HCSF
Haut Conseil de Stabilité Financière

NOTE

Risque cyber et stabilité financière : revue de littérature

Synthèse

La dimension potentiellement systémique du risque cyber fait l'objet d'une attention croissante de la part des régulateurs, superviseurs, organisations internationales, universitaires, think tanks, etc. Ce panorama s'attache à passer en revue les publications sur le sujet et aborde quatre principaux aspects :

- Le poids économique des incidents cyber. En dépit d'importantes difficultés de mesure, les études disponibles suggèrent une forte hausse du coût des cyberattaques ces dernières années et des pertes agrégées significatives pour le système financier.

- Les incidences du risque cyber pour la stabilité financière. Les cyberattaques peuvent constituer une menace pour la stabilité financière à travers leur impact sur une institution donnée, sur plusieurs composantes du système financier ou bien indirectement sur des infrastructures non financières sur lesquelles repose le système financier. Plusieurs canaux de transmission sont identifiés : perte de confiance dans le système financier, manque de substituabilité des services clés, interconnexions d'ordre financier et d'ordre technologique et opérationnel. De potentielles perturbations des infrastructures de marché tels que les systèmes de paiements d'importance systémique figurent ainsi parmi les scénarios à fort impact étudiés. Les liens de la chaine d'approvisionnement, les rendements des actions ou encore les interdépendances de l'externalisation croissante des services TIC (technologies de l'information et de la communication) sont autant de déclinaisons des interconnexions témoignant de la capacité de propagation des incidents cybers.

- Les récentes évolutions en termes d'innovation technologique, intelligence artificielle et informatique quantique. Elles ont initié de profonds changements, constituent de nouvelles menaces ou amplifient des risques déjà existants sur la cybersécurité du secteur financier.

- Les axes de renforcement de la résilience du système financier. La nécessité de mieux identifier les principales sources de risque cyber et leurs impacts à l'échelle du système financier ainsi que le renforcement de la capacité de réponse collective aux incidents cyber de grande ampleur figurent parmi les préconisations fréquemment évoquées. L'entrée en application du règlement Digital Operational Resilience Act (DORA) le 17 janvier 2025 et sa mise en œuvre par les autorités de supervision sont sources d'améliorations en la matière.

Le risque cyber[1] **figure parmi les risques à haute probabilité et à fort impact** identifiés dans le Global Risk Report du World Economic Forum (WEF, 2016). Outre la vitesse et l'ampleur de leur propagation, les chocs cyber se distinguent des chocs financiers traditionnels par la possibilité de choisir

[1] Selon le Cyber Lexicon du FSB (2018), le risque cyber fait référence à « *la combinaison de la probabilité de survenance d'incidents cyber et leur impact* ». Un incident cyber peut à son tour se définir comme « *toute occurrence observable dans un système d'information qui : (i) met en péril la cybersécurité d'un système d'information ou les informations traitées, stockées ou transmises par le système ; ou (ii) enfreint les politiques de sécurité, les procédures de sécurité ou les politiques d'utilisation acceptable, qu'elle résulte ou non d'une activité malveillante* ».

le moment de l'attaque pour maximiser les dommages, **la complexité du cyberespace et de ses effets en cascade**, et **l'intention malveillante** qui anime ses instigateurs (Healey et al., 2018).

Par ailleurs, contrairement aux risques financiers, tels que le risque de crédit ou de marché, et compte tenu de la nature très évolutive des cyberattaques et du manque de données empiriques, le risque cyber ne peut pas être facilement modélisé, mesuré ou couvert sur la base de données historiques, comme cela peut être fait avec le risque de crédit par exemple (Institute of International Finance, 2017).

La numérisation croissante des services financiers associée à la présence d'actifs et de données de grande valeur rend le système financier particulièrement vulnérable aux cyberattaques (CERS, 2020), qu'elles soient ciblées ou opportunistes. D'après le FMI (Rapport sur la stabilité financière du monde, 2024), les sociétés financières sont concernées par près d'un cinquième des attaques et les banques sont les établissements les plus exposés. Les analyses de l'ENISA (ENISA Threat Landscape : Finance Sector, février 2025) portant sur 432 cyberattaques rendues publiques ayant visé le secteur financier, principalement européen, entre janvier 2023 et juin 2024, montrent que les établissements bancaires sont les cibles les plus fréquentes (46 % des cyberattaques observées).

Trois dynamiques structurelles viennent encore accentuer cette exposition. Premièrement, le recours massif à des prestataires externes de services TIC crée des dépendances technologiques pouvant se transformer en vecteurs d'attaque. Deuxièmement, la détérioration du contexte géopolitique mondial alimente la multiplication des campagnes cyber hostiles. Les bases de données d'incidents montrent une accélération des attaques autour de périodes de tension internationale. Selon la CISSM Cyber Events Database et des analyses de la Banque de France (Rapport sur la stabilité financière, 2025), le nombre d'incidents déclarés est passé d'environ 1 300 en 2021 à plus de 2 000 en 2022. Cette augmentation est notable, mais doit être replacée dans une dynamique pluriannuelle : les données d'autres sources, comme Hackmageddon — qui recense davantage d'événements — suggèrent que la hausse la plus marquée s'est produite entre 2022 et 2023, et que l'intensification varie selon les régions, notamment celles directement concernées par des conflits. Par ailleurs, ces évolutions peuvent aussi refléter une amélioration des *reporting*. Troisièmement, l'innovation technologique agit comme un multiplicateur de risques. L'essor de l'intelligence artificielle dans les services financiers renforce à la fois les capacités de détection et de défense, mais aussi la surface d'attaque et les risques d'erreur ou de manipulation (ESMA, 2023 ; FMI, Shabsigh & Boukherouaa, 2023). De même, les progrès rapides de l'informatique quantique pourraient, à moyen terme, remettre en cause les fondements mêmes de la cryptographie moderne, sur laquelle repose la sécurité des échanges financiers (Radanliev, 2024).

La présente note propose une revue de la littérature récente sur le risque cyber : elle quantifie ses coûts économiques (I), analyse ses canaux de transmission à la stabilité financière (II) et synthétise les principaux leviers de renforcement de la résilience du système financier (III).

I. Le poids économique des incidents cyber

A. Des pertes financières en forte hausse dans le secteur financier

D'après le FMI, les pertes consécutives à une cyberattaque sont généralement jusqu'à cinq fois supérieures à celles résultant d'incidents non malveillants. En 2024, le secteur financier mondial aurait cumulé près de 12 milliards de dollars de pertes liées aux cyberattaques subies depuis 2004. Le FMI estime par ailleurs que le risque de pertes extrêmes continue de croître de manière significative : ainsi, en 2021, les pertes médianes pour les entreprises financières d'un pays sont estimées à 152m$ en 2021 contre 21m$ en 2017 (Rapport sur la stabilité financière du monde, 2024). Le FMI estime même qu'une fois tous les dix ans, un incident cyber peut générer, pour une institution, jusqu'à 2,2 milliards de dollars de pertes (contre 285 millions en 2017)[2]. Par ailleurs, le nombre d'organisations ciblées chaque semaine par une cyberattaque a doublé en quatre ans, atteignant environ 1 984 au deuxième trimestre 2025[3].

L'édition 2025 du rapport Marsh sur les dommages de cyber-assurance en Europe continentale (The Evolution of Cyber Claims in Europe, 2025) montre une hausse de 61 % des demandes d'indemnisation liées à des incidents cyber en 2024 par rapport à 2023[4]. En France, l'AMRAE (LUCY : Lumière sur la CYberassurance, 2025) fait état d'une légère augmentation du montant total des sinistres indemnisés, atteignant 54m€ en 2024.

B. Des coûts encore mal mesurés

Néanmoins, les coûts associés aux incidents cyber demeurent particulièrement difficiles à estimer de manière fiable. Outre une notification encore très partielle des incidents et des pertes associées, ainsi que des problèmes de comparabilité des données en raison de l'absence d'une classification commune, l'évaluation du coût total doit également intégrer les pertes indirectes : atteinte à la réputation, dépréciation des actifs immatériels tels que la propriété intellectuelle, ou encore augmentation du coût des primes d'assurance. Ces effets différés dans le temps complexifient l'estimation *ex ante* des coûts à long terme des incidents (FMI, 2017).

