التهديد السيبراني العالمي

تتزايد التهديدات السيبرانية للنظام المالي، وعلى المجتمع العالمي أن يتعاون لحمايته

تيم مورر وآرثر نيلسون

في فبراير ٢٠١٦، استهدف القراصنة بنك بنغلاديش المركزي واستغلوا مواطن ضعف في نظام سويفت، وهو نظام رسائل الدفع الإلكترونية الرئيسي للنظام المالي العالمي، في محاولة لسرقة مليار دولار. ورغم حظر معظم المعاملات، فقد اختفى مبلغ قدره ١٠١ مليون دولار. وكانت عملية السطو بمثابة جرس إنذار لعالم التمويل بأن المخاطر السيبرانية النظامية في النظام المالي قد تم التهوين من شأنها إلى حد كبير.

والنظر، في الوقت الحالي، إلى أي هجمة سيبرانية كبيرة باعتبارها تشكل تهديدا للاستقرار المالي يعتبر أمرا بديهيا – وليس سؤالا حول ماذا لو، بل متى. ومع ذلك، لا تزال حكومات وشركات العالم تكافح من أجل احتواء التهديد نظرا لاستمرار عدم الوضوح بشأن من تقع عليه مسؤولية حماية النظام. وهناك شخصيات بارزة تدق ناقوس الخطر إعرابا عن قلقها المتزايد. ففي فبراير ٢٠٢٠، حذرت كريستين لاغارد، رئيس البنك المركزي الأوروبي والرئيس السابق لصندوق النقد الدولي، من أن حدوث هجمة سيبرانية

والنظر، في الوقت الحالي، إلى أي هجمة سيبرانية كبيرة باعتبارها تشكل تهديدا للاستقرار المالي يعتبر أمرا بديهيا — وليس سؤالا حول ماذا لو، بل متى.

يمكن أن يؤدي إلى أزمة مالية خطيرة. وفي إبريل ٢٠٢٠، حذر مجلس الاستقرار المالي من أنه «إذا لم يتم احتواء أي حادثة إلكترونية كبيرة بشكل سليم، فقد تحُدث اضطرابات خطيرة في الأنظمة المالية، بما في ذلك البنية التحتية المالية الحيوية، مما يؤدي إلى تداعيات أوسع على الاستقرار المالي». وقد تكون التكاليف الاقتصادية المحتملة لهذه الأحداث هائلة، كما قد يكون الضرر كبيرا على اطمئنان الجمهور وثقته.

وهناك اتجاهان مستمران يؤديان إلى تفاقم هذه المخاطر. أولا، يمر النظام المالي العالمي بتحول رقمي غير مسبوق، ويشهد هذا التحول تسارعا بسبب جائحة كوفيد–١٩. فالبنوك تتنافس مع شركات التكنولوجيا، وشركات التكنولوجيا تتنافس مع البنوك. وفي الوقت نفسه، أدت الجائحة إلى تصاعد الطلب على الخدمات المالية عبر الإنترنت، وجعلت ترتيبات العمل من المنزل هي القاعدة. وتدرس البنوك المركزية في جميع أنحاء العالم دعم العملات الرقمية بقوة وتحديث نظم الدفع. وفي هذه المرحلة من التحول، عندما يمكن لحادثة أن تقوض الثقة بسهولة وتخرج هذه الابتكارات عن مسارها، يصبح الأمن السيبراني أكثر أهمية من أي وقت مضى.

ثانيا، تستفيد الجهات التي تقف وراء هجمات البرمجيات الخبيثة من هذا التحول الرقمي، وتشكل تهديدا متناميا للنظام المالي العالمي والاستقرار المالي والثقة في نزاهة النظام. وقد وفرت الجائحة أهدافا جديدة للقراصنة. فوفقا لبنك التسويات الدولية، يشهد القطاع المالي ثاني أكبر سلسلة من الهجمات السيبرانية المرتبطة بجائحة كوفيد–١٩، بعد القطاع الصحي.

