manera debería abordarse este problema?

3. En el contexto de un conflicto armado donde rige el derecho internacional humanitario, ¿puede distinguirse entre un ataque contra las estructuras físicas de las instituciones financieras y un ataque contra sus datos? En otras palabras, si se permite atacar a un banco por medios convencionales para destruir la moneda que este guarda de manera física, ¿no debería ser posible atacarlo por medios cibernéticos considerando el potencial daño colateral de estos últimos y, en especial, los efectos no deseados e imprevistos de las ciberoperaciones ofensivas?

4. Teniendo en cuenta que las instituciones financieras aprovechan los servicios en la nube para tercerizar parte de su gestión de datos a otras compañías, ¿es la redacción propuesta ("donde se encuentren almacenados") una manera efectiva de reflejar esta tendencia? ¿Es necesaria?

5. ¿Se aplicaría el acuerdo solo a los Estados que lo acepten o se esperaría que aquellos que acepten la norma apliquen sus requisitos y requerimientos frente a aquellos que no asumieron un compromiso de reciprocidad?

6. En términos más amplios, si una norma rechaza una actividad muy específica, ¿de qué manera los Estados evitarían dar la impresión de que toleran otras actividades que también pueden ser perniciosas? O a la inversa, ¿no es mejor elaborar una norma sencilla que dejar un ámbito totalmente fuera de su alcance?

7. Cuando se produce un incidente que implica la manipulación de la integridad de los datos de una institución financiera, ¿qué tipo de colaboración se espera que presten los Estados?

    a. ¿En qué áreas falta colaboración actualmente entre los equipos de respuesta a incidentes de seguridad informática y los organismos de aplicación de la ley?

    b. ¿Qué información se espera que compartan los Estados?

    c. ¿Debería esperarse que los Estados acepten equipos de investigación conjunta?

    d. ¿Debería esperarse que los Estados sancionen nuevas leyes o reformen las actuales para penalizar esa actividad en su territorio respecto de todos sus ciudadanos, independientemente de dónde se produzca la actividad, si es que aún no tienen normas de ese tipo?

    e. ¿Debería esperarse que los Estados respalden que el Consejo de Seguridad de la ONU aplique medidas punitivas si un Estado incurre en violaciones? ¿Es necesario que el Estado sea parte del acuerdo o debería el acuerdo complementarse con una resolución del Consejo de Seguridad de la ONU que disponga que se aplica a todos los miembros de esa organización?

    f. ¿Cuáles son las mejores prácticas que los miembros del Convenio sobre la Ciberdelincuencia pueden adoptar para este tipo de incidente más específico?

    g. ¿Qué medidas deberían incluirse, además de los actuales mecanismos de cooperación entre los miembros del Convenio sobre la Ciberdelincuencia?

    h. ¿Cómo debería ser un modelo que incorpore estos detalles?

8. ¿Pueden desarrollarse técnicas para detectar intrusiones que vulneren la integridad de los datos de las instituciones financieras? ¿Pueden desarrollarse técnicas para distinguir entre intrusiones destinadas a recabar información de inteligencia y aquellas que también tienen la potencialidad de corromper datos?

9. ¿Qué requisitos y régimen de notificaciones deberían implementarse para que los Estados tomen conocimiento de tales incidentes? ¿Qué protecciones deben existir?

Por último, reconocemos que otros sectores, como el de las telecomunicaciones y el de la energía, así como la integridad de los datos de otros sistemas son fundamentales para el sistema financiero. Sin embargo, es incluso más difícil negociar e implementar eficazmente acuerdos que abarquen a estos sectores. Por lo tanto, ofrecemos esta propuesta como punto de partida de un proceso que, probablemente, tomará bastante tiempo, hasta que pueda implementarse un régimen de seguridad integral efectivo.

CUADRO 1: Resumen de algunas entidades importantes para las actividades de extensión y participación

Miembros Permanentes del Consejo de Seguridad de La Onu	Miembros del G20	Miembros del Ungge 2014–2015	Miembros del Ungge 2016-2017	Comité de Supervisión Bancaria De Basilea	Países Con Bancos de Importancia Sistémica Mundial	Países Con Aseguradoras de Importan-cia Sistémica Mundial	Miembros del G7
China	China	China	China	China	China	China	
Francia	Francia	Francia	Francia	Francia	Francia	Francia	Francia
Rusia	Rusia	Rusia	Rusia	Rusia			
Reino Unido	Reino Unido	Reino Unido	Reino Unido	Reino Unido	Reino Unido	Reino Unido	Reino Unido
Estados Unidos	Estados Unidos	Estados Unidos	Estados Unidos	Estados Unidos	Estados Unidos	Estados Unidos	Estados Unidos
	Argentina			Argentina			
	Australia		Australia	Australia			
	Brasil	Brasil	Brasil	Brasil			
	Canadá		Canadá	Canadá			Canadá
	Alemania	Alemania	Alemania	Alemania	Alemania	Alemania	Alemania
	India		India	India			
	Indonesia		Indonesia	Indonesia			
	Italia	Italia		Italia	Italia		Italia
	Japón	Japón	Japón	Japón	Japón		Japón
	México	México	México	México			
	Arabia Saudita			Arabia Saudita			
	Sudáfrica			Sudáfrica			
	Corea del Sur	Corea del Sur	Corea del Sur	Corea del Sur			
	Turquía			Turquía			
		Bielorrusia					
		Colombia					
		Egipto	Egipto				
		Estonia	Estonia				
		Ghana					
		Israel					
		Kenia	Kenia				
		Malasia					
		Pakistán					
		España		España	España		
			Países Bajos	Países Bajos	Países Bajos	Países Bajos	
			Suiza	Suiza	Suiza		
				Bélgica	Bélgica		
				Suecia	Suecia		
			+ Botswana, Cuba, Finlandia, Kazajistán, Serbia, Senegal	+ Hong Kong*, Luxemburgo, Singapur			

APÉNDICE: ANÁLISIS DE INCIDENTES CIBERNÉTICOS QUE HAN AFECTADO A INSTITUCIONES FINANCIERAS

En esta sección se describen incidentes cibernéticos significativos que tuvieron como blanco instituciones financieras de todo el mundo, ocurridos entre 2011 y diciembre de 2016, y se añaden además algunos incidentes importantes específicos que se produjeron entre 2007 y 2011. Vale la pena señalar que no existen datos públicos que indiquen que en alguno de los incidentes sobre manipulación de la integridad de datos de instituciones financieras hayan participado Estados; esto sugiere que, hasta el momento, los Estados se han abstenido de realizar estos actos. Como excepción, podemos mencionar el ataque que, presuntamente, llevó a cabo Corea del Norte contra instituciones financieras de Corea del Sur en el cual se borraron discos duros y, quizás, los ataques distribuidos de denegación de servicio (DDoS), de baja intensidad, contra instituciones financieras rusas en diciembre de 2016.

Los incidentes cibernéticos que se mencionan en el cuadro más adelante incluyen modificaciones no autorizadas (*defacement*) en sitios web, ataques DDoS e intrusiones con tipos de *malware* más sofisticados. Los principales objetivos de los incidentes fueron bancos, pero también una bolsa de valores y un sistema de pago, y entre los países cuyos sectores financieros fueron afectados se encuentran Bélgica, Brasil, Corea del Sur, Estados Unidos, Estonia, Georgia, el Líbano, Rusia y Ucrania. Aunque en muchos casos es difícil saber con certeza quiénes cometieron el ataque, entre los presuntos responsables se encuentran desde delincuentes y grupos de piratería informática que actúan de manera independiente, hasta *hackers* que operan con el aval de Estados e incluso Estados mismos. Este análisis formó parte de la investigación preliminar que realizaron los autores y respaldó la presunción de que los Estados ya se abstienen considerablemente de realizar este tipo de acciones, en comparación con lo que sería posible desde el punto de vista técnico.