Dans une revue de littérature, Cremer et al. (2022) constatent cependant de profondes lacunes dans les données disponibles, souvent non standardisées, incomplètes, et fondées sur des méthodologies devenues obsolètes au regard des évolutions du *machine learning*. Ils soulignent également que les modèles et approches de modélisation restent, pour beaucoup, mal adaptés aux spécificités du risque cyber : phénomènes d'accumulation et de contagion, probabilité de sinistres extrêmes, forte dimension comportementale et humaine (erreurs, négligences, ingénierie sociale), qui échappent en partie aux cadres actuels de quantification. Ces lacunes s'avèrent d'autant plus coûteuses que les assureurs ne peuvent s'appuyer que sur des données historiques pour évaluer les coûts, pouvant induire une surévaluation des primes de couverture (Kshetri, 2019).

Le World Economic Forum a introduit en 2015 le concept de *Cyber Value-at-Risk*, une approche quantitative visant à standardiser la mesure du risque cyber, optimiser la fixation des primes d'assurance et améliorer la gestion des incidents (Erola et al., 2022 ; Franco et al., 2024). Toutefois, la qualité de ces estimations dépend, une fois de plus, étroitement de la fiabilité et de la profondeur des données

[2] Les estimations annuelles reposent sur la médiane des estimations, tandis que les pertes une fois par décennie reposent sur le dernier décile des estimations.

[3] Check Point Research (CPR), Threat Intelligence Report du 21 juillet 2025. CPR indique 1 984 attaques hebdomadaires en moyenne par organisation au T2 2025, avec l'éducation comme secteur le plus ciblé et l'Europe affichant la plus forte progression régionale (+22 %). Il s'agit d'un chiffre mondial, tous secteurs confondus, calculé à partir de la télémétrie CPR (tentatives/blocages compris, pas uniquement des compromissions réussies).

[4] Ces évolutions doivent toutefois être interprétées avec prudence : l'augmentation du nombre et du montant des indemnisations reflète non seulement une sinistralité accrue, mais aussi l'essor du marché de la cyberassurance (plus grand nombre d'entreprises couvertes, extension des garanties).

historiques disponibles. Dans cette lignée, la modélisation proposée par Dreyer et al. (2018) évalue les coûts totaux (directs et systémiques) entre 799 milliards et 22 500 milliards de dollars, selon les hypothèses d'interconnexion entre secteurs et les effets de cascade considérés. Jamilov et al. (2023) ont estimé, à partir des données de 13 000 entreprises réparties dans 85 pays entre 2012 et 2021, que le coût global du risque cyber dépassait 200 milliards de dollars par an. Leur approche innovante consiste à mesurer le coût de l'exposition au risque cyber, et non plus seulement celui des atteintes directes. Ils montrent ainsi que le degré d'exposition à ce risque prédit la survenance d'attaques et influe négativement sur les profits et les rendements boursiers. Les auteurs observent aussi des effets mesurables sur le marché des options.

Pour faciliter l'analyse et la classification du risque cyber, Eling et Wirfs (2019) proposent de le rapprocher des risques opérationnels, dont les origines présentent des similitudes importantes. Sur la base de 26 541 incidents recensés entre 1995 et mars 2014, ils identifient l'erreur ou l'acte humain comme première cause d'occurrence (près de 80 %), qu'il s'agisse d'actes malveillants (intrusion, vol de données) ou d'erreurs involontaires. Les autres causes relèvent de défaillances techniques, informatiques ou externes. Les auteurs mettent en avant le poids potentiellement déterminant de la dimension réputationnelle des incidents cyber, qui affectent la confiance et la valeur perçue de l'entreprise, même lorsque les pertes financières directes restent limitées. Cette appréciation doit toutefois être nuancée : d'autres travaux empiriques soulignent que la rupture d'activité, via l'interruption ou la dégradation des services, constitue souvent le principal poste de coût mesurable (par exemple Low, 2017). La littérature ne converge donc pas pleinement sur la hiérarchie des composantes de coût, en partie en raison des difficultés de quantification des effets réputationnels.

Certaines études ont cherché à quantifier plus précisément l'impact agrégé des cyberattaques sur le système financier. Bouveret (2018) évalue les pertes moyennes annuelles à 97 milliards de dollars pour les pays de l'échantillon, soit environ 9 % du revenu net des banques, et jusqu'à 268 milliards de dollars (26 %) dans un scénario aggravé où la fréquence des attaques serait doublée par rapport à 2013. L'introduction d'effets de contagion interbancaire augmenterait encore les pertes d'environ 20 %.

Aldasoro et al. (2020) montrent que les coûts liés aux incidents cyber sont plus élevés pour les grandes entreprises, ainsi que pour les attaques affectant simultanément plusieurs organisations. Le secteur financier, bien que plus souvent ciblé, subit des pertes moyennes moindres grâce à des investissements plus importants dans la sécurité informatique. *In fine*, les pertes associées au risque cyber ne représentent encore qu'une fraction des pertes opérationnelles totales, mais peuvent atteindre jusqu'à un tiers de la *Value-at-Risk* opérationnelle globale (BIS, 2020).

L'entrée en application du règlement (UE) 2022/2554, dit « DORA » (Digital Operational Resilience Act), devrait contribuer à pallier les manquements en termes de données dans l'évaluation des incidents cyber. Le règlement vise précisément à améliorer la visibilité sur les coûts des incidents TIC majeurs en imposant aux entités financières de son champ d'application, réparties en vingt-et-une catégorie, d'estimer les conséquences économiques de chaque incident informatique majeur au sens de DORA (article 18.1.f) et de produire annuellement un rapport agrégé des coûts et pertes directs et indirects causés par l'ensemble de leurs incidents informatiques majeurs sur l'année (article 11.10).

C. Un marché de la cyber-assurance en expansion mais encore immature

Plusieurs états des lieux réalisés à la fin des années 2010 – OCDE (2017), Geneva Association (2018), Institute of International Finance (2019) – soulignaient la maturité encore incomplète du marché. Des travaux menés dans le cadre du dialogue UE-États-Unis (The Cyber Insurance Market Working Group, 2020) et de l'IAIS (2020) ont confirmé ces constats, relevant des pratiques de supervision hétérogènes et identifiant cinq principaux obstacles à une meilleure évaluation du risque : manque d'historique, une volatilité intrinsèque élevée (forte variance et évolution très rapide du risque), une faible maturité du marché, des risques d'accumulation combinés à la possibilité d'événements individuels aux coûts

extrêmement élevés (événements extrêmes), et l'existence de couvertures non affirmatives. Les clauses cyber et les exclusions ont été progressivement clarifiées afin d'éviter les couvertures « silencieuses » et de sécuriser les assurés tout en consolidant la stabilité financière des assureurs.

L'assurance cyber poursuit néanmoins sa montée en puissance – les grandes entreprises sont presque toutes assurées et le taux de couverture des PME et ETI progresse chaque année. Le marché devrait continuer de croître sous l'effet de la numérisation généralisée des activités, de la hausse du nombre et de la gravité des incidents, ainsi que du renforcement des obligations réglementaires. En France, l'Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE) constate que le nombre de PME et d'ETI ayant souscrit une assurance cyber a progressé d'environ un tiers en 2024, confirmant une pénétration plus large au sein du tissu économique, alors que ce type de couverture a d'abord été souscrit par les grandes entreprises. Le dynamisme de la concurrence sur ce marché et la généralisation de mesures de protection élémentaires tirent les primes vers le bas, contribuant à faire de l'assurance cyber un produit de plus en plus abordable.

Bien que le marché reste relativement concentré (IAIS, Global Insurance Market Report, 2025) et encore largement tiré par les États-Unis, il devrait atteindre 16,3 milliards de dollars en 2025, contre 15,3 milliards en 2024 (Munich Re, Global Cyber Risk and Insurance Survey 2024).

