



UNIVERSITÉ DU QUÉBEC EN OUTAOUAIS

DÉPARTEMENT DES SCIENCES ADMINISTRATIVES

L'impact des cyberattaques sur la réputation des banques

Mémoire

Maîtrise en économie financière

Janvier 2025

Auteur : Hind Derqaoui

Directeur de recherche: Djerry Charli Tandja Mbianda, Ph.D

Table des matières

REMERCIEMENTS.....	4
RÉSUMÉ.....	5
LISTE DES TABLEAUX	6
1. INTRODUCTION.....	7
2. REVUE DE LITTÉRATURE	10
2.1. Le panorama des cyber risques et les types de cyberattaques	10
2.2. Les mécanismes de la réputation	13
2.3. L'impact des cyber-attaques sur la réputation des banques.....	14
2.4. Mécanismes Financiers des Prêts Syndiqués	21
3. HYPOTHÈSES ET PRÉDICTIONS EMPIRIQUES	28
3.1. Hypothèse 1	28
3.2. Hypothèse 2	Erreur! Signet non défini.
3.3. Hypothèse 3.....	28
4. BASE DE DONNÉES ET DESCRIPTION DES VARIABLES	30
4.1. Base de données	30
4.2. Analyse descriptive	30
4.2.1. Description des variables	31
4.2.2 Statistique descriptive	33
4.3. Matrice de corrélation	35
5. MÉTHODOLOGIE ÉCONOMÉTRIQUE.....	36
5.1. Modèle de Moindres Carrés Ordinaires.....	36
5.2. Tests de Diagnostics.....	38
5.2.1. Test de Breusch-Pagan pour l'Hétéroscédasticité	38

5.2.2. Test de Multi colinéarité à l'aide du VIF (Variance Inflation Factor)	38
6. DESCRIPTION DU MODÈLE DE RÉGRESSION LINÉAIRE MULTIPLE AVEC DES DONNÉES DE PANEL ET DES EFFETS FIXES	39
6.1. Utilisation des Effets Fixes pour `année` et `L'identifiant de l'emprunteur`	40
6.2. Prise en Compte des Facteurs Temporels et des Caractéristiques des Emprunteurs.....	40
7. RÉSULTATS DU MODÈLE À EFFETS FIXES	41
7.1. Analyse des Résultats de la Régression : Effets des cyberattaques sur les montants des prêts syndiqués	41
7.2. Analyse des Résultats de la Régression : Effets des cyberattaques sur la structure des prêts syndiqués	42
7.3. Analyse des Résultats de la Régression : Effets des cyberattaques sur le ratio de fonds propres des prêteurs .	43
8. CONCLUSION	45
9. BIBLIOGRAPHIE	46
10. TABLEAUX	50

Remerciements

Je souhaite exprimer ma profonde gratitude à toutes les personnes qui ont contribué à la réalisation de ce mémoire.

En premier lieu, je rends un hommage particulier à mon père, qui nous a quittés pour un monde meilleur, et dont la tendresse, la dévotion et l'incommensurable ont été des piliers inébranlables tout au long de ce parcours. Son souvenir continuera à illuminer chaque étape de ma vie, y compris celle-ci.

À ma famille, qui a toujours été mon refuge et ma source de force, je vous suis infiniment reconnaissante pour votre amour inconditionnel, votre soutien indéfectible et vos encouragements constants. Chaque succès que j'ai réalisé est le fruit de votre amour et de votre soutien infaillible.

Mon directeur de recherche, le professeur Djerry Charli Tandja Mbianda, mérite également une reconnaissance spéciale. Votre expertise, votre guidance et votre patience infinie ont été essentielles pour mener ce projet à bien. Vos conseils éclairés ont enrichi mon travail d'une manière inestimable.

En outre, je tiens à exprimer ma gratitude envers l'Université du Québec en Outaouais pour son soutien académique tout au long de ce projet de recherche. L'accès aux ressources et l'environnement académique de l'université ont été essentiels à la réalisation de ce travail.

Enfin, je souhaite exprimer ma reconnaissance envers toutes les personnes qui ont contribué de près ou de loin à ce mémoire. Ce travail est le résultat d'un effort collectif et de nombreuses heures de dévouement. Je suis reconnaissante envers chacun d'entre vous pour avoir rendu cela possible.

Merci du fond du cœur...

Résumé

Ce mémoire examine l'impact des cyberattaques sur les banques, en se concentrant sur les prêts syndiqués et la réputation institutionnelle. À travers une revue de la littérature sur les cyber-risques, les mécanismes de réputation et les prêts syndiqués, cette recherche explore trois hypothèses : (1) les cyberattaques réduisent les montants des prêts syndiqués, (2) elles modifient leur structure en augmentant la concentration des prêteurs principaux et en diminuant la diversité des participants, et (3) elles incitent les prêteurs à renforcer leurs ratios de fonds propres face à une perception accrue des risques.

Les cyberattaques affectent la réputation des banques, mesurée par une hausse du ratio de fonds propres de catégorie 1 (Tier One), un indicateur de stabilité financière qui revêt aussi une dimension réputationnelle. Dans un secteur où la confiance est cruciale, cette augmentation signale une résilience face aux risques accrus, rassurant ainsi les investisseurs et les parties prenantes.