من وراء التهديد؟

ينبغي توقع المزيد من الهجمات الخطيرة والصدمات اللاحقة لها في المستقبل. ويتمثل مصدر القلق الأكبر في الحوادث التي تفسد سلامة البيانات المالية، مثل السجلات والخوارزميات والمعاملات. وفي الوقت الحالي يتوافر عدد قليل من الحلول التقنية لهذه الهجمات القادرة على زعزعة الاطمئنان والثقة على نطاق أوسع. والجهات التي تقف وراء هجمات البرمجيات الخبيثة لا تشمل فقط مجرمين يزدادون جرأة — مثل مجموعة كارباناك التي استهدفت مؤسسات مالية لسرقة أكثر من مليار دولار خلال الفترة ٢٠١٣–٢٠١٨ — بل تشمل أيضا دولا ومهاجمين ترعاهم دول. فعلى سبيل المثال، سرقت كوريا الشمالية حوالي ملياري دولار من ٣٨ بلدا على الأقل في السنوات الخمس الماضية.

وهذه مشكلة عالمية. وبينما نجد أن الهجمات السيبرانية في البلدان ذات الدخل المرتفع تحتل غالبا العناوين الرئيسية في وسائل الإعلام، يتم توجيه اهتمام أقل للعدد المتزايد من الهجمات على أهداف أضعف في البلدان ذات الدخل المنخفض وتلك التي في الشريحة الأدنى من فئة الدخل المتوسط. غير أن الدافع نحو مزيد من الشمول المالي كان أكثر وضوحا في تلك البلدان، مما دفع الكثير منها إلى التقدم بخطى سريعة نحو الخدمات المالية الرقمية، مثل نظم الدفع عبر الأجهزة المحمولة. ورغم أن الخدمات المالية الرقمية حققت تقدما في إرساء الشمول المالي، فإنها أيضا توفر للقراصنة بيئة غنية بالأهداف. فعلى سبيل المثال، أدت عملية القرصنة التي تعرضت لها أكبر شبكتين للأموال المحمولة في أوغندا، إم تي إن وإيرتل، في أكتوبر ٢٠٢٠، إلى تعطيل كبير في معاملات الخدمات لمدة أربعة أيام.

فجوة المسؤولية

رغم اعتماد النظام المالي العالمي بشكل متزايد على البنية التحتية الرقمية، فلا يزال من غير الواضح من هو المسؤول

نظرة أقرب على الهجمات السيبرانية

الجهات التي تقف وراء هذه الحوادث لا تشمل فقط مجرمين يزدادون جرأة، بل تشمل أيضا دولا ومجموعات ترعاها دول، تختلف أهداف ودوافع كل منها.

الجهة التي تقف وراء التهديد	الدوافع	الأهداف	الأمثلة
دول قومية، مجموعات ترعاها دول	جغرافية–سياسية، أيديولوجية	الاضطراب، التدمير، الضرر، السرقة، التجسس، الكسب المالي	تلف البيانات الدائم، الضرر المادي المستهدف، تعطيل شبكة الكهرباء، تعطيل نظام الدفع، التحويلات الاحتيالية، التجسس
مرتكبو الجرائم الإلكترونية	الإثراء	السرقة، الكسب المالي	سرقة الأموال النقدية، التحويلات الاحتيالية، سرقة بيانات الاعتماد
الجماعات الإرهابية، القراصنة، التهديدات الداخلية	أيديولوجية، الاستياء	الاضطراب	التسريبات، التشهير، الهجمات الموزعة لتعطيل تقديم الخدمة

المصدر: المجلس الأوروبي للمخاطر النظامية. «المخاطر السيبرانية النظامية». https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

الرسم التوضيحي: ISTOCK/YOUR_PHOTO

وبدون اتخاذ إجراء موجه، سيصبح النظام المالي العالمي أكثر عرضة للخطر، حيث يؤدي الابتكار والمنافسة والجائحة إلى تأجيج الثورة الرقمية.