CUADRO 2: Resumen de ciberataques y fechas

Resumen	Fecha
Ataques DDoS contra bancos rusos	Fines de 2016
Golpe al Banco Central de Bangladés	Principios de 2016
Incidente en el Banco Nacional Belga	Principios de 2016
Manipulación del Índice Compuesto de Shanghái (incierto)	2015–2016
Robo de bancos rusos	Fines de 2015
Manipulación de la moneda rusa	Principios de 2015
Ataque del *malware* Metel contra bancos rusos	2015
Vulneración de datos del Ministerio de Finanzas ucraniano	Mediados de 2015
Vulneración de la seguridad en la Bolsa de Valores de Varsovia	Fines de 2014
Vulneración de la seguridad de datos en bancos ucranianos	Mediados de 2014
Ataque con *malware* Carbanak	2013-2015
Ataques con Dark Seoul en Corea del Sur	Principios de 2013
Vulneración de la seguridad de los datos de JPMorgan	2012-2015
Ataques DDoS contra bancos brasileños	2012 y 2014
Ataque contra sistema de pago brasileño	2012-2014
Ataques DDoS contra bancos estadounidenses	2012-2013
Manipulación del Índice Compuesto de Shanghái (incierto)	Mediados de 2012
Infecciones con el virus Gauss en el Líbano	2011-2012
Ataque contra bancos surcoreanos	Mediados de 2011
Intrusión en el Nasdaq	Fines de 2010
Modificaciones no autorizadas en sitio web de Georgia	Mediados de 2008
Ataques DDoS contra entidades estonias	Mediados de 2007

Ataques DDoS contra instituciones financieras rusas en 2016

El 2 de diciembre, el Servicio de Seguridad Federal ruso anunció el descubrimiento de que se estaban planificando ciberataques contra "varios importantes bancos rusos" a partir del 5 de diciembre[30]. Los servidores y centros de comando que, supuestamente, se utilizarían para estos ataques se

encontraban en los Países Bajos y pertenecían a una empresa ucraniana de alojamiento web denominada BlazingFast. Su director, Anton Onoprichuk, afirmó no tener información sobre los ataques anunciados y que su empresa no pudo encontrar datos maliciosos. El ministro de Seguridad y Justicia holandés manifestó que tenía conocimiento de que su infraestructura podía utilizarse para perpetrar ciberataques en otros sitios y señaló en una declaración que "si el lunes… se produce efectivamente un ciberataque, corresponderá a las autoridades rusas decidir si inician o no una investigación… Si lo desean, pueden solicitar asistencia a las autoridades de investigación holandesas"[31].

El 9 de diciembre, la operadora de telecomunicaciones rusa Rostelecom declaró que el 5 de diciembre había bloqueado ataques DDoS contra los cinco bancos e instituciones financieras más importantes de Rusia. Alcanzaron un volumen máximo de 3,2 millones de paquetes por segundo, una cantidad baja si se la compara con el volumen de otros ataques DDoS recientes, y el ataque más prolongado duró algunas horas. En la declaración también se señaló que en algunos de los ataques DDoS se utilizó un *botnet* similar al usado semanas antes contra Deutsche Telekom de Alemania y Eircom de Irlanda, que aprovechó una vulnerabilidad de los enrutadores internos[32].

No se identificó a agentes estatales o autores del ataque, aunque el Servicio de Seguridad Federal ruso alegó que la acción estaba siendo organizada por "servicios de inteligencia extranjeros" y persistieron las especulaciones de que, teniendo en cuenta dónde se encontraban los servidores y a quién pertenecían, esta acción se había realizado en nombre de Ucrania[33]. El Servicio de Seguridad Federal ruso señaló que esperaba que los ataques DDoS estuvieran acompañados de mensajes de texto, publicaciones en las redes sociales orientadas a causar conmoción y declaraciones de *blogs* acerca de una "crisis en el sistema crediticio y financiero de Rusia, la quiebra y la revocación de licencias de los principales bancos federales y regionales" y que "la campaña [estaría] dirigida a varias decenas de ciudades rusas"[34]. Supuestamente, con esto se intentaría generar una corrida en los bancos rusos que propiciara una crisis financiera. No existen pruebas de que, adicionalmente a los ataques DDoS, se haya intentado realizar ese tipo de acción.

Golpe contra el Banco Central de Bangladés en 2016

En febrero, los medios informaron que *hackers* se habían colado en la red del Banco Central de Bangladés y enviado treinta y cinco solicitudes fraudulentas de transferencia al Banco de la Reserva Federal de Nueva York, por un total de casi USD 1.000 millones[35]. Cuatro de esas solicitudes fraudulentas fueron aceptadas y los *hackers* pudieron transferir USD 81 millones a cuentas en las Filipinas, en lo que fue uno de los robos a bancos más importantes de la historia[36]. La quinta solicitud de envío de USD 20 millones a una cuenta en Sri Lanka pudo detenerse cuando un error de ortografía en el nombre del destinatario ("Shalika Fandation" en lugar de "foundation") levantó sospechas[37]. Las restantes transferencias, por un total de entre USD 850 y USD 870 millones, también pudieron detenerse antes de que se completaran[38].

Los *hackers* habían introducido un programa informático malicioso (*malware*) en el servidor del Banco Central de Bangladés e instalaron un *software keylogger* que les permitió robar las credenciales del banco para acceder al sistema SWIFT. Asimismo, crearon específicamente un conjunto de herramientas de *malware* que pusieron en peligro el sistema Alliance Access de SWIFT y que estuvieron diseñadas para cubrir sus rastros[39]. Con este conjunto de herramientas también pudieron eliminar registros de solicitudes de transferencia, eludir controles de validez, eliminar registros de ingresos, manipular presentaciones de informes de estados de cuentas y evitar que las impresoras conectadas imprimieran registros de transacciones. Si bien el *malware* estaba especialmente diseñado para ese robo, el conjunto de herramientas podía llegar a utilizarse contra otros bancos del sistema SWIFT que utilizaran el *software* Alliance Access.

Los ciberdelincuentes habían monitoreado las actividades habituales del banco y luego generaron solicitudes de transferencias de dinero que aparentaban ser genuinas y programaron los robos de modo que cuando la Reserva Federal intentó pedir

una confirmación de las transacciones, era ya fin de semana en Bangladés, y luego, cuando los empleados del Banco Central de Bangladés ordenaron a la Reserva Federal que cancelara las transacciones, era ya fin de semana en Nueva York.

Ataque DDoS al Banco Nacional Belga en 2016

El 22 de febrero, un grupo de *hackers* denominado DownSec Belgium hizo caer el sitio web del Banco Nacional Belga durante gran parte de la mañana mediante ataques DDoS[40]. Aunque no se ha proporcionado demasiada información sobre el ataque, sucedió luego de otros ataques DDoS similares perpetrados por el mismo grupo contra los sitios web de la Agencia Federal de Control Nuclear de Bélgica, el Centro de Crisis de ese país y el equipo federal de ciberemergencias de Bélgica. DownSec Belgium proclama luchar contra los abusos de gobiernos corruptos.

Caída en el Mercado de Valores de Shanghái en 2015 (incidente incierto)

A partir del 12 de junio, el Índice Compuesto de Shanghái comenzó a derrumbarse y para el 19 de junio había caído un 13 %[41]. Los mercados de valores chinos continuaron cayendo durante julio y agosto, y de vuelta en enero y febrero de 2016[42]. Si bien no hay pruebas públicas, algunos han especulado que el derrumbe repentino puede haber sido consecuencia de un ciberataque[43].