En utilisant des modèles économétriques à effets fixes appliqués à un échantillon de 50 banques américaines entre 2001 et 2021 (65 863 observations), les résultats confirment que les cyberattaques entraînent une réduction des montants des prêts syndiqués, une augmentation de la concentration des prêteurs principaux dans la structure des syndicats avec une diminution du nombre de participants, et une hausse des exigences en capital des prêteurs. Ces perturbations traduisent une perte de réputation des banques victimes, affectant leur capacité à attirer des participants diversifiés et à maintenir leur solidité perçue.

Cette étude apporte une perspective empirique sur les effets des cyberattaques sur la réputation bancaire et la dynamique des prêts syndiqués, tout en soulignant l'importance des mesures de cybersécurité pour protéger à la fois la solidité financière et l'image institutionnelle des banques.

Liste des tableaux

Tableau1: Statistiques descriptives

Tableau2: Coefficients de corrélation des variables

Tableau 3: Coefficients de corrélation des variables (suite)

Tableau 4: Coefficients de corrélation des variables (suite)

Tableau 5: Coefficients de corrélation des variables (suite)

Tableau6: Test de Breusch-Pagan

Tableau7: Test de multicolinéarité

Tableau 8: Impact des cyberattaques sur les montants des prêts

Tableau 9 : Impact des cyberattaques sur la structure des prêts syndiqués

Tableau 10 : Impact des cyberattaques sur la réputation des emprunteurs via le ratio de fonds propres de première catégorie

1. Introduction

Dans un environnement financier de plus en plus interconnecté et numérisé, la réputation des institutions bancaires s'affirme comme un atout stratégique fondamental (Linsley et Sharif, 2006). Elle est toutefois vulnérable aux cyberattaques, qui représentent une menace majeure tant pour les infrastructures critiques que pour la confiance des clients et des investisseurs. Ces attaques ont évolué en termes de portée et de sophistication, ciblant non seulement les données sensibles, mais aussi la perception que le public a des institutions financières, ce qui peut entraîner une dégradation de la réputation bancaire (Kamiya et al., 2021).

La réputation bancaire, définie comme l'ensemble des perceptions des parties prenantes vis-à-vis d'une banque, joue un rôle crucial dans la fidélisation des clients, l'accès au capital et la gestion des risques. Dans un secteur où la confiance constitue une pierre angulaire, la capacité des banques à se prémunir contre les cybermenaces devient une priorité stratégique. En effet, les études empiriques récentes soulignent l'impact délétère des cyberattaques sur la confiance des investisseurs et des clients, ainsi que sur la performance des actions et obligations (Bianchi et Tosun, 2018 ; Amir et al., 2019).

Les institutions bancaires, en raison de leur position centrale dans l'intermédiation financière, sont particulièrement exposées aux cybermenaces, qu'il s'agisse de vol de données, de ransomwares ou d'attaques ciblées sur les systèmes d'information. Ces événements peuvent entraîner des coûts financiers directs, mais aussi des pertes intangibles comme la réputation, ce qui peut avoir un effet domino sur d'autres segments de l'activité bancaire, y compris le marché des prêts syndiqués (Chen et al., 2019). Ce dernier, en tant qu'outil essentiel pour diversifier les risques et mobiliser des capitaux, est d'autant plus vulnérable aux perturbations induites par les cyberattaques (Bouveret, 2018).

Dans cette étude, nous analysons l'impact des cyberattaques sur la réputation des banques, ainsi que sur leurs répercussions spécifiques sur le marché des prêts syndiqués. Plus précisément, nous analyserons comment ces attaques influencent les perceptions des parties prenantes et les montants des prêts syndiqués, et leur structure. Ce lien entre la cybersécurité et les marchés financiers a déjà fait l'objet d'études importantes, mais reste peu exploré dans le contexte spécifique des prêts syndiqués (Eisenbach et al., 2022). Notre objectif est donc double : d'une part, évaluer les effets des cyberattaques sur la réputation des banques ; d'autre part, examiner leur impact sur les mécanismes financiers liés aux prêts syndiqués, en particulier le montant et la structure des prêts.

La littérature existante met en évidence la cybersécurité comme un enjeu crucial pour le secteur bancaire, notamment en ce qui concerne les risques opérationnels et réputationnels. Par exemple, Barakat et al. (2019) soulignent l'importance du discours médiatique dans l'amplification des risques réputationnels post-cyberattaque. De son côté, Kamiya et al. (2021) analysent les effets des cyberattaques sur la performance des entreprises, y compris une baisse significative de la capitalisation boursière. Bouveret

(2018) propose des outils pour quantifier les risques cybernétiques dans le secteur financier, et Grody (2020) explore des stratégies de gouvernance visant à les réduire.

En nous appuyant sur cette base théorique, nous tentons de relier deux dimensions clés : la réputation et les montants des prêts syndiqués. Les études précédentes, notamment celles de Berg et al. (2017) et Sufi (2007), se sont concentrées sur les déterminants des prêts syndiqués et les asymétries d'information qui influencent leur tarification. Cependant, peu de recherches ont exploré l'impact des cyberattaques sur ce marché spécifique. En positionnant notre étude dans cette niche, nous visons à combler ce vide en fournissant des insights nouveaux sur l'importance de la gestion des cyberrisques dans l'optimisation des montants de financement.