L'assurabilité du risque cyber demeure toutefois particulièrement complexe, en raison de l'évolution rapide des tactiques, techniques et procédures (TTPs) des attaquants et du caractère opportuniste de leurs cibles. La fréquence et l'intensité de la sinistralité en matière de cyberattaque restent volatiles : le ratio sinistres/primes est passé, pour les grandes entreprises, de 190 % en 2020 à 17 % en 2024, et pour les PME, de 45 % à 22 % sur la même période, avec un pic à 100 % en 2022 (AMRAE, 2025).

II. Risque cyber et stabilité financière

Dans un environnement financier de plus en plus numérisé et interconnecté, le risque cyber ne peut plus être appréhendé comme une menace isolée affectant uniquement chaque institution à titre individuel. Il s'agit désormais d'un risque critique capable de perturber l'ensemble du système financier par effet de contagion, en raison de la forte interdépendance entre les acteurs, les infrastructures critiques et les prestataires technologiques. A ce titre, les cyberattaques sont considérées par la BCE comme un risque croissant et majeur pour la stabilité financière (Macroprudential bulletin, 27 mars 2025, BCE) nécessitant une approche macroprudentielle mobilisant à la fois les autorités publiques, les régulateurs et les opérateurs privés. En outre, les exigences et dispositifs nouvellement introduits par le règlement DORA visent à mieux prémunir le secteur financier européen contre les cyberattaques, et à limiter les effets potentiels d'un incident systémique.

A. Un risque potentiellement systémique

Les cyberattaques peuvent constituer une menace pour la stabilité financière à travers leur **impact sur une institution donnée**, **sur plusieurs composantes du système financier** ou bien indirectement **sur des infrastructures (non financières) sur lesquelles repose le système financier**, telles qu'un fournisseur d'électricité, de télécommunications ou des opérateurs de câbles (IIF). Le CERS (2020) a développé un cadre d'analyse conceptuel appliqué à des scénarios historiques et hypothétiques pour évaluer dans quelles circonstances le risque cyber peut devenir une source de risque systémique pour le système financier.

Le rapport conclut qu'il est possible qu'un incident cyber de grande ampleur affectant le secteur financier puisse dans certaines conditions créer des perturbations pouvant avoir de fortes conséquences adverses sur les marchés et l'économie réelle. **Un incident cyber pourrait ainsi évoluer d'une panne opérationnelle à une crise de liquidité, susceptible de provoquer à son tour une crise systémique**. À cet égard, des pertes financières importantes (réelles ou anticipées) et l'érosion significative de la confiance dans le système financier constituent deux facteurs critiques.

Les premiers travaux empiriques relativisaient la portée intrinsèquement systémique du risque cyber mais mettaient en avant **les conditions dans lesquelles ce risque pouvait devenir systémique**. La Banque d'Angleterre (*Quarterly Bulletin Q4,* 2018) relevait en 2018 que **seuls les États-nations avaient la capacité de provoquer un choc d'une ampleur systémique**. Ce postulat n'est plus vrai en 2025, depuis que l'écosystème cybercriminel s'est fortement industrialisé (Agence nationale de la sécurité des systèmes d'information – ANSSI, 2021) et que les groupes cybercriminels se sont organisés, pour les plus sophistiqués, à la manière d'entreprises (TrendMicro, *Inside the Halls of a Cybercrime Business*, 2023). Ainsi, l'attaque par rançongiciel de 2022 contre des infrastructures critiques du Costa Rica, imputée au groupe cybercriminel Conti, n'a a priori pas été parrainée par un État-Nation. Pourtant, elle a tant affecté le fonctionnement des agences gouvernementales du pays que le président Rodrigo Chaves a dû déclarer l'état d'urgence national.

L'évolution technologique, rythmée notamment par la démocratisation de l'usage d'outils d'intelligence artificielle générative ainsi que par l'anticipation du passage à l'ère de la cryptographie post-quantique, contribue à renforcer la sophistication de la menace cyber, dans un environnement plus risqué, marqué par un contexte géopolitique tendu (AMRAE, 2025).

B. De multiples canaux de transmission

Plusieurs canaux sont susceptibles d'affecter la stabilité financière (FMI, 2020) :

- une **perte de confiance dans le système financier**, causée par de longues perturbations ou une corruption de l'intégrité des données, avec des conséquences sur la liquidité du système financier. Le FMI (Fabio Natalucci, Mahvash S. Qureshi, Felix Suntheim, *L'intensification des cybermenaces suscite de grandes inquiétudes pour la stabilité financière*, avril 2024) note qu'un incident cyber de grande ampleur dans une institution financière pourrait ébranler la confiance et, dans des cas extrêmes, provoquer des cessions d'actifs massives sur les marchés ou des ruées sur les dépôts bancaires ;
- un **manque de substituabilité des services clés**, parmi lesquels les services de conservation des titres, de compensation centrale ou de paiement. Les systèmes de paiement de gros en temps réel (*real time gross settlement systems*, RTGS) et le système de messagerie SWIFT, parce qu'ils sont cruciaux pour les paiements et règlements en espèces et en titres, sont considérés comme de potentiels « *single point of failure* » (cf. note 2, État des vulnérabilités) dans l'infrastructure de paiement mondiale (WEF). Ainsi, en décembre 2023, la cyberattaque subie par sa banque centrale a désorganisé le système de paiement du Lesotho, empêchant les banques du pays d'effectuer des opérations (Fabio Natalucci, Mahvash S. Qureshi, Felix Suntheim, *L'intensification des cybermenaces suscite de grandes inquiétudes pour la stabilité financière*, avril 2024) ;
- l'**interconnexion au sein du système financier qu'elle soit directe et d'ordre financier** (à travers les transactions bilatérales, les plateformes de trading, règlement, compensation ; la banque centrale ; les systèmes de paiement…) **ou qu'elle soit indirecte et d'ordre technologique et opérationnel** (exposition à du matériel et des logiciels communs, à des fournisseurs communs de services technologiques tels que le *cloud*).

Sur ce dernier point, Healey *et al.* (2018) identifient le manque de substituabilité des technologies de l'information et de la communication comme un canal à part entière. Ils notent en effet que les entreprises informatiques ont tendance à être extrêmement similaires et à dépendre des mêmes systèmes d'exploitation, des mêmes applications et des mêmes protocoles (e.g., Internet). Enfin, les catastrophes locales révèlent souvent des dépendances physiques inattendues en perturbant des régions ou des industries entières.

Parmi les services financiers clés, de potentielles perturbations d'un système de paiement d'importance systémique figurent parmi les scénarios à fort impact souvent examinés. L'incertitude quant au caractère

définitif des règlements aurait de larges répercussions sur les chaines complexes de participants impliqués (IIF). Un incident entrainant dans un premier temps l'indisponibilité des dépôts et des soldes de comptes d'une grande banque pourrait, à travers le canal de la confiance, induire des problématiques de liquidité pour d'autres banques qui n'étaient initialement pas affectées par l'incident, l'incertitude pouvant être alimentée par les fausses nouvelles propagées sur les réseaux sociaux (CERS). Un article d'Eisenbach, Kovner, and Lee (Fed Staff Report, 2020) montre qu'une cyberattaque sur le réseau de paiements de gros d'un des cinq plus grands participants du système de paiement américain affecterait en moyenne 38 % du réseau (en termes d'actifs bancaires, en dehors de la banque ciblée), tandis qu'un « scénario de cascade » dans lequel les institutions répondent cette fois stratégiquement à la dégradation de leurs soldes en cours de journée en renonçant à leurs paiements et en thésaurisant des liquidités, aboutirait à des abandons de paiements de l'ordre de 5 % à 35 % de la valeur totale des paiements quotidiens (soit 1 à 11 fois le PIB quotidien des États-Unis). À partir de l'analyse d'un échantillon de douze institutions financières américaines d'importance systémique, Duffie and Younger (2019) estiment que celles-ci disposent de stocks suffisants d'actifs liquides de haute qualité pour couvrir les retraits des investisseurs de gros en cas de *cyber-run*[5] relativement important mais suggèrent que cela ne garantit pas pour autant que le système de paiement continuerait à traiter les paiements suffisamment rapidement pour éviter des dommages à l'économie réelle. Des exemples d'attaques à visée de sabotage à l'encontre de banques sud-coréennes en 2013, imputées à la Corée du Nord (McAfee, 2013), ou en 2022, à l'encontre de banques ukrainiennes, imputées à la Russie (Microsoft, 2022), ou encore en 2024 à l'encontre de distributeurs automatiques de billets en Russie, imputées à l'Ukraine (Kyiv Post, 2024), illustrent que la perturbation du système de paiement d'un pays par le biais de cyberattaques visant ses banques est une technique de déstabilisation utilisée en appui d'un conflit armé. De même, les attaques par saturation (dites « DDoS »), ciblent régulièrement les banques de pays impliqués dans des conflits armés, et sont généralement soutenues par des campagnes d'agitation et de propagande à visée amplificatrice (Citalid, 2024).