Robos de bancos rusos a sus propios clientes en 2015

Aunque actualmente hay escasa información sobre este incidente, hace poco *SC Magazine UK* informó que, en 2015, el Banco Central de Rusia revocó las licencias de tres bancos de ese país tras descubrir en una investigación que algunos empleados y exempleados habían utilizado ciberataques para retirar dinero de cuentas de sus propios clientes y para encubrir otros delitos y transgresiones cometidos por los bancos[44]. El Banco Central de Rusia informó que, solo en el último trimestre de 2015, más de USD 20 millones fueron robados de las cuentas de clientes. Esa institución tiene la sospecha de que el delito se cometió con el conocimiento o la participación directa de los propios bancos. El Banco Central también informó que esos actos de piratería informática probablemente fueron consecuencia de los enormes recortes que la industria financiera rusa había experimentado durante el año anterior y que, debido a esos recortes, por un lado, algunos exempleados bancarios insatisfechos habían estado dispuestos a colaborar con *hackers* y, por el otro, los bancos no habían deseado o no pudieron afrontar el costo de actualizar sus medidas de ciberseguridad.

Manipulación de moneda con *malware* a través de un banco ruso en 2015

Un grupo de *hackers* que se comunicaban en ruso utilizaron un virus denominado Corkow Trojan para realizar ingresos no autorizados, a partir de septiembre de 2014, en los sistemas informáticos del banco Energobank, con casa central en Rusia[45]. Así pudieron hacerse de credenciales, lanzar su propio *software* de operaciones y, el 27 de febrero de 2015, colocaron más de USD 500 millones en órdenes a tasas que no eran las del mercado. De esta forma, consiguieron que durante catorce minutos el tipo de cambio oscilara con extrema volatilidad entre 55 y 66 rubros por dólar[46]. Es interesante señalar que, presuntamente, los *hackers* no habrían obtenido ganancias significativas de la operación en sí, aunque es posible que aprovecharan sus conocimientos internos para obtener ganancias en otros mercados. También es posible que este ataque fuera una prueba piloto para otros futuros. Energobank ha informado pérdidas por USD 3,2 millones como resultado de las operaciones.

Ataque del *malware* Metel contra bancos rusos en 2015

Un grupo de ciberdelincuentes utilizaron el ya conocido troyano para bancos Metel para robar directamente a los bancos, en lugar de a los usuarios finales. La banda delictiva (que se cree que estaría conformada por menos de diez miembros) utilizó mensajes de correo electrónico fraudulentos a destinatarios específicos para obtener sus datos (*spear phishing*) o aprovechó las vulnerabilidades de los navegadores para infiltrarse en los sistemas bancarios que tenían acceso a transacciones de dinero, como las computadoras utilizadas por los operadores de centros de llamadas o los equipos de soporte de los bancos.

Una vez dentro, el *malware* Metel automatizó la reversión de las transacciones en cajeros automáticos. Con esto, el grupo delictivo pudo utilizar tarjetas de los bancos afectados para retirar cantidades de dinero prácticamente ilimitadas, dado que, después de cada transacción, el saldo de la cuenta volvía al mismo valor de manera automática. No se han detectado infecciones de este tipo fuera de Rusia[47].

Violación a la seguridad de los datos del Ministerio de Finanzas ucraniano en 2015

En mayo, el grupo de *hackers* activistas prorrusos CyberBerkut se atribuyó el ingreso no autorizado en la red del Ministerio de Finanzas de Ucrania[48]. El grupo publicó lo que, según ellos, eran documentos robados de la red, que demostraban que Ucrania no podía pagar su deuda externa. Se desconoce la veracidad de lo alegado por el grupo y de qué manera, se supone, tuvieron acceso a la red del Ministerio. Información adicional sobre CyberBerkut está disponible en el registro sobre violación a la seguridad de datos en Ucrania de 2014.

Vulneración de la seguridad en la Bolsa de Valores de Varsovia en 2014

En octubre, un grupo que se decía vinculado al denominado Estado Islámico ingresó sin autorización en las redes internas de la Bolsa de Valores de Varsovia y publicó en línea decenas de credenciales de inicio de sesión de corredores[49]. Se desconoce de qué manera el grupo tuvo acceso a las redes de la bolsa, pero se supone que pudieron infiltrar un simulador de inversiones y un portal web para gestionar el paso de la Bolsa de Valores a un nuevo sistema mejorado de transacciones, e inhabilitaron el sitio web de la bolsa de valores por dos horas[50]. Los empleados de la bolsa afirman que no hubo violación a la seguridad del sistema de operaciones en sí mismo. Más tarde, funcionarios de la Organización del Tratado del Atlántico Norte (OTAN) señalaron en privado que creían que no era cierto que el grupo de piratería informática estuviera vinculado con milicias de Estado Islámico, y que, en realidad, la vulneración la llevó a cabo APT 28, un grupo que muchos especialistas en seguridad creen que tienen nexos con el gobierno ruso[51].

Vulneración de la seguridad de datos en bancos ucranianos en 2014

En julio, el grupo prorruso denominado CyberBerkut ingresó sin autorización en los sistemas de PrivatBank, uno de los bancos comerciales más importantes de Ucrania, y publicó datos robados de clientes en VKontakte, un sitio web de medios sociales de Rusia[52]. Se desconoce de qué manera tuvieron acceso a los datos. Se cree que atacaron PrivatBank porque uno de los copropietarios del banco, Igor Kolomoisky, había ofrecido una recompensa de USD 10.000 por la captura de milicianos respaldados por los rusos en Ucrania[53]. CyberBerkut advirtió a los clientes de PrivatBank que transfirieran su dinero a bancos estatales. Es posible que CyberBerkut tenga conexiones con el gobierno ruso, pero dada la relativa falta de sofisticación de sus ataques, algunos expertos han llegado a la conclusión de que es poco probable que existan vínculos oficiales[54].

Ataque con *malware* Carbanak contra varios bancos entre 2013 y 2015

Un grupo delictivo utilizó el *malware* Carbanak para atacar instituciones financieras, entre ellas, bancos y sistemas de pago electrónico, en casi treinta países. El *malware* instaló un instrumento de acceso remoto (*remote access tool*, RAT) por medio del cual los delincuentes pudieron vigilar las operaciones diarias de los bancos mediante videos y fotografías durante varios meses[55]. El grupo pudo, entonces, dar instrucciones a los cajeros automáticos de que entregaran efectivo en las terminales y hacerse pasar por funcionarios del banco para ordenar transferencias fraudulentas. Sin embargo, los montos de dinero más significativos fueron robados cuando estas personas, simulando ser funcionarios del banco, ingresaron sin autorización en los sistemas contables de los bancos y manipularon los saldos de las cuentas aumentando los montos disponibles y transfiriendo luego la cantidad adicional, de modo tal que el saldo después volvía a ser el original. Entre los países afectados estuvieron, por ejemplo, Alemania, Australia, Brasil, Bulgaria, Canadá, China, España, Estados

Unidos, Francia, Hong Kong, Islandia, India, Irlanda, Marruecos, Nepal, Noruega, Pakistán, Polonia, el Reino Unido, la República Checa, Rumania, Rusia, Suiza, Taiwán y Ucrania[56].

Ataque de *malware* contra bancos surcoreanos en 2013

Este ataque se produjo el 20 de marzo y utilizó el *malware* denominado Dark Seoul contra las redes informáticas de tres bancos surcoreanos —Shinhan, Nonghyup y Jeju—. Como consecuencia, se borraron datos y hubo problemas en cajeros automáticos y en sistemas de pago móviles[57]. Los servidores de banca por Internet de Shinhan Bank estuvieron temporalmente bloqueados durante parte del día, por lo cual los clientes no pudieron realizar operaciones en línea. Por su parte, las operaciones en algunas sucursales de Nonghyup y Jeju estuvieron paralizadas por dos horas después de que el virus borró archivos en las computadoras infectadas. Un cuarto banco, Woori, denunció actividades de piratería informática pero no sufrió daños. Los ataques también afectaron a varias organizaciones de medios coreanas; sus computadoras quedaron paralizadas, pero pudieron seguir transmitiendo con normalidad[58]. Corea del Sur atribuyó el ataque a Corea del Norte[59].