Pour quantifier les effets des cyberattaques, nous utilisons un modèle de régression linéaire multiple inspiré des travaux de Gopalan et al. (2011) et Chu et al. (2019). Ce modèle permet d'évaluer l'impact des cyberattaques sur les montants des prêts, en tenant compte des caractéristiques des emprunteurs, des prêteurs, ainsi que des modalités des prêts. Nous intégrons des variables indicatrices pour les cyberattaques et contrôlons des variables financières essentielles, telles que la taille des prêteurs, leur ratio de fonds propres, leur ROA, et la valeur de marché des emprunteurs. L'analyse économétrique est réalisée via le logiciel RStudio, ce qui garantit la rigueur de nos tests d'hypothèses.

L'échantillon utilisé provient de Dealscan, comprenant 65 863 observations de transactions de prêts syndiqués accordés par 50 banques américaines entre 2001 et 2021. Les résultats préliminaires indiquent que la variable indicatrice des cyberattaques présente un coefficient de -0,1071 avec une significativité élevée ($p < 0,001$), suggérant que ces attaques sont associées à une réduction des montants des prêts. En outre, une diminution du nombre de participants aux syndications est observée (coefficient estimé de -0,364, $p < 0,001$), ce qui témoigne d'une perturbation significative de la structure des prêts suite aux cyberattaques.

En complément, nous développons deux modèles pour examiner de manière approfondie les impacts des cyberattaques sur le marché des prêts syndiqués. Le premier modèle analyse l'impact des cyberattaques sur la participation des banques aux syndications, un facteur pouvant influencer la liquidité et la concurrence sur le marché. Le second modèle se concentre sur le ratio de fonds propres des prêteurs, afin de mesurer comment les cyberattaques peuvent affecter la structure de capital des institutions financières.

Ces analyses permettront de mieux comprendre comment les cyberattaques modifient les dynamiques de financement et les décisions de prêt sur le marché des prêts syndiqués, en dévoilant des effets qui ne seraient pas évidents dans une analyse simplifiée.

Cette étude enrichira la littérature en clarifiant les interactions entre cyberattaques, réputation bancaire et prêts syndiqués. En apportant des preuves empiriques actuelles, elle aidera les professionnels du secteur bancaire à mieux anticiper les risques liés à la cybersécurité et à mettre en œuvre des stratégies pour protéger leur réputation dans un environnement numérique de plus en plus complexe.

La suite de ce mémoire est structurée comme suit : la section 2 présente la revue de littérature, la section 3 les hypothèses et prédictions empiriques, suivies de la section 4 sur la base de données et les variables. La section 5 détaille la méthodologie économétrique, la section 6 le modèle à effets fixes, la section 7 les résultats, et la section 8 conclut l'étude, avec une bibliographie complète en section 9 et des annexes en section 10.

2. Revue de littérature

Les cyberattaques visant les institutions financières, en particulier les banques, ont suscité des inquiétudes ces dernières années en raison de leur capacité à ébranler la confiance dans le secteur bancaire. La présente analyse de littérature vise à étudier l'impact des cyberattaques sur la réputation des banques en examinant les études et les points de vue pertinents provenant de sources universitaires et de l'industrie. Nous synthétisons la littérature sur quatre principaux thèmes : le panorama des cyber risques et les types de cyberattaques ; les mécanismes de la réputation ; l'impact des cyberattaques sur la réputation des banques et Mécanismes financiers des prêts syndiqués.

2.1. Le panorama des cyber risques et les types de cyberattaques

Le Cyber Lexicon du Financial Stability Board (2019) constitue une ressource clé pour comprendre le risque cybernétique tel qu'il est perçu dans le secteur financier. Il définit le risque cybernétique comme la combinaison de la probabilité d'occurrence d'incidents cybernétiques et de leur impact potentiel sur les institutions financières ainsi que sur le système financier dans son ensemble.

Le lexique met en avant la capacité des cyberincidents à perturber les services financiers essentiels, à éroder la confiance des parties prenantes et à provoquer des pertes financières substantielles.

La définition de Cebula et Young (2010), largement adoptée dans les cercles académiques et au sein des normes internationales, positionne le risque cybernétique comme une forme de risque opérationnel. Ce risque peut compromettre la confidentialité, l'intégrité ou la disponibilité des données ou des systèmes d'information.

L'étude d'Eisenbach et al. (2022) met en lumière l'importance de la taxonomie des cyber-événements pour comprendre les répercussions économiques des cyberattaques sur les systèmes financiers. En se basant sur le Federal Information Security Management Act, les auteurs identifient trois catégories principales de cyber-événements : confidentialité, disponibilité et intégrité. Les auteurs mettent en lumière les implications économiques spécifiques de chaque catégorie sur les institutions financières. Les événements compromettant la confidentialité des données peuvent entraîner des pertes directes, des responsabilités légales et des coûts de réparation de réputation, tandis que ceux affectant la disponibilité peuvent immobiliser les capitaux et les liquidités, perturbant ainsi les opérations essentielles. De même, les événements altérant l'intégrité des données peuvent engendrer des coûts de restauration, des frais juridiques et des répercussions sur la capacité des banques à mener leurs activités principales. En définissant et en classifiant ces événements, les institutions financières peuvent mieux évaluer les risques et mettre en œuvre des mesures de sécurité adaptées pour atténuer les impacts potentiels sur leurs activités et leurs clients, renforçant ainsi leur résilience face aux cybermenaces croissantes.