Parmi les scénarios étudiés, une corruption simultanée de l'intégrité des données d'une banque dépositaire et de l'un des grands dépositaires centraux de titres rendrait difficile le recoupement ou la reconstruction des opérations communes entre ces entités, avec des effets négatifs sur le traitement et le prix des titres concernés, les échanges, et plus globalement sur la confiance (IIF, 2017). De même, la manipulation simultanée des flux de prix de plusieurs marchés de matières premières et de marchés à terme, ainsi que des informations données par une chambre de compensation, provoquerait des pertes importantes pour de nombreux participants de marché, même si cela ne menacerait pas nécessairement la stabilité financière (CERS). De manière générale, la corruption de l'intégrité des données peut exiger des arbitrages délicats entre la nécessité d'opérer une récupération rapide des données et celle de garantir leur exactitude et leur sûreté afin d'éviter une propagation des risques dans le système (OFR, 2017).

C. La portée des interconnexions

Des études s'attachent à analyser l'**ampleur de la propagation des impacts des incidents cyber, au-delà des victimes directes de ceux-ci**. En se fondant sur l'étude de l'attaque NotPetya[6] en 2017, Crosigni *et al*. montrent qu'à travers les liens de la chaine d'approvisionnement, **les effets de l'attaque se sont propagés en « aval » aux clients des entreprises directement touchées par le code malveillant**, affectant nettement leurs capacités productives et leurs bénéfices par rapport à leurs pairs (et ce, d'autant plus que leurs fournisseurs étaient peu substituables) et les contraignant à utiliser leurs liquidités et augmenter leurs emprunts. Les auteurs estiment la **chute des bénéfices pour les entreprises clientes** concernées à 7,3 milliards de dollars, soit un montant **quatre fois supérieur aux pertes**

[5] Un « *cyber-run* » est un scénario dans lequel une cyberattaque provoque un « *bank run* » et une crise de liquidité.
[6] Attaque par rançongiciel, imputée à la Russie, qui avait ciblé les systèmes d'information d'institutions et d'entreprises ukrainiennes et qui s'était ensuite propagée à d'autres pays.

signalées par les entreprises directement touchées par la cyberattaque. L'exemple plus récent, datant de novembre 2023, de la compromission par un rançongiciel de la filiale américaine de la banque nationale chinoise ICBC (ICBC Financial Services)[7], esquisse en outre l'ampleur que pourrait avoir une cyberattaque sur un acteur financier particulièrement interconnecté. Du fait de sa compromission par des affiliés du groupe de cybercriminels opérant le rançongiciel LockBit, ses employés n'ont pas pu régler d'importants lots d'opérations sur les bons du Trésor américain pour le compte d'autres participants du marché. ICBC a donc dû injecter des capitaux en urgence au sein de sa filiale et les détails du règlement ont été transmis aux participants du marché concernés de manière dégradée, à savoir via des clés USB (Banque de France, décembre 2023). D'autres participants, moins directement affectés, ont redirigé leurs transactions vers d'autres entreprises par précaution. Bien qu'ICBC Financial Services ne soit qu'une entreprise de taille moyenne par laquelle les plus grands acteurs du marché ne passent pas, et que l'attaque n'ait affecté qu'une partie limitée de son système d'information du fait du caractère obsolète de certains serveurs de l'entité qui n'a pas permis au code malveillant de s'y installer (Bloomberg, 2023), l'attaque a tout de même eu un impact sur la liquidité du marché des bons du Trésor (*cash* et repo), ainsi que sur certaines opérations actions, pour un total notionnel de transactions en suspens de 37 milliards de dollars environ.

À partir d'analyses textuelles portant sur les conférences de résultats trimestriels des entreprises, Jamilov *et al*. (2023) mettent en évidence un **impact négatif des incidents cyber non seulement sur les rendements des actions des entreprises affectées mais également sur les entreprises non affectées d'un même secteur dans un même pays**. Dans la même veine, Kamiya *et al*. (*2021*) montrent que les cyberattaques impliquant la perte d'informations financières personnelles induisent une perte de richesse importante pour les actionnaires des entreprises ciblées, en grande partie liées à des coûts réputationnels, et affectent également le cours des actions des autres entreprises de leur secteur. Ces coûts réputationnels peuvent être accentués par les attaquants eux-mêmes : par exemple, en juin 2024, la coopérative financière brésilienne Sicoob a été compromise par des attaquants qui ont revendiqué lui avoir dérobé des données sensibles et ont cherché à attenter à sa réputation en d'une part la qualifiant de « banque la plus dangereuse du Brésil » et d'autre part en incitant ses clients à retirer leurs dépôts (Citalid, 2024).

L'adoption de nouvelles technologies telles que le *cloud* crée de nouvelles interdépendances, y compris avec des entités opérant en dehors des limites des systèmes financiers réglementés. Si le *cloud* peut permettre de renforcer de manière significative la résilience des institutions considérées individuellement, la concentration potentielle de la fourniture de ces services pourrait entraîner des effets systémiques en cas de défaillance opérationnelle à grande échelle ou d'insolvabilité (FSB, 2019). Lloyds estime qu'un cyber-incident provoquant la mise hors ligne d'un des trois premiers fournisseurs de *cloud* aux États-Unis[8] pendant 3 à 6 jours entraînerait des pertes totales de l'ordre de 7 à 15 milliards de dollars, dont 1,5 et 3 milliards de pertes assurées (*Cloud Down*, 2018). À partir d'un modèle stylisé appliqué aux membres compensateurs d'une chambre de compensation centrale, l'étude d'Asensio, Bouveret, Harris (ESMA, 2021) suggère que la forte concentration des fournisseurs de *cloud* pourrait créer des risques pour la stabilité financière si une panne chez l'un d'entre eux affecte nombre de ses clients, augmentant la probabilité de pannes simultanées. Ce risque de concentration s'est matérialisé par la panne d'une durée approximative de 15 heures du service *Cloud* d'Amazon, Amazon Web Services, en octobre 2025, qui a affecté nombre de grandes entreprises parmi lesquelles la banque Lloyds et le service de paiement Venmo. Au-delà du secteur du *Cloud*, il est nécessaire d'évoquer également la panne mondiale de juillet 2024 qui a découlé d'une mise à jour défectueuse d'un logiciel fourni par le prestataire de services en cybersécurité Crowdstrike. 8,5 millions d'ordinateurs et de serveurs à travers

[7] ICBC Financial Services fournit principalement des services de compensation, d'exécution et de financement à des clients institutionnels et sert d'intermédiaire pour les gouvernements, les fonds spéculatifs et les négociateurs pour compte propre qui souhaitent acheter et vendre de la dette américaine.

[8] *Amazon Web Services*, *Microsoft Azure* et *Google Cloud*.

le monde utilisant le système d'exploitation Microsoft Windows n'ont en conséquence pas pu démarrer, affectant de nombreux secteurs économiques. Le recours à une stratégie multi-fournisseurs permettrait de réduire ce risque systémique si les fournisseurs de *cloud* présentent des vulnérabilités communes limitées. Cependant, la mise en œuvre d'une telle stratégie s'avère encore complexe pour divers facteurs dont les coûts, la dépendance au chemin et les limites de compatibilité technologiques, ou encore la forte concentration de certains services (e.g., Cloud).