Red delictiva responsable de la vulneración de la seguridad de los datos de JPMorgan entre 2012 y 2015

En agosto de 2014, JPMorgan denunció una vulneración masiva de la seguridad de los datos, en la cual *hackers* accedieron a la información de contacto de más de 80 millones de titulares de cuentas. Esto representó la violación a la seguridad de datos de una institución financiera estadounidense más importante de la historia[60]. Si bien al principio se especuló que el gobierno ruso había estado involucrado[61], en noviembre de 2015 las autoridades federales procesaron a cuatro hombres por la vulneración. Los acusados manifestaron que ese hecho formó parte de una enorme operación que involucraba actos de piratería informática en otras instituciones financieras, un plan para aumentar artificialmente los precios de las acciones y operaciones de juego en línea que, en total, les habían generado una suma neta de USD 100 millones[62]. Los delincuentes utilizaron las cuentas de correo electrónico que habían obtenido al ingresar sin autorización en los sistemas de JPMorgan para manipular el precio de las acciones y, además, tenían la intención de establecer su propia empresa de corretaje usando los datos robados para ponerse en contacto con posibles clientes[63]. Si bien el acto de piratería informática contra JPMorgan fue el de mayor envergadura que llevó adelante esa red, también ingresaron sin autorización en los sistemas de otras seis instituciones financieras, Scottrade, E-Trade, Dow Jones (la compañía controlante propietaria de *The Wall Street Journal*), otra organización de noticias financieras y varias empresas de corretaje de acciones en línea[64].

Ataques DDoS contra bancos brasileños en 2012 y 2014

En enero de 2012, el grupo de *hackers* Anonymous utilizó ataques DDoS para deshabilitar los sitios web de algunos de los bancos más importantes del país, según ellos, como medida de protesta contra la corrupción y la desigualdad en Brasil[65]. Los ataques, que el grupo denominó #OpWeeksPayment, hicieron caer los sitios web del Banco do Brasil, Itaú Unibanco y Bradesco, entre otros, durante varias horas cada vez[66].

En junio de 2014, Anonymous lanzó otra serie de ataques DDoS, esta vez a modo de protesta contra el Mundial de Fútbol.[67] Los ataques, llamados #OpHackingCup, hicieron caer varios sitios web brasileños, entre ellos, el del Banco do Brasil. Otros sitios web atacados fueron, por ejemplo, el del gobierno brasileño, el de Hyundai Brasil y el sitio oficial del Mundial de Fútbol[68].

Ataque de *malware* contra sistema de pago brasileño entre 2012 y 2014

Un grupo de ciberdelincuentes utilizaron el *malware* tipo "hombre en el navegador" para atacar Boleto Bancario, un conocido sistema de pago brasileño. Con este sistema de pago, los comercios pueden emitir boletos en papel o en línea con un código de barras que los clientes pueden usar parar enviar dinero a un banco[69]. El *malware* se inyectó a sí mismo en navegadores de casi 200.000 computadoras infectadas, donde pudo interceptar y alterar boletos legítimos y enviar pagos a las cuentas de los *hackers*[70]. El ataque puso en riesgo USD 3.750 millones en transacciones, aunque no queda claro cuánto de ese dinero los criminales pudieron depositar en sus propias cuentas[71].

Ataques DDoS contra instituciones financieras estadounidenses entre 2012 y 2013

Se produjeron dos olas coordinadas de ataques DDoS contra sitios web de instituciones financieras estadounidenses: la primera entre septiembre y octubre de 2012 y la segunda entre diciembre de 2012 y enero de 2013[72]. Un grupo de *hackers* activistas islámicos, llamado Izz ad-Din al-Qassam Cyber Fighters, se atribuyó la responsabilidad por los ataques, a los que denominaron Operación Ababil[73]; sin embargo, funcionarios del gobierno de EE. UU. han señalado en privado a medios de comunicación que creen que Irán sería responsable por los hechos[74]. La magnitud de los ataques no tuvo precedentes en cuanto a la cantidad de instituciones financieras afectadas y el volumen de tráfico que inundó las redes. Un especialista en seguridad comentó que "nunca ha habido tantas instituciones financieras sometidas a tal nivel de coacción"[75]. Si bien en ambas oportunidades el grupo anunció anticipadamente los ataques y los objetivos, los bancos no pudieron defenderse y el acceso a los sitios web de numerosas instituciones financieras estadounidenses se vio alterado, entre ellas, Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T y HSBC[76]. Hasta el momento, la adopción de medidas defensivas y correctivas ha supuesto un costo para los bancos de millones de dólares[77]. Izz ad-Din al-Qassam Cyber Fighters anunció otras dos olas de ciberataques en 2013, pero habrían sido menos efectivas[78].

Posible manipulación de la Bolsa de Valores de Shanghái en 2012 (incidente incierto)

El 4 de junio, el Índice Compuesto de Shanghái abrió con una cifra de 2.346,98 y para el cierre había caído exactamente 64,89 puntos[79]. El 4 de junio es la fecha aniversario de la infame represión de las manifestaciones estudiantiles ocurrida ese día de 1989 en la plaza Tiananmén de Pekín. Muchos en China especularon que ambas cifras tenían por objeto representar el aniversario de la tragedia[80]. La cantidad 2.346,98 puede leerse, de derecha a izquierda, como el año, el mes y la fecha, seguido del número 23 para representar que 2012 marcaba el vigésimo tercer aniversario de las manifestaciones. De manera similar, muchos observadores en China especularon que los 64,89 puntos que cayó el mercado ese día también representaban la fecha 6/4/89. La aparente coincidencia disparó las especulaciones, nunca demostradas, de que el índice podía haber sido objeto de piratería informática y de que fue manipulado para producir esos números. La numerología es muy importante en la cultura China, y se sabe que, en el pasado, los ciudadanos de ese país han utilizado los números como una forma sutil de protesta.

Virus Gauss infecta bancos libaneses en 2011 y 2012

El 9 de agosto de 2012, la empresa rusa de seguridad Kaspersky Lab anunció el descubrimiento del virus Gauss, diseñado para robar datos de bancos libaneses —entre ellos, el Banco de Beirut, EBLF, Banco BLOM, ByblosBank, Fransabank y Credit Libanais— así como de usuarios de Citibank y PayPal[81]. Los expertos de Kaspersky llegaron a la conclusión de que el virus es un *malware* patrocinado por un Estado y diseñado por los creadores de Stuxnet, Flame y la colección Duqu de troyanos de espionaje[82]. Más de 2500 computadoras de clientes de Kaspersky fueron infectadas en veinticinco países distintos —1660 de ellas en el Líbano—, aunque la empresa de seguridad advierte que la cantidad total de máquinas infectadas puede llegar a decenas de miles[83].

Una vez que una PC se ha infectado, el troyano roba información detallada, como el historial del navegador, contraseñas, *cookies*, configuraciones del sistema y credenciales de cuentas bancarias en línea, e instala, además, una fuente especial llamada Palida Narrow, cuyo propósito se desconoce[84]. Lo más interesante es que Gauss contiene una carga encriptada que los especialistas en seguridad no han podido descifrar y que indica la presencia de un contenido importante que los creadores del virus claramente han considerado que debe protegerse[85]. Dado que el Líbano es un centro bancario para toda la región de Oriente Medio y que la falta de transparencia de los bancos de ese país ha provocado a menudo inquietud entre las autoridades de regulación financiera que intentan

desarticular el financiamiento del terrorismo y el lavado de dinero, parece probable que el virus podría estar diseñado para controlar o desarticular flujos de dinero que se considera que pueden ser una amenaza para la seguridad nacional del Estado patrocinante[86].