Bouveret (2018) souligne que le secteur financier est l'un des secteurs les plus ciblés en raison de sa dépendance à l'égard de l'information et de son rôle central dans le processus d'intermédiation du crédit. Les institutions financières sont très exposées au risque cybernétique, les vulnérabilités découlant de leurs exigences réglementaires en matière de risque opérationnel, ce qui les rend plus susceptibles de collecter des données sur les incidents cybernétiques que les entreprises non financières. L'étude met en lumière le risque cybernétique pour les institutions financières en utilisant des données accessibles au public et des ensembles de données commerciales, dans le but de fournir des informations aux régulateurs, aux superviseurs et aux institutions financières.

En outre, l'étude indique que les économies avancées sont les principales cibles des cyberattaques, les banques étant les victimes de nombreuses attaques. Les banques centrales des économies avancées et des marchés émergents ont également été victimes de cyberattaques, allant de la violation de données à l'interruption des activités et à la fraude. L'étude souligne que les pertes directes dues aux cyberattaques ne sont pas nécessairement liées à la taille de l'institution financière ciblée, certaines des pertes les plus importantes étant enregistrées dans des institutions plus petites, peut-être en raison d'investissements moindres dans la sécurité informatique.

Dans l'ensemble, l'auteur souligne que le secteur financier est fortement ciblé par les cyberattaques et qu'il est important de comprendre et de gérer efficacement les cyber risques au sein des institutions financières afin d'atténuer les menaces et les vulnérabilités potentielles.

Aldasoro et al. (2020) utilisent une base de données unique de plus de 100 000 cyber événements dans tous les secteurs pour documenter les caractéristiques des cyber incidents. L'étude montre que les coûts des cybers incidents sont plus élevés pour les grandes entreprises et pour les incidents qui touchent plusieurs organisations à la fois. Il est intéressant de noter que le secteur financier subit un plus grand nombre de cyberattaques, mais que ses coûts sont en moyenne moins élevés grâce à ses investissements plus importants dans la sécurité informatique. L'utilisation de services en nuage est associée à des coûts moins élevés, en particulier lorsque les cybers incidents sont relativement limités. Toutefois, à mesure que les fournisseurs de services en nuage acquièrent une importance systémique, la dépendance à l'égard des services en nuage est susceptible d'accroître les risques de cyberattaques. Les activités liées aux cryptomonnaies, qui sont largement non réglementées, sont particulièrement vulnérables aux cyberattaques.

Dans leur étude, Firoozi et al (2023) se sont penché sur les divulgations en matière de cybersécurité effectuées par les 48 plus grandes banques canadiennes et américaines entre 2014 et 2020. Le secteur bancaire a été une cible majeure des cyberattaques en raison des données critiques qu'il contient. L'étude montre qu'après les directives de la CSA au Canada, la moyenne des banques divulguant l'impact d'une cyberattaque sur leurs clients et leur réputation est passée de 0,63 à 0,84. Aux États-Unis, après les directives de la SEC, cette moyenne est passée de 0,69 à 0,83. Par ailleurs, les banques américaines ont présenté des taux de divulgation significativement plus élevés au cours de la même période.

Kopp et al. (2017) soulignent que la quantification de l'impact des cyberattaques rencontre des obstacles majeurs, notamment en raison de la pénurie de données fiables et de l'absence de cadres normalisés pour estimer les pertes. Les difficultés proviennent du retard dans la déclaration des cyber incidents et de la sous-déclaration des entreprises touchées. Les cadres réglementaires et les approches prudentielles jouent un rôle essentiel dans la gestion des cyber risques au sein des institutions financières, mais ils sont confrontés à des asymétries d'information et à des inefficacités.

Eisenbach, T. M., Kovner, A., & Lee, M. J (2022) Soutiennent que la difficulté d'obtenir des sources de données pour l'analyse pré-mortem du risque cybernétique et du système financier américain tient à l'absence de consensus universel sur la taxonomie et la définition des cyber-événements, ainsi qu'à la rareté des données complètes sur la fréquence et la nature des cyber-attaques. Les cyberattaques sont des événements complexes et rares, ce qui les rend difficiles à prévoir et à analyser efficacement. L'étude souligne qu'il n'y a pas d'accord universel sur la manière de classer et de définir les cyber-attaques, ce qui complique l'évaluation des risques qu'elles posent. En outre, la disponibilité limitée de données détaillées sur les cyberattaques dans le secteur financier pose un problème pour quantifier avec précision l'impact potentiel de ces événements sur le système financier.

Le document reconnaît que les cyberattaques peuvent être conçues pour causer un maximum de perturbations, les attaquants pouvant posséder une connaissance détaillée des institutions ciblées et du système de paiement, ce qui entraîne des niveaux variables de risque systémique. En outre, l'étude souligne que la recherche traditionnelle sur l'interconnexion peut ne pas saisir toutes les vulnérabilités présentées par les fournisseurs de services tiers, soulignant l'importance de comprendre les liens opérationnels au-delà de la gestion conventionnelle du risque de contrepartie. Malgré ces difficultés, l'analyse intègre diverses sources de données, notamment les données de Fedwire sur les paiements de gros entre institutions financières aux États-Unis, les données réglementaires sur les listes de clients des principaux fournisseurs de services, et des exercices de simulation de crise inversée pour explorer les vulnérabilités et les impacts systémiques potentiels des cyberattaques sur le système financier.

