ارتفاع مخاطر الاستقرار المالي مع تغذية الذكاء الاصطناعي للهجمات السيبرانية[1]

Tobias Adrian

Financial Counsellor and Director of the IMF's Monetary

Tamas Gaidosch

Senior Cyber Security Expert of the IMF's Monetary

Rangachary Ravikumar

Senior Financial Sector Expert with the IMF's Monetary

إن الصمود والرقابة والتنسيق الدولي أمور أساسية لحماية الأسواق المالية العالمية بينما تمكّن أدوات الذكاء الاصطناعي الجديدة المهاجمين

يُغير الذكاء الاصطناعي الطريقة التي يتعامل بها النظام المالي مع نقاط الضعف ويتفاعل مع الحوادث. ومع ذلك، فهو يُضخم أيضًا التهديدات السيبرانية التي يمكن أن تُقوض الاستقرار المالي عندما تفوق القدرات الهجومية للمتسللين قدرات الدفاع. يُشير تحليل صندوق النقد الدولي إلى أن الخسائر الناجمة عن الحوادث السيبرانية الـــــــــــــشديدة قد تؤدي إلى ضغوط تمويلية، وتُثير مخاوف بشأن الملاءة المالية، وتُعطل الأسواق الأوسع.

يعتمد النظام المالي على بنية تحتية رقمية مشتركة شديدة الترابط، بما في ذلك البرامج وخدمات الحوسبة السحابية والشبكات الخاصة بالمدفوعات والبيانات الأخرى. يمكن لنماذج الذكاء الاصطناعي المتقدمة أن تُقلل بشكل كبير من الوقت والتكلفة اللازمين لتحديد نقاط الضعف واستغلالها، مما يزيد من احتمالية اكتشاف واستهداف نقاط الضعف في الأنظمة واسعة الانتشار في آن واحد. ونتيجة لذلك، يرتبط الخطر السيبراني بشكل متزايد بحالات الفشل المترابطة التي قد تُعطل الوساطة المالية والمدفوعات والثقة على المستوى النظامي.

سلط الإصدار الخاضع للرقابة الأخير من شركة Anthropic لنموذجها "Claude Mythos Preview" – وهو نموذج متقدم للذكاء الاصطناعي بقدرات استثنائية في المجال السيبراني – الضوء

[1] Tobias Adrian, Tamas Gaidosch, Rangachary Ravikumar, Financial Stability Risks Mount as Artificial Intelligence Fuels Cyberattacks, May 7, 2026, IMF, Link.

على مدى السرعة التي تتزايد بها المخاطر. فقد أظهر النموذج قدرة على اكتشاف واستغلال نقاط الضعف في كل نظام تشغيل ومتصفح ويب رئيسي، حتى عند استخدامه من قبل غير الخبراء. وهذا يُنذر بالكيفية التي قد تؤدي بها المخاطر السيبرانية السريعة الحركة والمدفوعة بالذكاء الاصطناعي إلى زعزعة النظام المالي إذا لم تتم إدارتها بعناية، ويُبين سبب ضرورة تركيز السلطات على بناء الصمود من خلال الرقابة والتنسيق، بدلاً من التعامل مع هذه التطورات باعتبارها مجرد قضايا تقنية أو تشغيلية.

من ناحية أخرى، يفترض الإصدار المتخصص والمقيد من GPT-5.5 من شركة OpenAI، والمخصص للمجال السيبراني، أن نقاط الضعف والهجمات سوف تزداد، ويؤكد على تجهيز المدافعين بشكل أسرع وعلى نطاق أوسع، في ظل أنظمة حوكمة مناسبة ونماذج وصول موثوقة.

التطورات تُغير معادلة المخاطر

توضح نماذج مثل Mythos طبيعة التحدي لأنها تُضخم تقنيات الهجمات السيبرانية الحالية من خلال العمل بسرعة آلية. يتمتع المهاجمون بميزة على المدافعين لأن اكتشاف نقاط الضعف واستغلالها يمكن أن يحدث بشكل أسرع من تصحيحها ومعالجتها. في نظام مالي مبني على برامج مشتركة ومقدمي خدمات موحدين، يمكن أن يؤدي ذلك إلى خلق نقاط ضعف متزامنة عبر العديد من المؤسسات.

في الوقت الحالي، لا تزال بعض العوامل التخفيفية قائمة. فالقدرات السيبرانية المتقدمة للذكاء الاصطناعي ليست متاحة على نطاق واسع بعد، كما أن البرامج المالية المغلقة والمخصصة للصناعة يصعب استهدافها مقارنة بالبنية التحتية مفتوحة المصدر. ولكن من المرجح أن تتآكل هذه الحواجز بسرعة مع توسع تدريب النماذج، وانتشار القدرات، وحدوث التسريبات. ومن غير المرجح أن يحل الاحتواء المؤقت محل الدفاعات المستدامة.

آثار الاستقرار المالي

تُركز أدوات الذكاء الاصطناعي الجديدة المُمكّنة سيبرانيًا النقاش حول الاستقرار المالي على النقاط التالية:

- **المخاطر نظامية**: تصبح الهجمات أكثر خطورة عندما يتسع نطاق الاكتشاف والاستغلال بسرعة، مما يُلحق الضرر بالاستقرار المالي.