Plus largement, alors que les entreprises améliorent la défense de leurs systèmes d'information, les attaquants cherchent de plus en plus à compromettre en amont un élément de la chaîne d'approvisionnement, jugé de confiance par la victime, afin de l'atteindre de manière indirecte. Les attaquants peuvent ainsi compromettre la mise à jour d'un logiciel, comme l'illustrent l'attaque de 2017 dite « NotPetya » ou plus récemment l'attaque de 2021 dite « SolarWinds ». Les attaquants peuvent également porter atteinte à des prestataires de services informatiques fournissant des services d'infogérance car ils disposent d'interconnexions réseau avec leurs clients leur offrant des possibilités de latéralisation vers le réseau de ceux-ci. L'ANSSI continue d'identifier en 2025 les attaques par la chaîne d'approvisionnement comme une tendance forte permettant aux attaquants d'atteindre leurs cibles finales plus discrètement (ANSSI, 2025).

D. Un impact sur la notation de crédit

Si les cyberattaques n'ont eu jusqu'à présent qu'un effet limité sur les notations de crédit des institutions financières, la fréquence et la complexité croissantes des attaques devraient se traduire à l'avenir par davantage d'actions de notation (S&P Global, *Cyber Risk In A New Era,* 2020-2021). La présence d'un cadre de cybersécurité robuste est essentielle, et les standards de gouvernance cyber font notamment l'objet d'une attention croissante. Toutefois, en cas de cyberattaque, une détection et une remédiation rapides peuvent constituer le facteur clé pour éviter d'affecter la réputation et la confiance des clients, et ainsi le profil de crédit de l'entreprise. En 2019, S&P a dégradé la note de la Bank of Valletta à la suite d'une cyberattaque ayant renforcé les inquiétudes relatives à la robustesse de son cadre de gestion des risques opérationnels. Les attaques causant une perturbation des opérations sont susceptibles d'avoir un effet négatif plus marqué sur les notes de crédit que celles ciblant le vol de données clients (S&P Global). La même année, Moody's a dégradé la perspective de notation de crédit (*credit rating outlook*) d'Equifax après qu'en 2017, des attaquants aient compromis son système d'information et fait fuiter les données d'environ 147 millions de consommateurs américains.

E. Un enjeu de disponibilités des données

Les travaux académiques spécifiques à la cybersécurité restent limités par la disponibilité des données. Cependant, de nouvelles bases de données émergent et permettent de suivre l'exposition de l'industrie aux risques cyber. Le *Center for international and security studies* (CISSM) de l'Université du Maryland propose une base de données consolidée des incidents cybers recensés sur les réseaux sociaux. En raison de sa couverture globale et multisectorielle, cette base fait désormais figure de référence internationale. Ainsi, en 2024, les industries financière et bancaire représentaient 12 % des attaques. En Europe, l'Agence européenne pour la cybersécurité (ENISA), recense 488 institutions victimes de cyber attaques entre juin 2023 et 2024. En France, Dacoragna et al. (2023) ont montré que les données de plaintes pour cyber attaques de la Gendarmerie Nationale pouvaient permettre une estimation des coûts associés aux incidents cyber pour les Français. En mobilisant des données sur les vulnérabilités informatiques issues de la National Vulnerability Database (NVD)[9], ainsi que la base d'incidents

[9] La National Vulnerability Database (NVD) est une base de données construite par la NIST (US National Institute of Standards and Technology) recensant vulnérabilités à l'échelle mondiale et non uniquement pour les entreprises américaines.

Hackmageddon[10], Boumezoued et al. (2023) montrent que des chocs externes, tels que la publication d'une vulnérabilité cyber, augmentent la probabilité d'être victime d'une attaque à court terme. Ce travail a été récemment actualisé (*Cyber Risk Frequency Modelling Using Hawkes Processes: Calibration on Attack and Vulnerability Data*, 2024), confirmant l'existence de dynamiques d'auto-excitation et de contagion dans la survenance des attaques. Shabad (2025) fait aussi remarquer que ce problème de disponibilité des données s'applique aussi aux prestataires de technologies opérationnelles et que ces manquements sont d'autant plus forts qu'ils se cumulent à des biais comportementaux, entre autres. Salzberger (2025) a démontré que les dirigeants d'entreprises allemands présentaient un biais systématique à sous-évaluer leurs expositions aux risques et à surévaluer leurs capacités de défense (Salzberger, 2025).

F. Des risques accentués par l'émergence de l'intelligence artificielle

La généralisation rapide de l'intelligence artificielle (IA) au sein de l'industrie financière appelle à la mise en place de nouveaux cadres de gestion. Pour autant, ces risques ne paraissent pas fondamentalement nouveaux. Il semble que l'IA tend surtout à amplifier les risques déjà présents pour l'industrie financière.

- Perte d'indépendance technologique

Le recours normalisé à l'IA génère de nouveaux risques de dépendance technologique vis-à-vis des fournisseurs. Les utilisateurs d'application d'IA sont ainsi entrés dans un rapport de force largement dominé par les éditeurs, fortement concentrés dans un oligopole[11]. Les prestataires tiers de service d'IA sont devenus des acteurs systémiques pour l'industrie financière, notamment, puisque le défaut de l'un d'eux peut constituer un risque de panne sur une fraction conséquente de l'industrie, d'autant qu'il est difficile pour un client de changer de fournisseur.

Il s'agit d'un risque de perte d'autonomie technologique auquel s'ajoute celui de la souveraineté de l'IA et de l'alignement avec les réglementations européennes et nationales, notamment en termes de protection des données. Si l'UE a fait de la souveraineté digitale l'un des principaux enjeux de son Cyber agenda, la capacité à protéger les citoyens d'utilisation non-désirée ou malintentionnée de leurs données est loin d'être acquise voire réaliste dans une industrie où l'essentiel des fournisseurs de ces services sont américains ou chinois (Calderaro et Blumfelde, 2022).

- Les risques opérationnels exacerbés

Pour dépasser les capacités computationnelles classiques et outrepasser des manquements de données, les modèles d'IA ont fréquemment recours à des données synthétiques. Cependant, cette pratique porte le risque de fonder des analyses sur des informations incomplètes et/ou opaques, au détriment de la compréhension des modèles (Shabsight et Boukherouaa, 2023). De plus, le recours à des données de sources alternatives pour le secteur financier (réseaux sociaux, presse, images, etc.) implique une attention plus importante pour tenir compte des spécificités de chaque source et échapper à des biais de subjectivité (Ntoutsi et al., 2019).

[10] Base de données indépendante couvrant des incidents sur toutes zones géographiques (35 % des incidents y sont recensés aux États-Unis).

[11] Le rapport de force est d'autant plus fort que les algorithmes d'IA générative sont, pour les principaux, la propriété unique de leur éditeur (Meta, OpenAI, Alphabet, …) qui protègent ces codes de la concurrence, les rendant opaques. À l'inverse, les précédentes avancées dans les algorithmes de *machine learning* ont été portées par les milieux académiques en *open source*, garantissant la transparence.

De manière générale, en plus des données, c'est le processus de décision des algorithmes d'IA qui est opaque et peut générer un déficit d'explicabilité[12], pouvant affecter les risques opérationnels liés aux prises de décisions des individus (Solaimani et Long, 2025). La confiance des investisseurs dans l'IA se heurte à la fiabilité et la prédictibilité de leurs résultats, notamment dans le cas des IA basées sur des modèles probabilistes (e.g., les IA génératives). Par ailleurs, les IA sont également sujettes à des erreurs pouvant résulter des modèles et leur entraînement ou encore de biais d'entrée, générant des hallucinations, c'est-à-dire des réponses incorrectes données avec un fort degré de certitude par l'IA (Lo et Singh, 2023).

L'IA crée aussi de nouvelles expositions aux risques pour les investisseurs. L'IA peut produire ou relayer des informations erronées d'apparence crédible, que ce soit du fait de biais dans ses données d'entraînement ou d'un usage malveillant par son concepteur ou son utilisateur, dans le but de tromper ou manipuler des individus. On parle alors de *fake news* : on peut penser à la fausse vidéo d'incendie du Pentagone le 22 mai 2023 qui avait entraîné des ventes très rapides sur les titres américains l'espace de quelques minutes. Le *deepfake* (manipulation audio-visuelle), est aussi un des cas les plus connus. Le *deepfake* peut conduire un salarié à une erreur opérationnelle ou orienter les décisions d'investisseurs particuliers par exemple.

