LA CYBERMENACE MONDIALE

Des cybermenaces grandissantes pèsent sur le système financier et la communauté mondiale doit coopérer pour le protéger

Tim Maurer et Arthur Nelson

En février 2016, des pirates informatiques ont attaqué la banque centrale du Bangladesh et exploité les vulnérabilités de SWIFT, le principal système de messagerie pour les paiements électroniques du système financier mondial, pour tenter de dérober 1 milliard de dollars. Bien que la majorité des transactions aient été bloquées, 101 millions de dollars ont tout de même disparu. Cet incident a été un électrochoc pour le monde financier, car il a rappelé que les cyberrisques dans le système financier ont été gravement sous-estimés.

Aujourd'hui, l'idée qu'une cyberattaque majeure menace la stabilité financière est une évidence — le risque est certain, la seule inconnue concerne le moment

L'idée qu'une cyberattaque majeure menace la stabilité financière est une évidence — le risque est certain, la seule inconnue concerne le moment auquel il se réalisera.

auquel il se réalisera. Pourtant, les États comme les entreprises ont toujours des difficultés à maîtriser la menace parce qu'on ne sait pas très bien qui est responsable de la protection du système. De plus en plus préoccupés, des acteurs majeurs sonnent l'alarme. En février 2020, Christine Lagarde, présidente de la Banque centrale européenne et ancienne directrice générale du Fonds monétaire international, a mis en garde contre le risque de grave crise financière déclenchée par une cyberattaque. En avril 2020, le Conseil de stabilité financière (CSF) a averti qu'« un cyberincident majeur, s'il n'est pas correctement maîtrisé, pourrait gravement perturber les systèmes financiers, y compris des infrastructures financières critiques, ce qui aurait des implications plus larges pour la stabilité financière ». Les coûts économiques potentiels d'événements de ce genre peuvent être immenses et l'atteinte à la confiance du public considérable.

Deux tendances accentuent ce risque. Premièrement, une transformation numérique sans précédent est à l'œuvre au sein du système financier mondial, transformation qui est accélérée par la pandémie de COVID-19. Les banques font concurrence aux sociétés de technologie, et les sociétés de technologie font concurrence aux banques. Pendant ce temps, la pandémie a accru la demande de services financiers en ligne et fait du télétravail la norme. Les banques centrales du monde entier envisagent de se lancer dans les monnaies numériques et de moderniser les systèmes de paiement. Dans cette période de transformation, où un incident pourrait aisément saper la confiance et faire dérailler ces innovations, la cybersécurité est plus indispensable que jamais.

Deuxièmement, des acteurs malveillants profitent de cette transformation numérique et font peser une menace grandissante sur le système financier mondial, la stabilité financière et la confiance dans l'intégrité du système. La pandémie a même fourni de nouvelles cibles aux pirates informatiques. Selon la Banque des règlements internationaux, le secteur financier est la deuxième victime des cyberattaques liées à la COVID-19, devancé seulement par le secteur de la santé.

Qui se cache derrière cette menace ?

Un plus grand nombre d'attaques dangereuses et de chocs consécutifs est à prévoir. Les incidents les plus préoccupants sont ceux qui corrompent l'intégrité des données financières comme les registres, les algorithmes et les transactions ; il existe peu de solutions techniques aujourd'hui pour de telles attaques, qui peuvent porter plus largement atteinte à la confiance. Les acteurs malveillants à l'origine de ces attaques sont non seulement des criminels de plus en plus audacieux — comme le gang des Carbanak, qui a dérobé plus d'un milliard de dollars à des établissements financiers entre 2013 et 2018 —, mais aussi des États et des attaquants parrainés par des États (voir le tableau). La Corée du Nord, par exemple, a volé quelque 2 milliards de dollars à au moins 38 pays au cours des cinq dernières années.