عن حماية النظام من الهجمات السيبرانية. ومن أسباب ذلك أن البيئة تتغير بسرعة كبيرة. وبدون اتخاذ إجراء موجه، سيصبح النظام المالي العالمي أكثر عرضة للخطر، حيث يؤدي الابتكار والمنافسة والجائحة إلى تأجيج الثورة الرقمية. ورغم تركيز العديد من الجهات التي تقف وراء التهديدات على جني الأموال، فإن عدد الهجمات التي لا تستهدف سوى إحداث الاضطراب والتدمير آخذ في الازدياد. وإلى جانب ذلك، فإن أولئك الذين يتعلمون كيفية السرقة يكتسبون أيضا معلومات عن شبكات النظام المالي وعملياته، مما يتيح لهم شن مزيد من الهجمات التي تهدف إلى إحداث الاضطراب والتدمير في المستقبل (أو بيع هذه المعلومات والقدرات لآخرين). وهذا التطور السريع في طبيعة المخاطر يشكل عبئا ثقيلا على استجابة النظام الذي لولا ذلك لكان مكتمل النمو وجيد التنظيم.

ويعد توفير حماية أفضل للنظام المالي العالمي تحديا تنظيميا في المقام الأول. فالجهود المبذولة لتقوية الدفاعات وتشديد اللوائح مهمة، ولكنها ليست كافية لتجاوز المخاطر المتزايدة. وعلى خلاف العديد من القطاعات، نجد أن معظم مجتمع الخدمات المالية لا تنقصه الموارد أو القدرة على تنفيذ الحلول التقنية. فالقضية الرئيسية هي مشكلة العمل الجماعي: أي كيفية تنظيم عملية حماية النظام بين الحكومات والسلطات المالية والصناعة على أفضل وجه، وكيفية الاستفادة من هذه الموارد بفعالية وكفاءة.

وتعد الجوانب المتفردة للمخاطر السيبرانية وطبيعتها المتطورة من أسباب التفتت الحالي بين الأطراف المعنية والمبادرات. فالمجتمعات المختلفة تعمل في صوامع منفصلة وتعالج القضية من خلال تكليفات كل منها. فمجتمع الرقابة المالية يركز على الصمود، ومجتمع الدبلوماسيين على معايير سلوك الدولة، وهيئات الأمن القومي على محاولة ردع الأنشطة الخبيثة، والمديرون التنفيذيون في الصناعة على مخاطر الشركة بدلا من مخاطر القطاع. ونظرا لأن الخطوط الفاصلة بين شركات الخدمات المالية وشركات التكنولوجيا قد أصبحت غير واضحة، يتزايد بالمثل عدم وضوح خطوط المسؤولية عن الأمن.

وهناك انفصال واضح بشكل خاص بين مجتمع التمويل ومجتمع الأمن القومي والمجتمع الدبلوماسي. فرغم أن السلطات المالية تواجه مخاطر متفردة من التهديدات السيبرانية، فإن علاقاتها لا تزال هشة مع هيئات الأمن القومي التي تُعتبر مشاركتها ضرورية للتصدي الفعال لتلك التهديدات. وتتفاقم المخاطر بسبب فجوة المسؤولية هذه واستمرار حالة عدم اليقين بشأن الأدوار والتكليفات المطلوبة لحماية النظام المالي العالمي. ومن أسباب حالة عدم اليقين هذه المناخ الجغرافي–السياسي الحالي وارتفاع مستويات عدم الثقة، اللذان يعوقان التعاون داخل المجتمع الدولي. وقد واجهت جهود التعاون في مجال الأمن السيبراني إعاقة وتشتتا، واقتصرت غالبا على أصغر دوائر الثقة لأنها تمس المصالح الحساسة للأمن القومي. والتعاون بين الدول أو التعاون متعدد الأطراف ليس أمرا «محبذا» ولكنه «ضروري».