G. De nouveaux risques induits par l'émergence de l'informatique quantique

L'informatique quantique (*quantum computing* ou QC) est une innovation technologique qui permettra à terme d'augmenter exponentiellement les capacités computationnelles actuelles. Si les bénéfices potentiels sont nombreux pour le secteur financier (e.g. modélisation/simulation, optimisation de processus, puissance de calcul[13]), ce nouveau développement apporte également de nouveaux risques, notamment en ce qui concerne la sécurité des algorithmes de chiffrement utilisés par les entités financières pour sécuriser leurs données[14]. Il existe deux grandes catégories de de chiffrement (NISTRI, 2016 ; Mavroeidis et al., 2018) :

- **Le chiffrement symétrique**, qui est basé sur l'utilisation d'une même clé pour chiffrer et déchiffrer des données. Le chiffrement symétrique est a priori moins exposé au cassage par les QC pour peu que la taille des clés utilisées soit suffisante (Rao et al, 2017) ;
- **Le chiffrement asymétrique**, qui est basé sur l'utilisation de deux clés - l'une publique pour chiffrer, l'autre privée pour déchiffrer - qui sont complémentaires et mobilisées systématiquement pour tout envoi et réception de message sur un système. Les messages peuvent prendre plusieurs formes, du texte ou des transferts monétaires notamment. C'est aussi le système utilisé sur les blockchains pour le transfert de cryptoactifs par exemple. Les algorithmes de recherche du QC sont particulièrement performants pour identifier les clés privées et en déduire les clés publiques, posant un danger important.

Des travaux réalisés dans les années 90 participent déjà à démontrer les implications du QC sur la sécurité des clés de chiffrement : d'une part, l'algorithme cryptographique quantique de Shor (1994) qui démontre la possibilité de casser la cryptographie asymétrique classique, et d'autre part l'algorithme de Grover (1996) sur la réduction du temps pour casser un chiffrement symétrique n'ayant pas une taille de clé suffisante (Auer et al., 2024 ; Vadisetty, 2024).

Ces implications révèlent l'importance de se préparer pour un environnement post-QC (PQC). Les secteurs les plus vulnérables seraient les banques en ligne et mobile, les systèmes de paiements

[12] L'explicabilité dans le domaine de l'IA est définie par la CNIL comme la capacité de mettre en relation et de rendre compréhensible les éléments pris en compte par un système d'IA pour la production d'un résultat.

[13] Quantum computing and the financial system: opportunities and risks, BIS papers n°149, Oct. 2024

[14] La hausse des capacités computationnelles du QC permettra de résoudre avec efficience et dans un délai court les problèmes mathématiques complexes qui servent à chiffrer des clés de sécurités

(virements ou retraits), la sécurité des échanges inter-entreprises et les réseaux VPN selon Deodoro et al. (2021). Dans l'environnement des cryptoactifs, deux études publiées par Deloitte[15] estiment que 25 % du nombre total de Bitcoins en circulation et 65 % des Ethers seraient exposés à un risque de piratage par informatique quantique.

Les risques portés par le QC sont prospectifs et rétroactifs. La technologie n'est pas encore opérationnelle et son horizon reste encore incertain (selon les visions d'expert entre 2030 pour les plus prudents ; 2035 d'après le *Quantum Threat Timeline Report* 2024 du *Global Risk Institute*). Cependant, comme le rappelle Auer et al. (2024) les données chiffrées peuvent, dès à présent, être piratées, non lisibles donc, pour être stockées jusqu'à ce que la technologie soit prête, une menace appelée « *harvest now, decrypt latter* ». Doerr et al (2022) estiment que ces attaques pourraient coûter 1 point de PIB aux économies avancées dans les 15 à 20 prochaines années.

III. Les axes de renforcement de la résilience du système financier face au risque cyber

A. Une harmonisation par le haut pour renforcer la maturité cyber du secteur financier

La nécessité d'une plus grande cohérence des cadres réglementaires nationaux en matière de cybersécurité a longtemps été promue par différentes instances internationales, comme axe de renforcement de la résilience du système financier. Dans un rapport publié en avril 2024, le FMI indique d'ailleurs que les pays où la législation cyber est plus développée apparaissent moins propices à être victimes de cyber incidents (FMI, 2024). Le paquet réglementaire européen DORA, entré en application le 17 janvier 2025, vise, à l'échelle européenne, à renforcer la résilience des entités financières aux cyberattaques (mais aussi aux incidents informatiques d'origine opérationnelle) via plusieurs piliers : un cadre de gestion des risques informatiques et du risque de tiers renforcé, une gestion assidue des incidents informatiques et une déclaration des incidents majeurs au superviseur, le partage d'informations entre pairs et avec le superviseur, l'instauration d'un cadre européen de surveillance permanente d'un certain nombre de prestataires informatiques considérés comme critiques (*Critical Third-Party Providers* ou CTPPs) ainsi que la mise en place de tests de résilience. Sur ce dernier volet, tandis que l'ensemble des entités financières du champ d'application de DORA doivent disposer d'un programme annuel de tests de résilience, un certain nombre d'entités financières, réputées systémiques au niveau national et/ou au sein du Mécanisme de supervision unique (s'agissant des établissements de crédit d'importance significative sous la supervision de la BCE), doivent réaliser des tests d'intrusion avancés fondés sur la menace environ tous les trois ans. Ces tests, dits « TLPT » (pour *Threat-led penetration tests*) sont encadrés par les autorités TLPT. L'ACPR et la Banque de France ont ainsi fondé la TLPT Cyber Team France (TCT-FR), à laquelle s'est jointe l'AMF en 2024. Cette équipe nationale est en charge en France de l'application de l'exigence DORA de réalisation de TLPT triennaux (Banque de France, 2025)[16].

Au niveau international, la BRI (*Committee on Payment and Market Infrastructure*) et l'*International Organization of Securities Commissions* (IOSCO) travaillent de concert sur des orientations sur le risque opérationnel à destination des infrastructures de marchés financiers. Dans la continuité de l'orientation

[15] Deloitte, Quantum computers and the Bitcoin blockchain; et Quantum risk to the Ethereum blockchain – a bump in the road or a brick wall ?

[16] Quand TIBER-SSM l'est pour les établissements de crédit d'importance significative.

cyber publiée en 2017 [17], le *Committee on Payments and Market Infrastructures* (CPMI-IOSCO) a mis en place l'*Operational Resilience Group* en 2024 pour travailler sur les enjeux du risque opérationnel. Le groupe, auquel participe la Banque de France, travaille actuellement sur trois axes : (i) publier un ensemble d'orientations opérationnelles et recommandations sur la gestion du risque cyber (horizon S1 2026), (ii) approfondir les enjeux liés au risque de tiers, (iii) faire une veille sur les risques émergents.

L'ACPR et la Banque de France sont également membres du Comité de Bâle sur le contrôle bancaire (BCBS) qui fixe les normes internationales de la réglementation bancaire, y compris celles relatives à la cybersécurité. L'ACPR échange également avec le Conseil de stabilité financière (CSF), qui coordonne les autorités financières nationales et les organismes internationaux de normalisation et contrôle la mise en œuvre de normes clés, notamment celles relatives à la cybersécurité.

B. Le rôle central de la coordination internationale des crises

Au niveau international, le groupe d'experts du G7 sur la cybersécurité (CEG), dont la Banque de France, l'ACPR, l'AMF et la DGT sont membres, s'emploie à renforcer la stabilité financière mondiale grâce à des efforts coordonnés visant à atténuer les risques cyber. À ce titre, le CEG organise régulièrement des exercices transfrontaliers de gestion de crise cyber majeure, dont les plus récents se sont tenus en 2019 et 2024. Par ailleurs, au sein de cette enceinte, plusieurs groupes de travail sont dédiés à l'analyse des risques cyber et des menaces émergentes, notamment celles liées à l'intelligence artificielle et aux technologies quantiques. Le CEG a également pour vocation de produire des documents de référence, tels que les « Fundamental Elements », qui définissent les meilleures pratiques en matière de cybersécurité pour le secteur financier.