Ataque con *malware* contra un banco surcoreano en 2011

Este incidente que atacó las operaciones bancarias de Nonghyup, una cooperativa agrícola surcoreana, comenzó el 12 de abril. El *malware* infectó los sistemas de Nonghyup en septiembre de 2010, cuando un subcontratista lo descargó de manera involuntaria en una computadora portátil, que los atacantes utilizaron para propagar el *malware* en las redes del banco[87]. El ataque destruyó los registros de algunos usuarios de tarjeta de crédito y provocó una caída del servicio durante tres días, lo cual afectó los cajeros automáticos, la banca en línea y móvil, y el uso de tarjetas de crédito. Corea del Sur atribuyó el ataque a Corea del Norte[88].

Intrusión en el Nasdaq en 2010

La intrusión en las redes del Nasdaq fue revelada por *Bloomberg Business* en exclusiva, y por primera vez, en 2014[89]. En octubre de 2010, el FBI detectó una intrusión en los servidores de las computadoras del Nasdaq. La intrusión utilizó dos vulnerabilidades de día cero similares al *malware* diseñado en el pasado por la principal agencia de inteligencia rusa, el Servicio de Seguridad Federal. El *malware* ingresó, primero, a través de Directors Desk del Nasdaq, un sistema que utilizan cientos de compañías para que los miembros de sus juntas directivas compartan información financiera confidencial. Según una declaración del propio Nasdaq en ese momento, la intrusión se limitó solo a ese sistema, aunque *Bloomberg* informó que, en realidad, existía la posibilidad de que la intrusión se hubiera expandido más ampliamente a través de las redes de la bolsa de valores, si bien nunca ingresó en la plataforma de transacciones.

En un principio, la Agencia de Seguridad Nacional (*National Security Agency*, NSA) consideró que el *malware* tenía la capacidad de interrumpir de manera generalizada en las redes informáticas de la Nasdaq y, posiblemente, de anular toda la bolsa. También había indicios de que se había robado un importante caché de datos, aunque los investigadores tenían pocas pruebas sobre qué fue exactamente lo que se llevaron. Más tarde, la Agencia Central de Inteligencia (*Central Intelligence Agency*, CIA) sostuvo que el *malware* tenía un poder de destrucción menor al que se pensó en un primer momento, y que, si bien no podía anular por completo un sistema informático, sí podía apoderarse de algunas funciones y utilizarlas para alterar la red. Finalmente, los investigadores concluyeron que el principal objetivo de la intrusión había sido robar tecnología crítica de propiedad exclusiva para que Rusia pudiera imitarla o incorporarla en sus propias bolsas de valores en un intento por convertir a Moscú en un centro financiero internacional. El *malware* no se ha analizado públicamente, y los informes de *Bloomberg* presentaron pocas precisiones. Por tanto, no se encuentra disponible más información técnica sobre el *malware* y sus capacidades en la bibliografía de código abierto.

Modificaciones no autorizadas en sitio web durante el conflicto armado ruso-georgiana en 2008

Las ciberoperaciones ofensivas contra objetivos en Georgia comenzaron el 20 de julio, antes de que se desencadenara el conflicto armado, y continuaron hasta mediados de agosto, cuando el conflicto terminó[90]. Esta fue la primera vez en la historia que se combinaron ciberoperaciones ofensivas con un conflicto armado, y se supone que fue el gobierno ruso o *hackers* activistas rusos vinculados con el gobierno los que llevaron adelante estas operaciones[91]. El día en que el conflicto armado comenzó, aparecieron en sitios web listas de páginas que se atacarían e instrucciones precisas y formularios de encuestas para que los *hackers* informaran sus acciones después del hecho, demostrando así que existía un grado revelador de preparación y que se sabía con anticipación sobre el inicio del conflicto[92]. Las operaciones consistieron en la manipulación no autorizada de sitios web y en ataques DDoS, y entre los objetivos estuvieron el sitio web del presidente georgiano y otros sitios gubernamentales. El único impacto en el sector financiero fue la manipulación no autorizada del sitio web del Banco Nacional de Georgia[93].

Ataques DDoS contra Estonia, incluidos bancos estonios, en 2007

El 26 de abril comenzaron una serie de ataques DDoS coordinados contra sitios web del gobierno, bancos, universidades y periódicos de Estonia, que duraron tres semanas[94]. En la primera semana, los ataques DDoS únicamente tuvieron como blanco sitios web y servidores de correo electrónico del gobierno y de partidos políticos, mientras que durante la segunda semana la lista se amplió también a sitios web de medios de noticias de Estonia[95]. Para poder restablecer la actividad en línea de sus sitios web, los administradores de redes tuvieron que cerrarlos al tráfico extranjero, y esto hizo, paradójicamente, que la posibilidad de los medios estonios de informar al resto del mundo lo que estaba ocurriendo quedara limitada.

La tercera ola del ataque, que comenzó el 9 de mayo, fue la más intensa y se concentró en el sector bancario de Estonia[96]. Debido a estos ataques, dos importantes bancos estonios (incluido Hansabank, el más importante del país) tuvieron que suspender sus operaciones de banca en línea, cortar la conexión del banco con los cajeros automáticos y avisar a los clientes que no usaran las tarjetas de débito estonias fuera del país[97]. Esta ola de ataques se agudizó el 9 y 10 de mayo y luego fue mermando en forma gradual hasta el 19 de mayo, cuando, aparentemente los contratos de *botnet* de los hackers vencieron[98].

Los ataques fueron perpetrados por *hackers* activistas rusos que se comunicaban abiertamente en ruso en salas de *chat*, donde los usuarios compartían instrucciones precisas sobre cómo realizar los ataques. Estonia responsabilizó al gobierno ruso de ordenar los ataques, pero no pudo producir pruebas concluyentes[99].

AGRADECIMIENTOS

Los autores desean agradecer a Taylor Brooks, Steven Nyikos y Elizabeth Whitfield por la ayuda prestada para esta publicación, así como a los casi cincuenta funcionarios y expertos de más de diez países que nos brindaron sus comentarios y opiniones.

NOTAS

1. Ministros de Finanzas y gobernadores de los bancos centrales del G20, "Comunicado", University of Toronto, 18 de marzo de 2017, http://www.g20.utoronto.ca/2017/170318-finance-en.html.
2. Se puede consultar en el apéndice un análisis detallado de este y otros incidentes cibernéticos que se han producido en relación con instituciones financieras. Krishna N. Das y Jonathan Spicer, "The SWIFT Hack—How the New York Fed Fumbled Over the Bangladesh Bank Cyber-Heist", Reuters, 21 de julio de 2016, http://www.reuters.com/investigates/special-report/cyber-heist-federal/.
3. Es probable que aumente la dependencia de los Estados en los datos financieros y también la interdependencia del sistema. Por ejemplo, en diciembre de 2015, el periódico *The New York Times* publicó un artículo sobre la iniciativa del Gobierno sueco de implementar en el país una economía que funcionara absolutamente sin efectivo, y la ONU, a través de su programa Better Than Cash Alliance, apoya a varios países que proyectan que sus economías funcionen sin efectivo. El gobierno de la India también está intentando que su economía funcione prescindiendo del efectivo.