L'étude menée par Antoine Bouveret (2018) met en lumière plusieurs défis cruciaux dans l'évaluation du risque cybernétique pour les institutions financières. Parmi ces défis figurent la rareté des données disponibles, la présence d'ensembles de données incomplets, ainsi que les problèmes de comparabilité entre différentes sources d'informations. La diversité des niveaux de menace et de vulnérabilité rencontrés ajoute également à la complexité de cette évaluation.

Ces limitations compliquent la tâche d'évaluer et de gérer les risques cybernétiques dans le secteur financier. En effet, la rareté et l'incomplétude des données empêchent d'établir une vision claire de la situation. De plus, la diversité des sources et des types de menaces rend la comparabilité des données difficile, limitant ainsi la capacité des institutions financières à prendre des décisions éclairées. Pour surmonter ces défis, il est nécessaire d'améliorer la collecte de données et de standardiser les processus afin de faciliter l'analyse et la gestion des risques.

Enfin, l'élaboration et la mise en œuvre de stratégies de gestion des risques efficaces sont indispensables pour atténuer l'impact des cybermenaces sur les institutions financières. Cela implique non seulement une meilleure compréhension des menaces et des vulnérabilités spécifiques, mais aussi la mise en place de mesures proactives pour prévenir les attaques et en limiter les conséquences potentielles. Cette étude souligne ainsi l'urgence d'améliorer la collecte des données, la normalisation et les stratégies de gestion des risques afin de renforcer la résilience des institutions financières face aux cybermenaces croissantes.

Dans son étude, Antoine Bouveret (2018) propose une perspective étendue du risque cybernétique, allant au-delà des seules attaques délibérées pour inclure également les conséquences néfastes découlant de perturbations ou d'une mauvaise utilisation des systèmes et infrastructures technologiques. Cette approche holistique englobe non seulement les incidents résultant d'actions malveillantes, mais aussi ceux causés par des erreurs humaines, des défaillances techniques ou des événements extérieurs.

Bouveret reconnaît que cette menace est complexe et en constante évolution, influencée par divers facteurs. D'une part, les changements rapides dans le domaine technologique introduisent continuellement de nouvelles vulnérabilités, car de nouveaux systèmes et logiciels sont mis en service avant que leurs failles potentielles ne soient entièrement comprises ou corrigées. D'autre part, l'évolution des capacités des attaquants, alimentée par l'émergence de nouvelles techniques et outils, accroît la sophistication et la diversité des menaces.

En outre, l'interconnectivité croissante des systèmes financiers, due à la dépendance accrue vis-à-vis des réseaux informatiques et des technologies de communication, amplifie les risques. Elle expose davantage les institutions financières aux attaques et étend les répercussions potentielles des incidents cybernétiques au-delà de leurs frontières traditionnelles. Il devient donc crucial pour ces institutions de prendre en compte ces multiples dimensions du risque cybernétique dans leurs stratégies de gestion des risques, en mettant l'accent sur la prévention, la détection précoce et la réponse rapide pour améliorer leur résilience face à cette menace évolutive.

2.2. Les mécanismes de la réputation

La réputation est un actif immatériel essentiel pour les banques, car elle influence la confiance des clients, la confiance des investisseurs et la perception des autorités de réglementation. Une gestion efficace de la réputation implique le maintien de la crédibilité, de la fiabilité et de la fiabilité aux yeux des parties prenantes.

Le premier article de Nadine Gatzert en 2015, explore la relation entre la réputation des entreprises et leur performance financière. L'auteur met en évidence l'importance croissante de la réputation des entreprises dans le contexte actuel, en particulier face aux événements dommageables pour la réputation tels que les crises médiatiques. L'article

souligne l'importance d'une gestion proactive du risque de réputation pour atténuer les effets négatifs sur la performance financière des entreprises.

Le deuxième article publié par Ahmed Barakat et al. en 2019, se concentre sur les effets de la tonalité médiatique sur le risque opérationnel et la réputation des institutions financières. Les auteurs mettent en évidence le rôle critique des annonces de risques opérationnels dans la création de problèmes de gouvernance d'entreprise et de faibles mécanismes de contrôle interne. Ils montrent comment les tonalités médiatiques négatives et litigieuses peuvent avoir des effets néfastes sur la réputation des institutions financières, soulignant ainsi l'importance d'une gestion proactive du risque de réputation dans un environnement médiatique en évolution rapide.

Le troisième article de Simon Ashby et Ahmed Barakat datant de 2021 examine les recherches antérieures sur le risque de réputation dans les institutions financières et le cadre réglementaire qui les entoure. Les auteurs soulignent l'importance de la réputation des institutions financières comme avantage concurrentiel, tout en mettant en évidence les défis liés à la gestion du risque de réputation dans un contexte réglementaire.

Enfin, l'article publié par Franco Fiordelisi, Maria-Gaia Soana et Paola Schwizer, en mai 2013 dans le *Journal of Banking & Finance*, étudie empiriquement les facteurs influençant le risque de réputation dans le secteur bancaire à la suite de pertes opérationnelles. Les auteurs identifient une lacune dans la littérature concernant la compréhension du risque de réputation dans les services financiers et visent à combler cette lacune en analysant un grand échantillon de pertes opérationnelles subies par des banques cotées en Europe et aux États-Unis entre 2003 et 2008.