Dans son rapport publié en avril 2024 (CERS, 2024), auquel a contribué l'ACPR, le Comité européen du risque systémique (CERS) a analysé des pistes stratégiques contre le risque cyber. Ces pistes incluent tout d'abord l'amélioration de la gestion et du partage d'information. À ce titre, DORA prévoit que les autorités compétentes aient la possibilité de fournir aux entités financières leur ayant déclaré un incident majeur des commentaires pertinents et proportionnés ou des orientations de haut niveau ; que les autorités européennes de surveillance partagent sur base annuelle des informations anonymisées et agrégées sur les incidents majeurs reçus ; et que les entités financières partagent entre elles des informations sur la cyber menace, au sein de communautés de confiance.

Ensuite, le rapport du CERS préconise l'harmonisation des pratiques de gestion et de coordination des crises et l'implémentation de dispositifs de résolution en cas d'incident cyber. Le développement de protocoles de réponse nationaux et transfrontaliers permettrait en effet d'améliorer la capacité de réponse collective aux incidents cyber (CERS 2021 ; FMI 2020). Au niveau français, la Banque de France héberge le Secrétariat du Groupe de Place Robustesse (GPR), dont les principaux acteurs privés du secteur financier et des acteurs publics tels que ANSSI, l'ACPR, l'AMF ou encore la DGT, sont membres. Au fil de ses 20 années d'existence, le GPR a prouvé sa capacité à coordonner le secteur financier français en cas de crise opérationnelle majeure, notamment d'origine cyber et a développé une pratique régulière de gestion et d'exercice de crise[18]. Depuis 2023, l'ACPR s'est en parallèle dotée d'un protocole de crise cyber pour la gestion d'une crise sectorielle (banque et assurance). Ce protocole comprend des interfaces et des mécanismes de coordination avec le GPR et le protocole de gestion des crises cyber de la BCE. En outre, depuis l'entrée en application du règlement DORA, les trois autorités européennes de surveillance (l'ABE, l'EIOPA et l'ESMA) ont établi le cadre de coordination de l'Union européenne en matière d'incidents cyber systémiques (EU-SCICF), préconisé par le CERS (CERS,

[17] Guidance on cyber resilience for financial market infrastructures – orientation publiée en 2017 pour compléter les *Principles for market Infrastructures* (2012), publiés en 2012 pour poser les bases règlementaires applicables aux opérateurs d'infrastructures de marchés financiers.

[18] https://www.banque-france.fr/system/files/2025-02/20250211_CP_Rapport_GPR_vf.pdf

2021), qui vise à faciliter une réponse efficace du secteur financier à un incident cyber présentant un risque pour la stabilité financière, en renforçant la coordination entre les autorités financières et les autres organismes pertinents de l'Union européenne, ainsi qu'avec les principaux acteurs au niveau international. C'est la Banque de France qui représente les autorités financières françaises au sein de l'EU-SCICF.

C. Mieux identifier, quantifier et tester le risque cyber systémique

Parmi les autres axes de renforcement du cadre de cybersécurité figurent aussi l'identification des principales sources de risque cyber à l'échelle du système financier et l'analyse de leur impact potentiel sur la stabilité financière, à travers des outils tels que la cartographie des interconnexions financières et technologiques clés, que l'analyse des registres d'information DORA sur les contrats avec des prestataires de services informatiques facilitera ; l'amélioration de la quantification de l'impact potentiel des incidents cyber (FMI 2018 ; Healey *et al*. 2018), que les déclarations d'incidents majeurs obligatoires et le rapport de coûts et pertes agrégés DORA favoriseront ; ainsi que les tests de résistance, comme celui organisé par la Banque centrale européenne en juillet 2024 sur un périmètre de 109 banques européennes dont les résultats ont alimenté le processus de contrôle et d'évaluation prudentiel (BCE, 2024). La participation à des exercices de gestion de crise cyber, comme ceux que peuvent organiser le G7 (BCE, 2024) ou le GPR (Banque de France, 2025), est également conseillée, dans un souci d'anticipation et de coopération avec les autorités.

D. Adapter les outils macroprudentiels à la spécificité du risque cyber

La vitesse et l'échelle de propagation du risque cyber justifient le développement d'une réflexion sur l'adaptation des instruments macroprudentiels à la gestion d'un incident cyber de grande ampleur (CERS ; Banque d'Espagne, *FSR*, 2021). L'ACPR et la BdF, en tant que membre du CERS et de l'ESCG (*European systemic cyber expert group*), ont ainsi participé à une réflexion sur l'adaptation des outils existants à la gestion d'un incident cyber de grande ampleur. Le CERS a par la suite publié des rapports sur la mise en place d'outils plus ciblés comme, parmi d'autres outils macroprudentiels et opérationnels déjà évoqués ci-dessus (CERS, 2023 et CERS, 2024), des exercices basés sur des scénarios de crise cyber (CyRST) (CERS, *Advancing macroprudential tools for cyber resilience*, 2023).

E. Anticiper les risques technologiques émergents, l'exemple de l'informatique quantique

Dans l'esprit de DORA, le secteur financier doit également adopter une posture proactive sur les risques émergents. À cette fin, l'informatique quantique est identifiée comme un risque majeur pour la stabilité financière nécessitant une mobilisation des autorités et des entités financières. S'il n'y a pas encore un réel consensus sur l'horizon d'apparition des circuits quantiques spécifiques pour l'algorithme de Shor (« cryptographically relevant quantum computers » ou CRQC), le risque appelle d'ores et déjà une vigilance, notamment sur les attaques de type « *harvest now, decrypt later* ». Des travaux visant à mettre en œuvre la cryptographie « post-quantique » sont déjà engagés par les autorités financières (ex : projet LEAP du BISIH impliquant la BdF et la BBk [19], *Next-generation Commercial Cryptographic Algorithms Program* lancé par la Chine en fév. 2025 [20]), notamment sur la base de la campagne de standardisation post-quantique d'algorithmes classiques résistants aux attaques quantiques de la *National Institute of Standards and Technology* [21].

Dans le cadre de la phase 2 du projet LEAP, le BISIH a organisé en février 2025 une conférence sur le sujet[22] afin d'engager une discussion entre autorités sur la nécessaire préparation ordonnée des

[19] Project Leap: quantum-proofing the financial system (bis.org)
[20] Institute of Commercial Cryptography Standards
[21] Post-Quantum Cryptography | CSRC (nist.gov)
[22] Quantum-readiness for central banks and supervisors

communautés financières (BIS, 2025). L'enjeu est relativement fort dans la mesure où il s'agit de réfléchir sur les premières actions à entreprendre, qui relèvent de considérations à la fois techniques, organisationnelles et stratégiques (e.g. sensibilisation, inventaire cryptographique, cartographie des dépendances, conception d'une stratégie de migration, adoption d'une posture « crypto-agile », transition hybride, etc.).

Dans une démarche d'anticipation du « Q-day », les autorités compétentes commencent également à communiquer des objectifs de migration. Le NIS Cooperation Group, sponsorisé par la Commission européenne, a publié en juin 2025 une première feuille de route coordonnée pour la migration vers la cryptographie post-quantique, fixant 2030 comme échéance pour la sécurisation des infrastructures critiques des États membres. Le G7 CEG a publié une feuille de route visant à donner un positionnement public sur les risques et objectifs de transition. La principale recommandation sera de migrer globalement d'ici 2035, et pour les systèmes les plus critiques d'ici 2030/32. Lors des Assises de la cybersécurité en octobre 2025, l'ANSSI a annoncé qu'à partir de 2027, elle cessera de qualifier tout produit de sécurité ne disposant pas de cryptographie post-quantique (PQC). À compter de 2030, elle recommande que toutes les solutions acquises soient résistantes à l'informatique quantique, renforçant ainsi ses recommandations actuelles.