   Ver Liz Alderman, "In Sweden, a Cash-Free Future Nears", *The New York Times*, 26 de abril de 2015, http://www.nytimes.com/2015/12/27/business/international/in-sweden-a-cash-free-future-nears.html?_r=0; Better Than Cash Alliance, consultado el 21 de abril de 2016, https://www.betterthancash.org/; "From Eradicating Black Money to Cashless Economy: PM Modi's Changing Narrative Since Demonetisation", *Indian Express*, 22 de diciembre de 2016, http://indianexpress.com/article/india/demonetisation-modi-cashless-economy-black-money-narratives-4439843/.
4. En este tipo de acuerdo puede incluirse el *malware* cuya función sea borrar discos, pero no abarcaría actividades para descifrar criptografía que se realicen con el objeto de recabar datos de inteligencia. También proponemos que los Estados analicen la posibilidad de que esos acuerdos incluyan la disponibilidad de datos de determinados sistemas críticos, pero, en vista de los desafíos conceptuales que esto plantea, recomendamos que esta cuestión se estudie durante un proceso ulterior.
5. Si bien no somos los primeros en proponer este tipo de acuerdo, creemos que en esta publicación se plantean el análisis y la propuesta más detallados e integrales que se han presentado hasta el momento. Por ejemplo, Richard Clarke y Robert Knake

propusieron una norma similar en su publicación de 2011; ver Richard A. Clarke y Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (Nueva York: HarperCollins, 2011), 269. Greg Austin y Eric Cappon del EastWest Institute también escribieron un breve artículo sobre este tema e hicieron una analogía con la Convención de 1977 sobre la Prevención y el Castigo de Delitos contra Personas Internacionalmente Protegidas; ver Greg Austin y Eric Cappon, "Internationally Protected Facilities in Cyberspace: The Examples of Stock Exchanges and Clearing Houses", EastWest Institute, diciembre de 2014.

6. Un acuerdo internacional como el propuesto también podría plantear, en teoría, un problema de riesgo moral, pero esto es poco probable dada la importante amenaza que representan los agentes no estatales. Además, ya existe presión por mejorar la resiliencia mediante medidas más rigurosas de diligencia debida y, por lo tanto, un acuerdo internacional que limite el comportamiento del Estado sería oportuno y complementaría las iniciativas en marcha.

7. Asamblea General de las Naciones Unidas, A/70/174, "Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional", 22 de julio de 2015, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.

8. "Comunicado de Líderes del G20, Cumbre de Antalya, 15 y 16 de noviembre de 2015", comunicado de prensa, Consejo Europeo, 16 de noviembre de 2015, http://www.consilium.europa.eu/en/press/press-releases/2015/11/16-g20-summit-antalya-communique/.

9. Joe Uchill, "Israel Cyber Head: US-Backed Cyber Norms Too Broad", *Hill*, 13 de septiembre de 2016, http://thehill.com/policy/cybersecurity/295651-israel-cyber-head-us-supported-cyber-norms-too-broad.

10. John Markoff y Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk", *The New York Times*, 1 de agosto de 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html; Clarke y Knake, *Cyber War*, 202–3.

11. Ministerio de Relaciones Exteriores de Rusia, Convención Internacional sobre Seguridad Informática, 22 de septiembre de 2011, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

12. Mark Fahey y Nick Wells, "Charts: Who Loses When the Renminbi Joins the IMF Basket?", CNBC, 2 de diciembre de 2015, http://www.cnbc.com/2015/12/02/who-loses-when-the-renminbi-joins-the-imf-basket.html.

13. Sandhya Dangwal, "Budget 2017: Computer Emergency Response Team to Be Set Up to Check Cyber Frauds", *India*, 1 de febrero de 2017, http://www.india.com/news/india/budget-2017-computer-emergency-response-team-to-be-set-up-to-check-cyber-frauds-1802854/.

14. Con respecto a la falsificación de moneda en tiempos de guerra, el consejero jurídico del Fondo Monetario Internacional, Francois Gianviti, escribió en un artículo de 2004: "¿Se aplica en épocas de guerra la prohibición de falsificar moneda? Ha habido algunos ejemplos de esas prácticas". Por ejemplo, la Operación Bernhard, en Alemania, tuvo como blanco la economía británica durante la Segunda Guerra Mundial. El Gobierno de EE. UU. habría falsificado moneda vietnamita e iraquí durante los conflictos bélicos que mantuvo con esos países. F. A. Mann, *The Legal Aspect of Money*, 5.a ed. (Oxford: Oxford University Press, 1992); "Nazi Fake Banknote 'Part of Plan to Ruin British Economy", *The Telegraph*, 29 de septiembre de 2010, http://www.telegraph.co.uk/history/world-war-two/8029844/Nazi-fake-banknote-part-of-plan-to-ruin-British-economy.html; Lizzie Suiter, Jennifer Hucke y Courtney Schultz, "The War at Home: A Look at Media Propaganda in WWII, Vietnam, and the War in Iraq" (documento definitivo, programa Stanford EDGE, diciembre de 2004); Youssef M. Ibrahim, "Fake-Money Flood Is Aimed at Crippling Iraq's Economy", *The New York Times*, 27 de mayo de 1992, http://www.nytimes.com/1992/05/27/world/fake-money-flood-is-aimed-at-crippling-iraq-s-economy.html?pagewanted=all.

15. Nicholas A. Lambert, "The Strategy of Economic Warfare: A Historical Case Study and Possible Analogy to Contemporary Cyber Warfare", en *Cyber Analogies*, ed. Emily O. Goldman y John Arquilla (Monterey, CA: Naval Postgraduate School, 2014), http://calhoun.nps.edu/bitstream/handle/10945/40037/NPS-DA-14-001.pdf?sequence=1.

16. Más de ochenta países han firmado y ratificado este convenio. China, la India y Estados Unidos han firmado este instrumento pero no lo han ratificado.

17. Francois Gianviti, "Current Legal Aspects of Monetary Sovereignty", Fondo Monetario Internacional, 24 de mayo de 2004, https://www.imf.org/external/np/leg/sem/2004/cdmfl/eng/gianvi.pdf.

18. El ejemplo más reciente y ampliamente documentado de una transgresión de esta norma es el superdólar, la falsificación realizada por Corea del Norte; Stephen Mihm, "No Ordinary Counterfeit", *The New York Times*, 23 de julio de 2006, http://www.nytimes.com/2006/07/23/magazine/23counterfeit.html.