- **تتجاوز المخاطر القطاعات**: يتقاسم القطاع المالي أسسه الرقمية مع قطاعات الطاقة والاتصالات والخدمات العامة. وهذا يعني أن الهجمات المدعومة بالذكاء الاصطناعي يمكن أن تنتشر عبر القطاعات التي تعتمد على البنية التحتية نفسها.
- **قد يُركز الذكاء الاصطناعي المخاطر والإخفاقات**: حيث يمكن لثغرة أمنية واحدة أن تؤثر على العديد من المؤسسات. فالاعتماد على عدد صغير من منصات البرامج أو مقدمي الخدمات السحابية أو نماذج الذكاء الاصطناعي يزيد من تأثير أي ضعف يتم استغلاله.

ترفع هذه السمات المخاطر السيبرانية إلى مرتبة الصدمات المالية الكلية المحتملة. فقد تتبعها تأثيرات على الثقة، واضطرابات في المدفوعات، وضغوط على السيولة، وديناميكيات البيع بأسعار بخسة إذا تأثرت مؤسسات متعددة في وقت واحد. بالنسبة للسلطات المالية، يتمثل السؤال في ما إذا كان النظام مستعداً لاستيعاب الحوادث السيبرانية دون زعزعة الوظائف المالية الأساسية.

الذكاء الاصطناعي في الدفاع السيبراني

يمثل الذكاء الاصطناعي أيضًا جزءًا حاسمًا من الحل. فعندما يعمل المهاجمون بسرعة آلية، يجب على المدافعين أن يفعلوا الشيء نفسه. تستخدم المؤسسات المالية بشكل متزايد أدوات مدعومة بالذكاء الاصطناعي للكشف عن التهديدات، ومنع الاحتيال، وتحديد نقاط الضعف، والاستجابة للحوادث. يمكن للذكاء الاصطناعي أيضًا المساعدة في تقليل نقاط الضعف في مرحلة التطوير بدلاً من معالجتها بعد الإصدار. بالنسبة للبنية التحتية المالية واسعة الاستخدام، يمكن لهذه المكاسب أن تُقلل بشكل كبير من التعرض النظامي.

لكن هذه الفوائد لن تتحقق إلا إذا استثمرت المؤسسات في التكامل والحوكمة والإشراف البشري، وهي المجالات التي يحتاج المشرفون بشكل متزايد إلى تقييمها. ويشمل ذلك أيضًا استمرارية الأعمال والتعافي من الكوارث، وبرامج الأمن السيبراني وضمان الجودة، وممارسات النظافة السيبرانية الجيدة.

إطار سياسات قائم على الصمود

تتطلب المخاطر السيبرانية المدفوعة بالذكاء الاصطناعي استجابة سياسية تتعامل مع الأمن السيبراني باعتباره قضية محورية تتعلق بالاستقرار المالي. تظل التدابير القائمة ذات صلة، ولكن يجب توسيعها وشحذها لعالم يتسم بهجمات أسرع وآلية ومتطورة بشكل متزايد.

ينبغي على صانعي السياسات إعطاء الأولوية لوضع معايير صمود قوية، ورقابة تركز على قنوات الانتقال النظامية، وتعاون وثيق بين القطاعين العام والخاص بشأن المعلومات الاستخباراتية عن التهديدات والاستجابة للحوادث. لا مفر من اختراق الدفاعات، لذا يجب أن يكون الصمود أولوية أيضاً، وتحديداً للحد من مدى انتشار الحوادث وضمان التعافي السريع. يمكن للضوابط التي تهدف إلى وقف انتشار الهجمات أن تمنع تصاعد الاختراقات المحلية إلى اضطرابات على نطاق النظام بأكمله. غالباً ما تكون هذه التدابير مكلفة ومعقدة، لكنها من بين أكثر الأدوات فعالية لاحتوائها.

من منظور إشرافي، يؤكد هذا على ضرورة التركيز ليس فقط على الوقاية، بل أيضاً على الاستجابة والتعافي واستمرارية الوظائف الحيوية. أصبح اختبار التحمل السيبراني، وتحليل السيناريوهات، والإشراف على مستوى مجالس الإدارة للمخاطر السيبرانية عناصر لا غنى عنها في أطر الاستقرار المالي.

التعاون الدولي أمر حيوي

تُسلط حادثة Mythos الضوء أيضاً على تحديات الحوكمة. فالمخاطر السيبرانية لا تعترف بالحدود. مع انتشار قدرات الذكاء الاصطناعي عبر البلدان، قد تؤدي الرقابة غير المتسقة إلى إضعاف نظام عالمي شديد الترابط. قد تكون الاقتصادات الناشئة والنامية، التي تعاني غالباً من قيود موارد أكثر حدة، معرضة بشكل غير متناسب لاستهداف المهاجمين للمناطق ذات الدفاعات الأضعف.

لهذا السبب، فإن تعزيز التنسيق الدولي، وزيادة تبادل المعلومات، وتوسيع نطاق تطوير القدرات أمور بالغة الأهمية للحفاظ على الاستقرار المالي العالمي. بينما يعيد الذكاء الاصطناعي تشكيل المشهد السيبراني، يتمثل السؤال المحوري للسلطات في ما إذا كان النظام المالي قادراً على الاستمرار في العمل في ظل ضغوط شديدة. والإجابة على هذا السؤال تتطلب وضع المخاطر النظامية – والأدوات اللازمة لإدارتها – في قلب الحوار بين الذكاء الاصطناعي والأمن السيبراني.