Il s'agit d'un problème mondial. Alors que les cyberattaques dans les pays à revenu élevé font souvent la une des journaux, on porte moins d'attention au nombre croissant d'attaques visant des cibles plus fragiles dans les pays à faible revenu et les pays à revenu intermédiaire de la tranche inférieure. Ce sont pourtant ces pays qui ont fait le plus d'efforts pour accroître l'inclusion financière, ce qui a conduit de nombreux individus à adopter directement les services financiers numériques comme les systèmes de paiement mobile sans passer au préalable par les services traditionnels. S'ils favorisent effectivement l'inclusion financière, les services financiers numériques offrent aussi de

Les cyberattaques à la loupe

Les acteurs à l'origine de ces incidents sont non seulement des criminels de plus en plus audacieux, mais aussi des États et des groupes parrainés par des États, dont les objectifs et les motivations sont divers.

AUTEUR DE LA MENACE	MOTIVATIONS	OBJECTIFS	EXEMPLES
 **États nations, groupes parrainés par des États**	Géopolitique, idéologie	Perturbations, destruction, dommages, vol, espionnage, gains financiers	Corruption permanente des données, dommages physiques ciblés, perturbation des réseaux d'électricité, perturbation des systèmes de paiement, transferts frauduleux, espionnage
 **Cybercriminels**	Enrichissement	Vol, gains financiers	Vol d'espèces, transferts frauduleux, vol de certificats
 **Groupes terroristes, hacktivistes, menaces internes**	Idéologie, mécontentement	Perturbations	Fuites, diffamation, attaques par déni de service distribué

Source : Comité européen du risque systémique, « Systemic Cyber Risk » (Rapport sur le cyberrisque systémique), 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

ILLUSTRATION : ISTOCK/YOUR_PHOTO

En l'absence de mesures spécifiques, la révolution numérique nourrie par l'innovation, la concurrence et la pandémie ne pourra qu'accroître la vulnérabilité du système financier mondial.

multiples cibles pour les pirates informatiques. Le piratage, en octobre 2020, des plus grands réseaux d'argent mobile en Ouganda, MTN et Airtel, par exemple, a gravement perturbé les services pendant quatre jours.

Le vide de responsabilité

Alors que le système financier mondial dépend de plus en plus de l'infrastructure numérique, on ne sait pas bien qui est responsable de sa protection contre les cyberattaques. Cette situation tient en partie à l'évolution extrêmement rapide de l'environnement. En l'absence de mesures spécifiques, la révolution numérique nourrie par l'innovation, la concurrence et la pandémie ne pourra qu'accroître la vulnérabilité du système financier mondial. Bien que de nombreux auteurs des menaces cherchent avant tout à s'enrichir, on observe une augmentation du nombre d'attaques visant uniquement à perturber et détruire. De plus, ceux qui apprennent comment dérober s'informent aussi sur les réseaux et les opérations du système financier, ce qui leur permettra de lancer des attaques plus perturbatrices et destructrices à l'avenir (ou de vendre ces connaissances et ces capacités à d'autres). Cette rapide évolution du paysage des risques met à l'épreuve la réactivité d'un système par ailleurs mature et bien régulé.

L'amélioration de la protection du système financier mondial est avant tout un défi organisationnel. Les efforts tendant à consolider les défenses et à renforcer la réglementation sont essentiels mais pas suffisants pour prendre de vitesse les risques croissants. Contrairement à de nombreux secteurs, la majeure partie de la communauté des services financiers ne manque ni de ressources ni de capacités pour mettre en œuvre des solutions techniques. Le problème principal est un problème d'action collective : comment organiser au mieux la protection du système entre les États, les autorités financières et l'industrie, et comment optimiser ces ressources ?

