LA CIBERAMENAZA MUNDIAL

El sistema financiero mundial está expuesto a crecientes ciberamenazas, y la comunidad mundial tiene que cooperar para protegerlo

Tim Maurer y Arthur Nelson

En febrero de 2016, piratas informáticos, o *hackers*, atacaron el banco central de Bangladesh, explotaron vulnerabilidades en SWIFT, el principal sistema de correspondencia de pagos electrónicos del sistema financiero mundial, y trataron de robarse USD 1.000 millones. La mayoría de las transacciones fueron bloqueadas, pero aun así desaparecieron USD 101 millones. El atraco alertó al mundo financiero de que los ciberriesgos sistémicos del sistema financiero habían sido gravemente subestimados.

Hoy en día la idea de que un gran ciberataque plantee una amenaza para la estabilidad financiera es una cuestión axiomática; no un *si*, sino un *cuándo*. Pero a los gobiernos y las empresas les sigue costando contener la amenaza porque aún no se sabe con certeza quién es responsable de proteger el sistema. Las principales voces de alarma suenan cada vez más preocupadas. En febrero de 2020, Christine Lagarde, Presidenta del Banco Central Europeo y ex Directora

La idea de que un gran ciberataque plantee una amenaza para la estabilidad financiera es una cuestión axiomática; no un *si*, sino un *cuándo*.

Gerente del Fondo Monetario Internacional, advirtió que un ciberataque podría desencadenar una grave crisis financiera. En abril de 2020, el Consejo de Estabilidad Financiera (CEF) advirtió que "un importante incidente cibernético, si no se contiene de forma adecuada, podría perturbar gravemente los sistemas financieros, incluida la infraestructura financiera crítica, con implicaciones más amplias para la estabilidad financiera". Estos incidentes pueden tener ingentes costos económicos y deteriorar considerablemente la confianza pública.

Dos actuales tendencias exacerban este riesgo. La primera es que el sistema financiero mundial está experimentando una transformación digital sin precedentes, acelerada por la pandemia de COVID-19. Los bancos compiten con las empresas de tecnología, y viceversa. Mientras tanto, la pandemia ha intensificado la demanda de servicios financieros en línea y ha normalizado el teletrabajo. Los bancos centrales en todo el mundo están considerando dar su respaldo a las monedas digitales y modernizar los sistemas de pago. En este momento de transformación, en el que un incidente podría fácilmente socavar la confianza y descarrilar las innovaciones, la ciberseguridad es más esencial que nunca.

La segunda es que los malhechores se han aprovechado de esta transformación digital y ahora constituyen una mayor amenaza para el sistema financiero mundial, la estabilidad financiera y la confianza en la integridad del sistema. La pandemia incluso ha creado nuevas posibles víctimas para los *hackers*. Según el Banco de Pagos Internacionales, el sector financiero registra el segundo mayor porcentaje de ciberataques relacionados con la COVID-19, detrás solo del sector sanitario.

¿Quién está detrás de la amenaza?

Cabe esperar que en el futuro se produzcan ataques más peligrosos, con sus consiguientes shocks. Los más preocupantes son los incidentes que corrompen la integridad de los datos financieros, como registros, algoritmos y transacciones; actualmente no existen muchas soluciones para este tipo de ataques, que pueden socavar la confianza de forma más generalizada. Los malhechores ya no son solo delincuentes cada vez más osados —como el grupo Carbanak, que robó más de USD 1.000 millones a instituciones financieras entre 2013 y 2018— sino también Estados y *hackers* auspiciados por Estados (cuadro). Corea del Norte, por ejemplo, ha robado unos USD 2.000 millones de por lo menos 38 países en los últimos cinco años.

Se trata de un problema mundial. Los ciberataques en los países de alto ingreso suelen acaparar titulares de prensa, pero se presta menos atención al creciente número de ataques a objetivos más blandos en países de ingreso bajo y mediano-bajo. Pero es en estos países donde el avance hacia la inclusión financiera ha sido más pronunciado, y ha llevado a muchos a dar el salto hacia los servicios financieros digitales como los sistemas de pago móvil. Si bien promueven la inclusión financiera, los servicios financieros digitales también ofrecen muchas posibles víctimas a los *hackers*. Por ejemplo, el ataque en octubre de 2020 a las principales redes de dinero móvil en Uganda, MTN y Airtel, sembró el caos en las transacciones de servicios durante cuatro días.

Los ciberataques en detalle

Los actores detrás de estos incidentes no son solo delincuentes cada vez más osados, sino también Estados y grupos auspiciados por Estados, con diversos fines y motivaciones.