Leurs résultats révèlent que les pertes opérationnelles ont un effet négatif significatif sur la réputation des banques. En particulier, elles constatent une augmentation des spreads de taux d'intérêt, ce qui indique que les banques doivent payer davantage pour emprunter sur les marchés financiers en raison de la détérioration de leur image. De plus, l'analyse montre une diminution des valeurs boursières des banques touchées, suggérant que les investisseurs intègrent le risque de réputation dans leurs évaluations. Les auteurs soulignent également que la manière dont les banques réagissent aux pertes, notamment à travers la communication avec les parties prenantes, influence fortement l'ampleur de l'impact sur leur réputation. Cette étude met ainsi en lumière l'importance pour les institutions financières d'adopter des stratégies de gestion de crise et de communication efficaces pour atténuer les conséquences négatives sur leur réputation en période de crises.

2.3. L'impact des cyber-attaques sur la réputation des banques

Les pertes financières résultant des cyberattaques selon Gogolin, (2021) et Kamiya et al., (2021) sont considérables, atteignant des milliards de dollars chaque année, engendrant des coûts directs pour la réparation des systèmes et des pertes indirectes dues à la dégradation de la réputation des institutions financières, mais les atteintes à la réputation qui les accompagnent peuvent être tout aussi préjudiciables, voire plus. En effet, une

mauvaise réputation peut entraîner une perte de confiance des clients, ce qui se traduit par une diminution des dépôts et une baisse des investissements.

Par exemple, une étude récente a révélé que 30 % des clients envisagent de changer de banque après un incident de cybersécurité. De plus, les institutions financières peuvent faire face à des coûts accrus liés à la nécessité de redresser leur image, comme des campagnes de communication coûteuses ou des ajustements dans leurs offres de produits. Cette dégradation de la réputation peut également affecter les relations avec les partenaires commerciaux et les régulateurs, limitant ainsi les opportunités de croissance et d'expansion. Les atteintes à la réputation peuvent conduire à une perte de confiance de la part des clients, à une augmentation du taux de désabonnement et à une réduction de l'accès aux capitaux, ce qui a un impact sur les résultats de l'institution financière.

Contrairement aux pertes financières directes, les atteintes à la réputation peuvent persister pendant des années, entravant les efforts de redressement des institutions financières et ayant des conséquences durables sur leur image et leurs relations avec les clients Iyer et al., (2020) ainsi Perera, (2019). Ces atteintes peuvent également compliquer les interactions avec les régulateurs et les partenaires commerciaux, augmentant ainsi la difficulté de retrouver une position stable sur le marché. Le caractère durable des atteintes à la réputation souligne leur importance en tant que risque à long terme pour les institutions financières.

Kotidis et al. (2023) expliquent que l'atteinte à la réputation d'une institution financière peut avoir des effets d'entraînement et se propager à d'autres au sein du même marché ou du même secteur. L'interconnexion au sein de l'industrie financière suscite des inquiétudes quant aux risques systémiques et souligne la nécessité de coordonner les efforts de gestion des risques.

Aldasoro et al. (2020) étudient le rôle des médias sociaux dans la perception des cyberattaques par le public et dans les atteintes à la réputation. Ils constatent que le sentiment négatif et la désinformation qui se répandent sur les médias sociaux peuvent exacerber l'impact sur les banques.

Dans une autre étude, Kamiya et al. (2021) construisent un modèle pour explorer les répercussions des cyberattaques réussies sur la réputation de l'entreprise et la richesse des actionnaires. Leur définition des cyberattaques englobe les brèches externes qui compromettent les défenses d'une entreprise et entraînent la perte d'informations financières personnelles. La recherche met notamment en lumière l'érosion substantielle de la richesse subie par les actionnaires à la suite de telles attaques et l'utilisation de services infonuagiques.

Sufi (2007) et Gogolin et al. (2021) ont souligné que l'ampleur des atteintes à la réputation dans le secteur financier est le résultat de multiples facteurs interconnectés qui agissent de manière complexe et souvent simultanée. Parmi ces facteurs, la gravité des événements et leur nature spécifique occupent une place prépondérante. La nature de l'attaque, qu'il s'agisse de violations de données ou d'interruptions de service, ainsi que son degré de gravité, exercent une influence significative sur l'impact sur la réputation. Les

attaques hautement médiatisées, par leur capacité à capter l'attention des médias et à susciter un large écho dans l'opinion publique, peuvent avoir des répercussions particulièrement dommageables sur la réputation d'une organisation.

Kamiya et al. (2021) ainsi que Perera (2019) ont noté que la manière dont une organisation gère la crise qui découle de la cyberattaque joue un rôle crucial dans l'atténuation des dommages à sa réputation. Des pratiques de gestion de crise efficaces, telles que la communication transparente, la mise en œuvre de stratégies de réponse proactives et la prise en compte des préoccupations des parties prenantes, sont essentielles pour restaurer la confiance et la crédibilité de l'organisation. Une communication opportune et honnête avec les différentes parties prenantes, y compris les clients, les partenaires commerciaux et les autorités réglementaires, est particulièrement cruciale dans ce contexte.