La fragmentation actuelle des parties prenantes et des initiatives découle en partie des caractéristiques particulières des cyberrisques et de leur caractère évolutif. Différentes communautés travaillent en silos et abordent le problème sous le prisme de leurs mandats respectifs. La communauté de la surveillance financière se concentre sur la résilience, les diplomates sur les normes de comportement étatique, les agences de sécurité nationale sur les moyens de dissuader ces activités malveillantes et les fabricants sur les risques propres aux entreprises plutôt que sur les risques sectoriels. L'effacement progressif des frontières entre les entreprises de services financiers et les sociétés de technologie s'accompagne d'un brouillage progressif des lignes de responsabilité en matière de sécurité.

La déconnexion entre la finance, la sécurité nationale et les communautés diplomatiques est particulièrement marquée. Alors que les autorités financières sont exposées à des risques exceptionnels provenant des cybermenaces, elles n'ont que des relations ténues avec les organismes chargés de la sécurité nationale, dont l'intervention est pourtant nécessaire pour parer à ces menaces. Ce vide de responsabilité et cette incertitude continue quant aux fonctions et aux mandats en matière de protection du système financier mondial nourrissent les risques. Cette incertitude tient en partie au climat géopolitique actuel et à de fortes méfiances, qui font obstacle à la collaboration au sein de la communauté internationale. La coopération sur la cybersécurité a été entravée, fragmentée et souvent limitée aux cercles de confiance les plus étroits parce qu'elle touche à des intérêts sensibles en matière de sécurité nationale. Pourtant, la coopération internationale et entre les parties prenantes n'est pas un « plus » mais une nécessité.

Une stratégie internationale

Pour une protection plus efficace du système financier mondial contre les cybermenaces, la Fondation Carnegie pour la paix internationale (Carnegie Endowment for International Peace) a publié en novembre 2020 un rapport intitulé *International Strategy to Better Protect the Global Financial System against Cyber Threats*. Rédigé en collaboration avec le Forum économique mondial, ce rapport recommande des mesures précises pour réduire la fragmentation en encourageant la collaboration, aussi bien à l'échelle internationale qu'entre les autorités et organismes publics, les sociétés financières et les entreprises de technologie.

La stratégie repose sur quatre principes. Premièrement, *il faut clarifier les fonctions et les responsabilités*. Quelques pays seulement ont bâti des relations nationales efficaces entre leurs autorités financières, les services de répression, les diplomates ou les autres acteurs publics concernés et l'industrie. La fragmentation actuelle gêne la coopération internationale et nuit à la résilience collective du système international, à son redressement et à ses capacités de riposte.

Deuxièmement, *la collaboration internationale est nécessaire et urgente*. Étant donné l'ampleur de la menace et l'interdépendance mondiale qui caractérise le système, les

États, les sociétés financières et les entreprises de technologie ne peuvent pas se protéger efficacement contre les cybermenaces si elles travaillent seules.

Troisièmement, *une réduction de la fragmentation libérera des capacités pour s'attaquer au problème*. De nombreuses initiatives sont en cours pour mieux protéger les établissements financiers, mais elles demeurent cloisonnées. Certaines sont redondantes, ce qui accroît les coûts de transaction, mais plusieurs d'entre elles sont suffisamment matures pour être partagées, mieux coordonnées et déployées à plus grande échelle à l'international.

Quatrièmement, *la protection du système financier mondial peut être un modèle pour d'autres secteurs*. Le système financier est l'un des rares domaines dans lesquels les pays ont un intérêt commun évident à coopérer, même lorsque les tensions géopolitiques sont fortes. Un effort ciblé sur le secteur financier est un point de départ et pourrait déboucher sur une meilleure protection des autres secteurs.

Parmi les mesures destinées à renforcer la cyberrésilience, le rapport recommande que le CSF établisse un cadre élémentaire pour superviser la gestion des cyberrisques dans les établissements financiers. Les pouvoirs publics et l'industrie doivent renforcer la sécurité en partageant des informations sur les menaces et en créant des équipes d'intervention en cas d'urgence informatique (« Computer Emergency Response Team »/CERT), sur le modèle de la FinCERT d'Israël.