ACTORES	MOTIVACIONES	FINES	EJEMPLOS
 **Naciones-Estado, grupos auspiciados por Estados**	Geopolíticas, ideológicas	Perturbación, destrucción, daño, robo, espionaje, provecho financiero	Corrupción permanente de datos, daños físicos focalizados, perturbación del sistema eléctrico, perturbación del sistema de pagos, transferencias fraudulentas, espionaje
 **Ciberdelincuentes**	Enriquecimiento	Robo/provecho financiero	Robo de efectivo, transferencias fraudulentas, robo de credenciales
 **Grupos terroristas, activistas informáticos, amenazas internas**	Ideológicas, descontento	Perturbación	Filtraciones, difamación ataques de denegación de servicios distribuidos

Fuente: Junta Europea de Riesgo Sistémico 2020. "Systemic Cyber Risk". https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

ARTE: ISTOCK / YOUR_PHOTO

Sin medidas específicas, el sistema financiero mundial se irá haciendo más vulnerable conforme la innovación, la competencia y la pandemia sigan impulsando la revolución digital.

Brecha de responsabilidad

Pese a que el sistema financiero mundial depende cada vez más de la infraestructura digital, no está claro quién se encarga de proteger el sistema de los ciberataques, en parte porque el entorno evoluciona muy rápidamente. Sin medidas específicas, el sistema financiero mundial se irá haciendo más vulnerable conforme la innovación, la competencia y la pandemia sigan impulsando la revolución digital. Muchas de las amenazas apuntan a sacar dinero, pero están en aumento los ataques puramente disruptivos y destructivos; además, los que aprenden a robar también se familiarizan con las redes y operaciones del sistema financiero, para lanzar ataques más disruptivos o destructivos en el futuro (o para vender lo aprendido a otros). Esta rápida evolución del panorama de riesgos está poniendo a prueba la capacidad de respuesta de un sistema maduro y bien regulado.

Proteger mejor el sistema financiero mundial es ante todo un reto organizativo. Los esfuerzos para reforzar las defensas y la regulación son importantes, pero no bastan para adelantarse a los crecientes riesgos. A diferencia de muchos sectores, la mayor parte de la comunidad de servicios financieros cuenta con los recursos y la capacidad para implantar soluciones técnicas. El mayor problema es de coordinación: definir la mejor forma de organizar la protección del sistema entre diferentes gobiernos, autoridades financieras y sectores, y de aprovechar estos recursos eficaz y eficientemente.

La actual fragmentación entre las partes interesadas y las iniciativas se debe en parte a los aspectos singulares y el carácter cambiante de los ciberriesgos. Las diferentes comunidades operan aisladamente y abordan la cuestión conforme a sus respectivos mandatos. La comunidad de supervisión financiera se centra en la resiliencia, los diplomáticos en el comportamiento de los Estados, los organismos de seguridad nacional en la disuasión de delitos y los ejecutivos en cuestiones que atañen específicamente a sus empresas y no al sector. A medida que la demarcación entre las empresas de servicios y de tecnología se difumina, lo mismo sucede con las responsabilidades relativas a la seguridad.

La desconexión entre las comunidades financiera, diplomática y de seguridad nacional es especialmente notable. Las autoridades financieras se enfrentan a riesgos específicos de ciberamenazas, pero su interacción con los organismos de seguridad nacional, cuya participación es necesaria para afrontar eficazmente las amenazas, sigue siendo escasa. Esta brecha de responsabilidad y la persistente incertidumbre acerca de las funciones y los mandatos de protección del sistema financiero mundial alimentan los riesgos. Esta incertidumbre obedece en parte al actual clima geopolítico y los altos niveles de desconfianza, que dificultan la cooperación en la comunidad internacional. La cooperación en cuestiones de ciberseguridad se ha visto entorpecida y fragmentada, y a menudo reducida a mínimos círculos de confianza ya que atañe a delicados intereses de seguridad nacional. La cooperación internacional y entre múltiples partes interesadas no es algo conveniente sino indispensable.

Una estrategia internacional

Para proteger más eficazmente el sistema financiero mundial de las ciberamenazas, el Fondo Carnegie para la Paz Internacional publicó en noviembre de 2020 un informe sobre la estrategia internacional para ese fin. Elaborado junto con el Foro Económico Mundial, el informe recomienda medidas concretas para reducir la fragmentación promoviendo la colaboración internacional y entre organismos del gobierno, empresas financieras y tecnológicas.

La estrategia se basa en cuatro principios: el primero es la *aclaración de funciones y responsabilidades*. Solo unas pocas empresas han desarrollado relaciones internas eficaces entre las autoridades financieras, las fuerzas del orden, los diplomáticos, otras entidades pertinentes del gobierno y la industria. La fragmentación actual dificulta la cooperación internacional y debilita la capacidad colectiva de resistencia, recuperación y respuesta del sistema internacional.

El segundo es la *urgente necesidad de colaboración internacional*. Dadas la magnitud de la amenaza y la interdependencia mundial del sistema, los gobiernos y las empresas financieras y tecnológicas no pueden protegerse eficazmente de las ciberamenazas si trabajan aisladamente.