En outre, Gopalan (2023) a souligné que la réputation préexistante d'une organisation, en particulier dans le cas des institutions financières, joue un rôle déterminant dans sa résilience face aux atteintes à la réputation. Les institutions dotées d'une réputation solide, fondée sur la confiance et des pratiques responsables, sont généralement mieux préparées à faire face aux conséquences d'une cyberattaque. En agissant comme un tampon, une réputation positive peut atténuer l'impact des événements négatifs sur la perception du public et sur la confiance accordée à l'organisation, limitant ainsi les dommages à sa réputation à long terme.

Les cyberattaques entraînent des répercussions étendues dans le secteur financier, touchant divers acteurs : Pour les institutions financières, les conséquences peuvent être sévères. Perera, (2019) et Gogolin et al., (2022) souligne que la perte de confiance des clients, les fuites de ces derniers vers des concurrents et les sanctions réglementaires peuvent entraîner des pertes financières significatives et une réduction de leur rentabilité. Iyer et al., (2020) démontrent que les investisseurs, qu'ils soient détenteurs d'obligations ou actionnaires, ne sont pas épargnés. Une atteinte à la réputation peut se traduire par des pertes de richesse à travers une dépréciation de la valeur de leurs investissements. Les perceptions négatives concernant les institutions financières peuvent conduire à une baisse des cours des actions et de la valeur des obligations.

Quant aux déposants, selon Gogolin et al., (2022) ils peuvent également être affectés. Les craintes liées aux violations de données et à la stabilité financière peuvent entraîner des retraits massifs de dépôts, surtout dans le cas des petites banques. Les déposants peuvent alors transférer leurs fonds vers des institutions perçues comme plus sûres, créant ainsi des problèmes de liquidité pour les banques touchées.

Aldasoro et al.(2022) analysent les caractéristiques et les facteurs des cyber incidents aux États-Unis dans divers secteurs, y compris le secteur financier. Leurs conclusions révèlent que les grandes entreprises subissent des coûts liés aux cyberattaques plus élevés, que les incidents ayant un impact sur plusieurs organisations entraînent des pertes financières plus importantes et que les cyberattaques malveillantes peuvent entraîner des conséquences financières majeures, en particulier dans les cas extrêmes. L'étude souligne également le rôle des services en nuage dans l'atténuation des coûts liés aux

cyberattaques et l'importance des dépenses informatiques dans la réduction des incidents cybernétiques futurs.

Jamilov et al. (2021) introduisent une nouvelle mesure de l'exposition au cyber-risque au niveau de l'entreprise, basée sur les conférences téléphoniques trimestrielles sur les résultats des entreprises cotées en bourse. Les données couvrent 13 000 entreprises de 85 pays sur la période 2002-2021. L'étude utilise la linguistique informatique pour analyser les transcriptions de ces appels et identifier les mentions de cyber-risques. Cela permet d'obtenir une perspective unique, au niveau de l'entreprise, sur l'exposition au cyber-risque, qui peut être utilisée pour comprendre comment différentes entreprises et différents secteurs perçoivent et gèrent le cyber-risque.

Amir, Levi et Livne (2019) cherchent à savoir dans une étude si les entreprises sous-déclarent les informations sur les cyber-attaques. En utilisant des données sur les cyber-attaques que les entreprises ont volontairement divulguées, et celles qui ont été retenues et plus tard découvertes par des sources extérieures à l'entreprise, les auteurs estiment la mesure dans laquelle les entreprises retiennent des informations sur les cyber-attaques. Ils constatent que les cyberattaques non divulguées sont associées à une baisse d'environ 3,6 % de la valeur des actions au cours du mois où l'attaque est découverte, et que les attaques divulguées sont associées à une baisse beaucoup plus faible de 0,7 %. Cela suggère que les dirigeants peuvent ne pas divulguer des informations négatives en dessous d'un certain seuil et ne pas divulguer d'informations sur les attaques les plus graves.

Tosun (2021) examine comment les marchés financiers réagissent aux violations inattendues de la sécurité des entreprises à court et à long terme. Les principaux résultats montrent que les rendements excédentaires quotidiens chutent, que le volume des transactions augmente en raison de la pression à la vente et que la liquidité se détériore après la divulgation publique des premiers événements de piratage d'entreprise. Les données relatives à la fréquence des recherches sur Google suggèrent que cette réaction de courte durée du marché est due à l'attention accrue des investisseurs. Les cyberattaques affectent les politiques des entreprises à long terme, jusqu'à cinq ans après l'annonce de la faille de sécurité. Ces résultats sont compatibles avec l'hypothèse selon laquelle les failles de sécurité représentent des chocs négatifs inattendus pour la réputation des entreprises.

En résumé, ces études permettent de comprendre l'impact des cyber-risques et des cyber-attaques sur les entreprises et les marchés financiers. Elles soulignent l'importance de la transparence dans la divulgation des cyberattaques et la nécessité de mettre en place des mesures de cybersécurité solides pour atténuer ces risques. Elles soulignent également les implications financières significatives des cyberattaques, à la fois en termes de réactions immédiates du marché et de changements politiques à long termes. Ces résultats soulignent l'importance cruciale d'une gestion efficace des cyber risques pour les entreprises modernes.

Le document de travail du FMI, présenté par Antoine Bouveret en juin 2018, aborde un cadre d'évaluation quantitative du cyber-risque dans le secteur financier. Il met en lumière

la nature en constante évolution des cybermenaces ainsi que les défis inhérents à la quantification de leur impact. Parmi les conclusions principales, on relève que les pertes financières des incidents cybernétiques sont plus élevées pour les grandes entreprises, soulignant ainsi l'importance cruciale d'investir dans les technologies de l'information pour réduire les coûts cybernétiques futurs. De plus, le document met en évidence les implications systémiques du risque cybernétique et insiste sur la nécessité d'adopter des stratégies proactives de gestion du risque dans le secteur financier.