Les autorités financières devraient aussi faire une priorité du renforcement de la résilience du secteur financier contre les attaques ciblant des données et des algorithmes. Ces mesures devraient comprendre la mise en chambre forte sécurisée des données chiffrées pour permettre aux membres de sauvegarder les données des comptes clients en toute sécurité pendant la nuit. Des exercices réguliers simulant des cyberattaques devraient être effectués pour déceler les failles et établir des plans d'action.

Pour renforcer les normes internationales, le rapport recommande que les États indiquent clairement comment ils appliqueront le droit international au cyberespace et qu'ils renforcent les normes pour protéger l'intégrité du système financier. L'Australie, les Pays-Bas et le Royaume-Uni ont déjà fait un premier pas en déclarant que les cyberattaques émanant de l'étranger peuvent être considérées comme un recours illégal à la force ou une ingérence dans les affaires internes d'un autre État.

La cyberrésilience et des normes internationales renforcées peuvent faciliter une riposte collective sous forme de mesures d'exécution du droit ou de réactions multilatérales avec l'industrie. Les ripostes peuvent être des sanctions, des arrestations et des saisies d'avoirs.

Les États peuvent soutenir ces mesures en créant des organismes chargés de les aider à évaluer les menaces et à coordonner les ripostes. Les services de renseignement devraient s'intéresser aux menaces pesant sur le système financier et les États devraient communiquer ces renseignements à leurs alliés et aux pays qui partagent leurs vues.

Renforcer les capacités

La stratégie très complète exposée par le rapport Carnegie repose à son tour sur l'augmentation du personnel chargé de la cybersécurité, l'expansion des capacités du secteur financier en matière de cybersécurité et la protection des progrès en matière d'inclusion financière accomplis grâce à la transformation numérique.

La hausse du chômage due à la pandémie offre une importante occasion de former et recruter des individus de talent afin de renforcer les effectifs de cybersécurité. Les entreprises de services financiers doivent investir dans des initiatives pour développer le vivier de talents, notamment dans des programmes avec les établissements d'enseignement supérieur et universitaire et dans des programmes d'apprentissage.

Renforcer les capacités en matière de cybersécurité implique de s'efforcer de porter assistance là où c'est nécessaire. Le FMI et d'autres organisations internationales ont reçu de nombreuses demandes d'assistance dans le domaine de la cybersécurité émanant des pays membres, en particulier après l'incident de 2016 au Bangladesh. Les États membres du G20 et leurs banques centrales pourraient créer un mécanisme international qui viserait à renforcer les capacités en matière de cybersécurité pour le secteur financier et dont les efforts seraient coordonnés par une organisation internationale comme le FMI. L'Organisation de coopération et de développement économiques et les institutions financières internationales devraient inclure le renforcement des capacités en matière de cybersécurité dans leurs programmes d'aide au développement et fortement augmenter les aides aux pays qui en ont besoin.

Enfin, la poursuite des progrès dans le domaine de l'inclusion financière exige de renforcer les liens entre l'inclusion financière et la cybersécurité. Ceci est particulièrement urgent en Afrique, où le secteur financier de nombreux pays enregistre une transformation sensible à mesure que progressent l'inclusion financière et l'adoption des services financiers numériques. Il conviendrait par ailleurs de créer un réseau d'experts qui se consacrerait à la cybersécurité en Afrique.

Le moment est venu pour la communauté internationale — États, banques centrales, autorités de surveillance, industrie et autres parties prenantes — de se réunir pour relever ce défi urgent et important. Une stratégie bien pensée, comme celle qui est exposée ci-dessus, constitue une feuille de route pour traduire les paroles en actes. FD

TIM MAURER est directeur de la Cyber Policy Initiative et chercheur principal dans le cadre du programme Technologies et affaires internationales de la Fondation Carnegie pour la paix internationale. **ARTHUR NELSON** est analyste de recherche au sein de la Cyber Policy Initiative de la Fondation Carnegie.