استراتيجية دولية

لتحقيق حماية أكثر فعالية للنظام المالي العالمي إزاء التهديدات السيبرانية، أصدرت مؤسسة كارنيغي للسلام الدولي تقريرا في نوفمبر ٢٠٢٠ بعنوان «استراتيجية دولية لزيادة حماية النظام المالي العالمي من التهديدات السيبرانية» (International Strategy to Better Protect the Global Financial System against Cyber Threats). ويوصي التقرير، الذي تم تنقيحه بالتعاون مع المنتدى الاقتصادي العالمي، باتخاذ إجراءات محددة للحد من التشتت من خلال التشجيع على مزيد من التعاون على المستوى الدولي وبين الهيئات الحكومية والشركات المالية وشركات التكنولوجيا.

وتستند الاستراتيجية إلى أربعة مبادئ: أولا، يجب زيادة وضوح الأدوار والمسؤوليات. فلم يقم سوى عدد قليل من البلدان ببناء علاقات محلية فعالة بين سلطاتها المالية، وهيئات إنفاذ القانون، والدبلوماسيين، والجهات الحكومية المعنية الأخرى، والصناعة. والتشتت الحالي يعوق التعاون الدولي ويُضعف قدرات النظام الدولي الجماعية على الصمود والتعافي والاستجابة.

ثانيا، التعاون الدولي ضروري وعاجل. فنظرا لحجم التهديد وطبيعة النظام المترابطة عالمية، لا تستطيع فرادى الحكومات والشركات المالية وشركات التكنولوجيا أن توفر حماية فعالة من التهديدات السيبرانية إذا كانت تعمل بمفردها.

ثالثا، سيؤدي الحد من التشتت إلى تحرير القدرة على التصدي للمشكلة. فهناك عدة مبادرات جارية لتحسين حماية المؤسسات المالية، لكنها لا تزال معزولة. وهناك ازدواجية في بعض هذه الجهود، مما يزيد من تكاليف المعاملات. وقد بلغ العديد من هذه المبادرات من التطور ما يكفي لتعميمها، وتحسين التنسيق بينها، وزيادة تدويلها.

رابعا، يمكن أن تكون حماية النظام المالي الدولي نموذجا للقطاعات الأخرى. فالنظام المالي أحد المجالات القليلة التي يكون للبلدان فيها مصلحة مشتركة واضحة في التعاون، حتى عندما تكون التوترات الجغرافية–السياسية كبيرة. ويعد التركيز على القطاع المالي بمثابة نقطة انطلاق وقد يمهد الطريق نحو توفير حماية أفضل للقطاعات الأخرى في المستقبل.

ومن إجراءات تعزيز الصمود في مواجهة الهجمات السيبرانية، يوصي التقرير بأن يقوم مجلس الاستقرار المالي بوضع إطار أساسي للرقابة على إدارة المخاطر السيبرانية في المؤسسات المالية. وينبغي للحكومات والصناعة تعزيز الأمن من خلال تبادل المعلومات حول التهديدات وإنشاء فرق الاستجابة للطوارئ الحاسوبية المالية (CERTs)، على غرار فريق الاستجابة للطوارئ الحاسوبية المالية (FinCERT) في إسرائيل.

وينبغي للسلطات المالية أيضا إعطاء أولوية لزيادة صمود القطاع المالي في مواجهة الهجمات التي تستهدف البيانات والخوارزميات. وينبغي أن يشمل ذلك التخزين الآمن والمشفر للبيانات بما يتيح للأعضاء إجراء نسخ احتياطي آمن لبيانات حسابات العملاء بين عشية وضحاها. وينبغي استخدام التمارين المنتظمة لمحاكاة الهجمات السيبرانية في تحديد مواطن الضعف ووضع خطط العمل.

ولتعزيز المعايير الدولية، يوصي التقرير الحكومات بإيضاح كيفية تطبيق القانون الدولي على الفضاء الإلكتروني وتعزيز معايير حماية نزاهة النظام المالي. وقد اتخذت حكومات أستراليا وهولندا والمملكة المتحدة بالفعل خطوة أولى بإصدار بيانات تشير إلى أن الهجمات السيبرانية من الخارج يمكن اعتبارها استخداما غير مشروع للقوة أو تدخلا في الشؤون الداخلية لدولة أخرى.