19. Oona Hathaway y otros, "The Law of Cyber Attack", *California Law Review* 100 (2012): http://digitalcommons.law.yale.edu/fss_papers/3852/.
20. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 56–57.
21. Por ejemplo, en 2016 el Ejército de EE. UU. destruyó un edificio en Mosul donde se guardaban millones de dólares, en una "iniciativa total destinada a menoscabar la situación financiera [de Estado Islámico]". A diferencia de los ejemplos anteriores de falsificación de moneda en tiempos de guerra, este es un ejemplo de destrucción de la moneda física; Charlie Dunlap, "The Loyola Conference and the Evolving Definition of Military Objective", *Lawfire* (blog), Duke University, 14 de febrero de 2016, http://sites.duke.edu/lawfire/2016/02/14/the-loyola-conference-and-the-evolving-definition-of-military-objective/.
22. Se podría alegar que no sería necesario cambiar la doctrina de EE. UU. sobre sostenimiento bélico por un acuerdo del tipo que venimos analizando, si tal doctrina distingue entre la posibilidad permitida de atacar instituciones financieras en su forma física, pero prohíbe atacar la integridad de los datos de las instituciones financieras.
23. James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community", Comité de Servicios Armados del Senado, 9 de febrero de 2016, http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.
24. Clarke y Knake, *Cyber War*, 202–3.
25. Por ejemplo, informando sobre una vulnerabilidad a otros agentes que llevan a cabo acciones maliciosas o haciendo la vista gorda respecto de la actividad de agentes no estatales.
26. Asamblea General de las Naciones Unidas, A/70/174.
27. "Policy Measures to Address Systemically Important Financial Institutions", Consejo de Estabilidad Financiera, 4 de noviembre de 2011, http://www.fsb.org/wp-content/uploads/r_111104bb.pdf?page_moved=1.
28. "Capítulo 11: Servicios financieros", en "Trans-Pacific Partnership", Oficina del Representante de Comercio de Estados Unidos, https://ustr.gov/sites/default/files/TPP-Final-Text-Financial-Services.pdf.
29. Comité de Sistemas de Pago y Liquidación, Comité Técnico de la Organización Internacional de Comisiones de Valores, "Principios aplicables a las infraestructuras del mercado financiero", Banco de Pagos Internacionales y OICV, abril de 2012, https://www.bis.org/cpmi/publ/d101_es.pdf, 176.
30. "FSB Reports Foreign Special Services Preparing Massive Cyber Attacks", TASS, 2 de diciembre de 2016, http://tass.com/politics/916315.
31. Ivana Kottasova, "Russia: Foreign Hackers Are Trying to Take Down Our Banks", CNN, 2 de diciembre de 2016, http://money.cnn.com/2016/12/02/technology/russia-hack-banks-foreign/.
32. Ibíd.
33. Ibíd.
34. "FSB Reports", TASS.
35. Steve Herman, "Historic Bangladesh Bank Heist Muddled in Mystery", *Voice of America*, 24 de marzo de 2016, http://www.voanews.com/content/historic-bangladesh-bank-heist-muddled-in-mystery/3252379.html; Rick Gladstone, "Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million", *The New York Times*, 15 de marzo de 2016, http://www.nytimes.com/2016/03/16/world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html?_r=0.
36. Reuters, "Spelling Mistake Prevented Hackers Taking $1bn in Bank Heist", *The Guardian*, 10 de marzo de 2016, http://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank-heist.
37. Gladstone, "Bangladesh Bank Chief", *The New York Times*.
38. Reuters, "Spelling Mistake", *The Guardian*.
39. Sergei Shevchenko, "Two Bytes To $951m", *Bae Systems Threat Research Blog*, 25 de abril de 2016, http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html.
40. Laurens Cerulus, "Belgian Government Plagued by Hackers", *Politico*, 22 de febrero de 2016, http://www.politico.eu/article/belgium-government-agencies-plagued-hackers-downsec-ddos-attacks-cyber-crime/.
41. Charles Riley, "China Stocks Plunge as Bubble Fears Grow", *The Open* (*blog*), CNN, 19 de junio de 2015, http://money.cnn.com/2015/06/19/investing/china-stocks-shanghai-correction/.
42. "Chinese Stocks Tumble for a Second Day After Global Fall", BBC, 25 de agosto de 2015, http://www.bbc.com/news/

business-34048084; Diane Alter, "What Today's China Stock Market Crash Means for Your Money in 2016", *Money Morning*, 25 de febrero de 2016, http://moneymorning.com/2016/02/25/what-todays-china-stock-market-crash-means-for-your-money-in-2016/.

43. AJ Vicens, "The Shocking Truth About Wednesday's Apocalypse Involving Wall Street, China, ISIS, and United Airlines", *Mother Jones*, 8 de julio de 2015, http://www.motherjones.com/politics/2015/07/nyse-glitch-hack-china-cia-cyber-isis.

44. Eugene Gerden, "Russian Bank Licences Revoked for Using Hackers to Withdraw Funds", *SC Magazine UK*, 17 de febrero de 2016, http://www.scmagazineuk.com/russian-bank-licences-revoked-for-using-hackers-to-withdraw-funds/article/474464/.

45. Graham Cluley, "Corkow—the Lesser-Known Bitcoin-Curious Cousin of the Russian Banking Trojan Family", We Live Security, 11 de febrero de 2014, http://www.welivesecurity.com/2014/02/11/corkow-bitcoin-russian-banking-trojan/; y "How malware moved the exchange rate in Russia", We Live Security, 12 de febrero de 2016, http://www.welivesecurity.com/2016/02/12/malware-moved-exchange-rate-russia/.

46. Jake Rudnitsky e Ilya Khrennikov, "Russian Hackers Moved Ruble Rate With Malware, Group-IB Says", Bloomberg, 8 de febrero de 2016, http://www.bloomberg.com/news/articles/2016-02-08/russian-hackers-moved-currency-rate-with-malware-group-ib-says?mod=djemRiskCompliance.

47. Kate Kochetkova, "Dozens of Banks Lose Millions to Cybercriminals Attacks", *Kaspersky Lab Daily* (*blog*), 8 de febrero de 2016, https://blog.kaspersky.com/metel-gcman-carbanak/11236/.

48. "Cyberberkut Hacked the Site of Ukrainian Ministry of Finance: The Country Has No Money", SouthFront, 25 de mayo de 2015, https://southfront.org/cyberberkut-hacked-the-site-of-ukrainian-ministry-of-finance-the-country-has-no-money/.

49. Cory Bennett, "Hackers Breach the Warsaw Stock Exchange", *Hill*, 24 de octubre de 2014, http://thehill.com/policy/cybersecurity/221806-hackers-breach-the-warsaw-stock-exchange.

50. Michael Riley y Jordan Robertson, "Cyberspace Becomes Second Front in Russia's Clash With NATO", Bloomberg, 14 de octubre de 2015, http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato.

51. Ibíd.

52. "'Cyber Berkut' Hackers Target Major Ukrainian Bank", *The Moscow Times,* 4 de julio de 2014, http://www.themoscowtimes.com/business/article/cyber-berkut-hackers-target-major-ukrainian-bank/502992.html.

53. "Pro-Russian Hackers Mug Key Ukrainian Bank", *ThreatWatch* (*blog*), Nextgov, 4 de julio de 2014, http://www.nextgov.com/cybersecurity/threatwatch/2014/07/stolen-credentials-network-intrusion-data-dump-pro/1225/.

54. Bill Gertz, "Russian Cyber Warfare Suspected in Bank Attacks", *Flash//CRITIC Cyber Threat News*, 30 de agosto de 2014, http://flashcritic.com/russian-cyber-warfare-suspected-bank-attacks-sophisticated-hackers/.

55. David E. Sanger y Nicole Perlroth, "Bank Hackers Steal Millions via Malware", *The New York Times*, 14 de febrero de 2015, http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=0.

56. Kaspersky Lab's Global Research and Analysis Team, "The Great Bank Robbery: The Carbanak APT", *Securelist* (*blog*), Kaspersky Lab, 16 de febrero de 2015, https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/.

57. Choe Hang-Sun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks", *The New York Times*, 20 de marzo de 2013, http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html; Juan C. Zarate, "The Cyber Financial Wars on the Horizon", Foundation for Defense of Democracies, julio de 2015, http://www.defenddemocracy.org/content/uploads/publications/Cyber_Financial_Wars.pdf, 12–13.

58. Hang-Sun, "Computer Networks in South Korea", *The New York Times*; Zarate, "Cyber Financial Wars", Foundation for Defense of Democracies.

59. K.J. Kwon, "Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes", CNN, 22 de abril de 2015, http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/.

60. James O'Toole, "JPMorgan: 76 Million Customers Hacked", CNN, 3 de octubre de 2014, http://money.cnn.com/2014/10/02/

technology/security/jpmorgan-hack/?iid=EL; Jose Pagliery, "JPMorgan's Accused Hackers Had Vast $100 Million Operation", CNN, 10 de noviembre de 2015, http://money.cnn.com/2015/11/10/technology/jpmorgan-hack-charges/.