En tercer lugar, hay que *reducir la fragmentación a fin de contar con más capacidad para encarar el problema*. Están en curso muchas iniciativas para proteger mejor las instituciones financieras, pero cada una avanza por su propio camino. Hay duplicación de esfuerzos, y eso incrementa los costos de transacción. Varias de estas iniciativas han llegado al punto en que pueden compartirse, coordinarse mejor e internacionalizarse más.

Y cuarto, *la protección del sistema financiero internacional puede servir de modelo para otros sectores*. El sistema financiero es uno de los pocos aspectos en que los países tienen un claro interés común de cooperación, aun si las tensiones geopolíticas están elevadas. La atención en el sector financiero es un punto de partida y podría sentar las bases para proteger mejor otros sectores en el futuro.

Entre otras medidas para incrementar la resiliencia cibernética, el informe recomienda que el CEF formule un marco básico para la supervisión de la gestión de los riesgos cibernéticos en las instituciones financieras. Para reforzar la seguridad, los gobiernos deberían intercambiar información sobre amenazas y crear equipos de respuesta ante emergencias informáticas (CERT, por sus siglas en inglés) basados en el FinCERT de Israel.

Las autoridades financieras también deben concentrarse en incrementar la resiliencia del sector financiero ante ataques contra los datos y algoritmos, por ejemplo, con bóvedas de datos seguras y cifradas que permitan crear de un día a otro respaldos seguros de los datos de cuentas de clientes. Deben realizarse periódicamente simulacros de ciberataques para detectar deficiencias y formular planes de respuesta.

Para reforzar las normas internacionales se recomienda que los gobiernos aclaren la aplicación del Derecho internacional en el ciberespacio y apuntalen las normas para proteger la integridad del sistema financiero. Los gobiernos de Australia, los Países Bajos y el Reino Unido ya han dado el primer paso al declarar que los ciberataques provenientes del exterior pueden tipificarse como uso ilegal de la fuerza o intervención en los asuntos internos de otro Estado.

La resiliencia cibernética y las normas internacionales reforzadas pueden facilitar una respuesta colectiva mediante la aplicación de la ley o acciones multilaterales concertadas con el sector. Las respuestas pueden ser multas, arrestos e incautaciones de activos.

Los gobiernos pueden apoyar estos esfuerzos estableciendo entidades que ayuden a evaluar las amenazas y coordinar las respuestas. La recopilación de inteligencia debe centrarse en las amenazas contra el sistema financiero, y los gobiernos deben compartir la información con países aliados y afines.

Desarrollar capacidad

La estrategia integral del informe Carnegie depende de que se desarrolle la fuerza laboral de ciberseguridad, se amplíe la capacidad de ciberseguridad del sector financiero y se protejan las mejoras en inclusión financiera derivadas de la transformación digital.

El fuerte desempleo debido a la pandemia presenta una gran oportunidad para formar y contratar gente talentosa a fin de mejorar la fuerza de trabajo de ciberseguridad. Las empresas de servicios financieros deben invertir en iniciativas para desarrollar una cantera de talento mediante programas escolares, universitarios y de pasantías.

Para reforzar la capacidad de ciberseguridad hay que proporcionar asistencia donde se la necesita. El FMI y otros organismos internacionales han recibido de sus miembros muchos pedidos de asistencia sobre ciberseguridad, particularmente tras el incidente de 2016 en Bangladesh. Los gobiernos y bancos centrales del G-20 podrían crear un mecanismo internacional para desarrollar capacidad de ciberseguridad en el sector financiero, con un organismo internacional como el FMI como coordinador. La Organización para la Cooperación y el Desarrollo Económicos y las instituciones financieras internacionales deben incorporar el fortalecimiento de la capacidad de ciberseguridad en los programas de asistencia para el desarrollo y brindar mucha más asistencia a los países que la necesiten.

Por último, para preservar la mayor inclusión financiera hay que reforzar sus vínculos con la ciberseguridad. Esto es especialmente urgente en África, en donde los sectores financieros de muchos países están transformándose profundamente al ampliar la inclusión financiera y adoptar servicios financieros digitales. Se debe crear una red de expertos dedicada específicamente a la ciberseguridad en África.

Es hora de que la comunidad internacional —gobiernos, bancos centrales, supervisores, industria y otros interesados— se una para afrontar este urgente e importante reto. Una estrategia bien trazada, como la descrita, es lo que permite pasar del dicho al hecho. FD

TIM MAURER es Director de la Iniciativa de Política Cibernética e Investigador Principal en el Programa de Tecnología y Asuntos Internacionales del Instituto Carnegie para la Paz Internacional.
ARTHUR NELSON es Analista de Investigación en la Iniciativa de Política Cibernética del Instituto Carnegie para la Paz Internacional.