ويمكن أن يؤدي الصمود في مواجهة الهجمات السيبرانية والمعايير الدولية المعززة إلى تيسير الاستجابة الجماعية من خلال إجراءات إنفاذ القانون أو رد الفعل متعدد الأطراف مع الصناعة. ويمكن لهذه الاستجابة أن تشمل عقوبات واعتقالات ومصادرة أصول.

ويمكن للحكومات دعم هذه الجهود من خلال إنشاء كيانات تساعد في تقييم التهديدات وتنسيق الاستجابات. وينبغي أن يتضمن جمع المعلومات الاستخباراتية التركيز على التهديدات التي يتعرض لها النظام المالي، كما ينبغي للحكومات تبادل هذه المعلومات الاستخباراتية مع الحلفاء والبلدان ذات الفكر المماثل.

بناء القدرات

تعتمد الاستراتيجية الشاملة التي وردت في تقرير مؤسسة كارنيغي بدورها على بناء القوى العاملة في مجال الأمن السيبراني، وتوسيع قدرات الأمن السيبراني في القطاع المالي، وحماية مكاسب الشمول المالي التي تحققت نتيجة التحول الرقمي.

ويتيح ارتفاع معدل البطالة بسبب الجائحة فرصة مهمة لتدريب الموهوبين وتوظيفهم لتعزيز القوى العاملة في مجال الأمن السيبراني. وينبغي أن تستثمر شركات الخدمات المالية في مبادرات بناء خط الإمداد بالمواهب، بما في ذلك برامج المدارس الثانوية والتلمذة المهنية والجامعات.

ويُقصد ببناء قدرات الأمن السيبراني التركيز على تقديم المساعدة عند الحاجة. وقد تلقى صندوق النقد الدولي والمنظمات الدولية الأخرى من البلدان الأعضاء العديد من طلبات المساعدة في مجال الأمن السيبراني، لا سيما بعد حادثة بنغلاديش في عام ٢٠١٦. ويمكن للحكومات والبنوك المركزية في مجموعة العشرين إنشاء آلية دولية لبناء قدرات الأمن السيبراني في القطاع المالي، مع تحديد وكالة دولية مثل صندوق النقد الدولي لتنسيق الجهود. وينبغي لمنظمة التعاون والتنمية في المجال الاقتصادي والمؤسسات المالية الدولية جعل بناء القدرات في مجال الأمن السيبراني عنصرا من عناصر حزَم المساعدات الإنمائية، كما ينبغي لها أن تزيد على نحو كبير من مساعداتها للبلدان المحتاجة.

وأخيرا، يتطلب الحفاظ على التقدم المحرز في مجال الشمول المالي تعزيز الروابط بين الشمول المالي والأمن السيبراني. والحاجة لذلك ماسة على وجه الخصوص في إفريقيا، حيث يشهد العديد من البلدان في القارة تحولا كبيرا في قطاعاتها المالية، مع قيامها بتوسيع نطاق الشمول المالي والتحول إلى الخدمات المالية الرقمية. وينبغي إنشاء شبكة من الخبراء للتركيز تحديدا على الأمن السيبراني في إفريقيا.

لقد حان الوقت لتعاون المجتمع الدولي — بما في ذلك الحكومات والبنوك المركزية والجهات الرقابية والصناعة والأطراف المعنية الأخرى ذات الصلة — لمواجهة هذا التحدي العاجل والمهم. وتعد الاستراتيجية الموضوعة بعناية، كالمذكورة أعلاه، بمثابة خطة لتحويل الأقوال إلى أفعال. FD

تيم مورر هو مدير مبادرة السياسة الإلكترونية وزميل أول في برنامج التكنولوجيا والشؤون الدولية التابع لمعهد كارنيغي للسلام الدولي.

آرثر نيلسون هو محلل أبحاث في مبادرة السياسة الإلكترونية التي أطلقها معهد كارنيغي.