Bibliographie

- Ahaus, K., Asensio, C., Bouveret, A., & Harris, R. (2021). *Cloud outsourcing and financial stability risks* (in *ESMA Report on Trends, Risks and Vulnerabilities*). ESMA.
- Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). *The drivers of cyber risk*. BIS.
- AMRAE. (2025). *LUCY : Lumière sur la CYberassurance - Édition 2025*. AMRAE.
- ANSSI. (2021). *État de la menace rançongiciel à l'encontre des entreprises et des institutions*. ANSSI.
- ANSSI. (2024). *Panorama de la cybermenace 2024*. ANSSI.
- Lo, A. W., & Singh, M. (2023). From ELIZA to ChatGPT: The Evolution of Natural Language Processing and Financial Applications. *Journal of Portfolio Management*, *49*(7).
- Auer, R. A., Dupont, A., Gambacorta, L., Park, J. S., Takahashi, K., & Valko, A. (2024). *Quantum computing and the financial system: opportunities and risks*. BIS, Bank for International Settlements.
- Banque de France. (2023, déc.). *Évaluation des risques du système financier français*. BdF.
- Banque de France. (2025). *Rapport sur la stabilité financière*. BdF.
- Banque de France. (2025). *Le Groupe de Place Robustesse teste la résilience des paiements par carte et mobile face à une crise cyber d'envergure* (communiqué). BdF.
- Banque centrale européenne (BCE). (2024). *La BCE conclut son test de résistance sur la cyberrésilience*. BCE.
- Banque centrale européenne (BCE). (2025, 27 mars). *Macroprudential Bulletin* (numéro consacré au risque cyber). BCE.
- Bank of England. (2018, Q4). *Cyber risk in the financial sector* (*Quarterly Bulletin*). BoE.
- Bouveret, A. (2018). *Cyber risk for the financial sector: a framework for quantitative assessment* (IMF Working Paper). FMI.
- Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, *31*(3), 415-434.
- CERS / ESRB. (2020). *Systemic cyber risk*.
- CERS / ESRB. (2021). *Recommendation on a pan-EU systemic cyber incident coordination framework (EU-SCICF)*.
- CERS / ESRB. (2023). *Advancing macroprudential tools for cyber resilience*.
- CERS / ESRB. (2024). *Advancing macroprudential tools for cyber resilience - Operational policy tools*.
- Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
- Citalid. (2024). *Banque & finance - Rapport sectoriel : État de la menace 2024*. Citalid.
- Cloud Security / Lloyd's. (2018). *Cloud Down: The impacts on the US economy*. Lloyd's & partners.
- Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva papers on risk and insurance. Issues and practice*, *47*(3), 698.

- Danielsson, J., et al. (2016). *The financial risk from cyber attacks*. LSE Systemic Risk Centre Paper.
- *Deodoro, J, M Gorbanyov, M Malaika and TS Sedik (2021): "Quantum computing and the financial system: spooky action at a distance?", IMF Working Papers, no 2021/071, March.* Deloitte. (s.d.). *Quantum threat to cryptoassets* (2 études sur Bitcoin & Ether). Deloitte.
- Doerr, S., Gambacorta, L., Leach, T., Legros, B., & Whyte, D. (2022). *Cyber risk in central banking*. Bank for International Settlements, Monetary and Economic Department.
- Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J. W., & Winkelman, Z. (2018). Estimating the global cost of cyber risk. *Research Reports RR-2299-WFHF, Rand Corporation*.
- Duffie, D., & Younger, W. (2019). *Cyber runs*. Working paper.
- ECB / G7 CEG. (2024). *G7 Cyber Expert Group conducts cross-border coordination exercise in the financial sector*. BCE.
- Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events?. *European Journal of Operational Research*, *272*(3), 1109-1119.
- ENISA. (2025, fév.). *Threat Landscape: Finance Sector*. ENISA.
- Erola, A., Agrafiotis, I., Nurse, J. R., Axon, L., Goldsmith, M., & Creese, S. (2022). A system to calculate Cyber Value-at-Risk. *Computers & Security*, *113*, 102545. Article.
- European Commission / EU legislators. (2022). *Règlement (UE) 2022/2554 (DORA)*. JOUE.
- FSB (Financial Stability Board). (2019). *Third-party dependencies in cloud services*. FSB.
- Franco, M. F., Künzler, F., Von der Assen, J., Feng, C., & Stiller, B. (2024). RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports. *Computers & Security*, *139*, 103737.
- Global Risk Institute. (2024). *Quantum Threat Timeline Report 2024*. GRI.
- Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 212-219).
- Healey, J., et al. (2018). *The future of financial stability and cyber risk*. Atlantic Council.
- IIF (Institute of International Finance). (2017). *Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system*. IIF.
- Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). *Cyber risk, market failures, and financial stability*. International Monetary Fund.
- FMI. (2020). *Cyber Risk and Financial Stability: It's a Small World After All* (Staff Discussion Note). FMI.
- FMI. (2024, avril). *Global Financial Stability Report* (chapitre cyber). FMI.
- FMI. (2024). *The Last Mile: financial vulnerabilities and risks*. FMI.
- IAIS (International Association of Insurance Supervisors). (2020). *Cyber Risk Underwriting: Identified Challenges and Supervisory Considerations for Sustainable Market Development*. IAIS.
- IAIS. (2025). *Global Insurance Market Report (GIMAR) 2025*. IAIS.
- Jamilov, R., Rey, H., & Tahoun, A. (2023). *The anatomy of cyber risk* (No. w28906). National Bureau of Economic Research.

- Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749.
- Kyiv Post. (2024). *Ukraine Hacks ATMs Across Russia in Ongoing Massive Cyberattack*. *Kyiv Post*.
- Kshetri, N. (2019). The economics of cyber-insurance. *IT Professional*, *20*(6), 9-14. Marsh. (2025). *The evolution of cyber claims in Europe (Continental)*. Marsh.
- Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*. McAfee. (2013). *Dissecting Operation Troy: Cyberespionage in South Korea*. McAfee.
- Microsoft. (2022). *Defending Ukraine: Early Lessons from the Cyber War*. Microsoft.
- Moody's. (2019). *Rating action on Equifax following 2017 breach* (credit outlook change). Moody's.
- Munich Re. (2024). *Global Cyber Risk and Insurance Survey 2024*. Munich Re.
- Natalucci, F., Qureshi, M. S., & Suntheim, F. (2024, avril). *L'intensification des cybermenaces suscite de grandes inquiétudes pour la stabilité financière*. Blog du FMI.
- Ntoutsi, E., Fafalios, P., Gadiraju, U., Iosifidis, V., Nejdl, W., Vidal, M. E., ... & Staab, S. (2020). Bias in data-driven artificial intelligence systems—An introductory survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(3), e1356.
- OFR (Office of Financial Research). (2017). *Cybersecurity and Financial Stability: Risks and Resilience*. OFR.
- Rao, S., Mahto, D., Yadav, D. K., & Khan, D. A. (2017). The AES-256 cryptosystem resists quantum attacks. *Int. J. Adv. Res. Comput. Sci*, *8*(3), 404-408.
- Radanliev, P. (2024). Artificial intelligence and quantum cryptography. *Journal of Analytical Science and Technology*, *15*(1), 4. S&P Global Ratings. (2020-2021). *Cyber Risk In A New Era* (series). S&P Global.
- Salzberger, A. (2025). The optimistic bias in cyber risk perception of German enterprises: do organizational and personal moderators matter?. *Organizational Cybersecurity Journal: Practice, Process and People*.
- Shabad, V. (2025). Flow-Constrained Risk Management for Operational Technology Security: A Multi-Criteria Framework for Critical Infrastructure. *Available at SSRN 5389934*.
- Shabsigh, M. G., & Boukherouaa, E. B. (2023). *Generative artificial intelligence in finance: Risk considerations*. International Monetary Fund.Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134).
- Ieee. Solaimani, S., & Long, P. (2025). Beyond the black box: operationalising explicability in artificial intelligence for financial institutions. *International Journal of Business Information Systems*, *49*(5), 1-38.
- Trend Micro. (2023). *Inside the Halls of a Cybercrime Business*. Trend Micro.
- World Economic Forum. (2015). *Cyber Value-at-Risk*. WEF.
- World Economic Forum. (2016). *Understanding Systemic Cyber Risk*. WEF.
- World Economic Forum. (2025). *Global Risks Report 2025*; *Cybercrime cost estimate (USD 10.5tn by 2025)*. WEF.