61. Michael Riley y Jordan Robertson, "FBI Said to Examine Whether Russia Tied to JPMorgan Hacking", Bloomberg, 27 de agosto de 2014, http://www.bloomberg.com/news/articles/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking.
62. Kim Zetter, "Four Indicted in Massive JP Morgan Chase Hack", *Wired*, 10 de noviembre de 2015, http://www.wired.com/2015/11/four-indicted-in-massive-jp-morgan-chase-hack/.
63. Ibíd.
64. Ibíd.; Pagliery, "JPMorgan's Accused Hackers", CNN.
65. Matthew Cowley, "Brazilian Banks' Websites Face Hacker Attacks", *The Wall Street Journal*, 31 de enero de 2012, http://www.wsj.com/articles/SB10001424052970204740904577194930748478316?cb=logged0.12500478560104966.
66. Esteban Israel, "Hackers Target Brazil's World Cup for Cyber Attacks", Reuters, 26 de febrero de 2014, http://www.reuters.com/article/us-worldcup-brazil-hackers-idUSBREA1P1DE20140226.
67. "#OpWorldCup: Anonymous wages cyber attacks against Brazil govt.", *RT*, 12 de junio de 2014, https://www.rt.com/news/165444-anonymous-brazil-world-cup/.
68. Paul Cooper, "Anonymous Lives Up to Threats: FIFA World Cup Hacks Get Underway", IT Pro Portal, 13 de junio de 2014, http://www.itproportal.com/2014/06/13/anonymous-lives-up-to-threats-fifa-world-cup-hacks-get-underway/#ixzz41DPxOwdR.
69. Robert Lemos, "Cyber-Attacks Seen Defrauding Brazilian Payment System of Billions", *eWeek*, 6 de julio de 2014, http://www.eweek.com/security/cyber-attacks-seen-defrauding-brazilian-payment-system-of-billions.html.
70. Eli Marcus, "RSA Uncovers Boleto Fraud Ring in Brazil", RSA, 2 de julio de 2014, https://blogs.rsa.com/rsa-uncovers-boleto-fraud-ring-brazil/.
71. "Boleto Malware May Lose Brazil $3.75bn", BBC, 3 de julio de 2014, http://www.bbc.com/news/technology-28145401.
72. Emilio Iasiello, "Cyber Attack: A Dull Tool to Shape Foreign Policy" (documento presentado en la 5.º Conferencia Internacional sobre Ciberconflicto de 2013), 11, https://ccdcoe.org/cycon/2013/proceedings/d3r1s3_Iasiello.pdf.
73. David Goldman, "Major Banks Hit With Biggest Cyberattacks in History", CNN, 28 de septiembre de 2012, http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/.
74. Barbara Slavin, "US Withholds Evidence for Iran Cyberattacks", *Al-Monitor*, 17 de enero de 2013, http://www.al-monitor.com/pulse/originals/2013/01/cyber-attacks-us-iran-ddos.html.
75. Nicole Perlroth y Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say", *The New York Times*, 8 de enero de 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.
76. Nicole Perlroth y Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say", 8 de enero de 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.
77. Slavin, "US Withholds Evidence", *Al-Monitor*.
78. Mathew J. Schwartz, "Bank Attackers Restart Operation Ababil DDoS Disruptions", *Dark Reading*, 6 de marzo de 2013, http://www.darkreading.com/attacks-and-breaches/bank-attackers-restart-operation-ababil-ddos-disruptions/d/d-id/1108955.
79. Pete Sweeney y John Ruwitch, "June 4 Crackdown Remembered in China Stock Index, or Chance?", Reuters, 4 de junio de 2012, http://www.reuters.com/article/us-china-stocks-tiananmen-idUSBRE8530F720120604.
80. Keith Bradsher, "Market's Echo of Tiananmen Date Sets Off Censors", *The New York Times*, 4 de junio de 2012, http://www.nytimes.com/2012/06/05/world/asia/anniversary-of-tiananmen-crackdown-echos-through-shanghai-market.html.
81. "Kaspersky Lab Discovers 'Gauss' – A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts", comunicado de prensa, Kaspersky Lab, 9 de agosto de 2012, http://usa.kaspersky.com/about-us/press-center/press-releases/2012/kaspersky-lab-discovers-gauss-new-complex-cyber-threat-desi.
82. Dan Goodin, "Puzzle Box: The Quest to Crack the World's Most Mysterious Malware Warhead", *Ars Technica*, 14 de marzo de 2013, http://arstechnica.com/security/2013/03/the-worlds-most-mysterious-potentially-destructive-malware-is-not-stuxnet/.

83. Kim Zetter, "Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload", *Wired*, 9 de agosto de 2012, http://www.wired.com/2012/08/gauss-espionage-tool/all/.

84. "Kaspersky Lab Discovers 'Gauss'", Kaspersky Lab.

85. Dan Goodin, "Puzzle Box", *Ars Technica*; Kim Zetter, "Suite of Sophisticated Nation-State Attack Tools Found With Connection to Stuxnet", *Wired*, 16 de febrero de 2015, http://www.wired.com/2015/02/kapersky-discovers-equation-group/.

86. Zarate, "Cyber Financial Wars", Foundation for Defense of Democracies; Kim Zetter,"Flame and Stuxnet Cousin", *Wired*.

87. Chico Harlan y Ellen Nakashima, "Suspected North Korean Cyber Attack on a Bank Raises Fears for S. Korea, Allies", *The Washington Post*, 29 de agosto de 2011, https://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html; "North Korea 'Behind South Korean Bank Cyber Hack'", BBC, 3 de mayo de 2011, http://www.bbc.com/news/world-asia-pacific-13263888.

88. "Prosecution Says N. Korea Behind Nonghyup's Network Breakdown", Yonhap, 3 de mayo de 2011, http://english.yonhapnews.co.kr/national/2011/05/03/23/0302000000AEN20110503007100315F.HTML?1a7c6120.

89. Michael Riley, "How Russian Hackers Stole the Nasdaq", Bloomberg, 21 de julio de 2014, http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.

90. John Markoff, "Before the Gunfire, Cyberattacks", *The New York Times*, 12 de agosto de 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

91. David J. Smith, "Russian Cyber Capabilities, Policy and Practice", *inFOCUS Quarterly* 5, n.º 1 (Invierno 2014): http://www.jewishpolicycenter.org/4924/russian-cyber-capabilities?utm_content=bufferbb5cd&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer; Markoff, "Before the Gunfire, Cyberattacks", *The New York Times*.

92. Smith, "Russian Cyber Capabilities, Policy and Practice", *inFocus Quarterly*.

93. Markoff, "Before the Gunfire, Cyberattacks", *The New York Times*.

94. Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security", *International Affairs Review* 18, n.º 2 (2009): http://www.iar-gwu.org/node/65.

95. "Cyberwarfare 101: Case Study of a Textbook Attack", Stratfor, 18 de abril de 2008, https://www.stratfor.com/analysis/cyberwarfare-101-case-study-textbook-attack; Jason Richards, "Denial-of-Service", *International Affairs Review*.

96. "Cyberwarfare 101", Stratfor; Richards, "Denial-of-Service", *International Affairs Review*.

97. "Cyberwarfare 101", Stratfor; Richards, "Denial-of-Service", *International Affairs Review*.

98. "Cyberwarfare 101", Stratfor; Joshua Davis, "Hackers Take Down the Most Wired Country in Europe", *Wired*, 21 de agosto de 2007, http://www.wired.com/2007/08/ff-estonia/.

99. "Cyberwarfare 101", Stratfor; Davis, "Hackers Take Down", *Wired*.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

El Fondo Carnegie para la Paz Internacional (Carnegie Endowment for International Peace) es una red mundial única de centros dedicados a la investigación de políticas en Rusia, China, Europa, Oriente Medio, la India y Estados Unidos. Desde hace más de cien años, nuestra misión ha consistido en promover la paz mediante el análisis y el desarrollo de nuevas ideas en materia de políticas y la participación y colaboración directas con quienes toman decisiones en gobiernos, empresas y en la sociedad civil. Nuestros centros, mediante el trabajo en conjunto, aportan una diversidad sumamente valiosa de puntos de vista nacionales sobre temas bilaterales, regionales y globales.