Dans leur étude en 2019, Shinichi Kamiya et al. développent un modèle pour examiner l'impact des cyberattaques réussies sur la réputation des entreprises, leurs stratégies de gestion des risques et la richesse des actionnaires. Leur analyse empirique révèle que les cyberattaques impliquant la perte d'informations financières personnelles entraînent une perte de richesse actionnariale importante, dépassant ainsi les pertes directes des attaques. L'étude met en lumière les coûts de réputation des cyberattaques pour les entreprises cibles, ce qui conduit à des changements dans les politiques de l'entreprise, à une surveillance accrue de la gestion des risques par le conseil d'administration et à des ajustements des incitations des PDG.

Santiago Pollmeier et ses al. (2023) présentent une étude de cas portant sur la conception d'un modèle de quantification financière du risque cybernétique dans le secteur bancaire. L'étude offre un aperçu détaillé du développement d'un modèle complet visant à évaluer l'exposition au cyber-risque, en prenant en compte des éléments tels que les pertes financières potentielles et les impacts sur la réputation de l'institution. Cette approche permet de mieux appréhender les conséquences financières et réputationnelles des cyberattaques, offrant ainsi aux institutions financières des outils précieux pour une gestion proactive du risque cybernétique.

En conclusion, les atteintes à la réputation causées par les cyberattaques posent des problèmes importants aux institutions financières, car elles ont un impact sur leur stabilité financière, leurs relations avec les clients et leur réputation globale sur le marché. Il est essentiel de comprendre les facteurs qui influencent les atteintes à la réputation et leurs implications pour les parties prenantes afin de gérer efficacement les risques et de réagir aux crises dans le secteur financier. Les cyberattaques constituent une menace importante pour la réputation des banques, car elles ont un impact sur la confiance des clients et des investisseurs, sur le respect de la réglementation et sur la perception du public. Des recherches supplémentaires sont nécessaires pour explorer les tendances émergentes et les défis liés à l'atténuation de l'impact des cyberattaques sur la réputation des banques.

En 2021, Gogolin et al. ont examiné les effets des cyberattaques sur les petites banques américaines et ils ont constaté que les cyberattaques réussies entraînent une baisse des dépôts dans les succursales des petites banques, car la perte de confiance des clients conduit à une réaffectation des fonds vers de plus grandes institutions. De plus, ces attaques influent sur les relations bancaires et les normes de crédit, forçant les banques piratées à abaisser leurs critères. Les chercheurs soulignent l'importance cruciale des investissements en cybersécurité pour attirer et retenir les clients dans un paysage bancaire de plus en plus numérique et vulnérable aux cybermenaces.

Dzhaparov en 2020 aborde dans son article les risques cybernétiques comme une menace majeure pour les banques, en raison de la numérisation généralisée du secteur financier. Les cyberattaques, telles que l'hameçonnage, les Logiciels malveillants, les attaques par déni de service distribué, entre autres, sont identifiées comme des menaces sérieuses.

Dzhaparov (2020) souligne que la dépendance accrue des banques aux technologies informatiques les rend plus vulnérables aux cybermenaces. Ces attaques compromettent la sécurité des données sensibles et érodent la confiance des clients dans le système financier. Ainsi, l'article met en évidence la nécessité pour les banques d'investir dans des mesures de cybersécurité robustes pour contrer ces risques émergents et protéger les informations financières de leurs clients.

Dans un article de N. Tariq en 2018, offre une analyse approfondie de l'impact croissant des cyberattaques sur les institutions financières. L'auteur souligne que les cyberattaques sont en augmentation rapide et que leur incidence est de plus en plus sévère, causant à la fois des pertes directes et indirectes pour les institutions financières. Une des conclusions principales de l'article est que les institutions financières font face à une menace majeure en raison de la fréquence croissante et de la gravité des cyberattaques.

N. Tariq met en lumière la vulnérabilité croissante des institutions financières face à ces attaques, qui peuvent compromettre la sécurité des données sensibles, entraîner des pertes financières importantes et nuire à la réputation des institutions. En outre, l'article met en évidence l'importance croissante pour les institutions financières de prendre des mesures proactives pour se protéger contre les cybermenaces. Tariq souligne la nécessité pour les institutions financières d'investir dans des technologies de cybersécurité avancées, ainsi que dans la formation et la sensibilisation du personnel pour mieux comprendre et prévenir les cyberattaques.

En résumé, l'article de N. Tariq offre une perspective précieuse sur les défis croissants auxquels sont confrontées les institutions financières en matière de cybersécurité. Il met en lumière l'urgence pour ces institutions de renforcer leurs défenses et de mettre en place des stratégies robustes pour faire face à la menace croissante des cyberattaques.

P. Vijayalakshmi et al. (2020), se penchent sur les répercussions de la cybercriminalité sur le secteur de la banque en ligne. Ils mettent en évidence les conséquences néfastes des cyberattaques réussies, en particulier celles impliquant des informations financières personnelles. Ces attaques entraînent une perte significative de richesse pour les actionnaires des institutions visées. Cette perte est principalement influencée par l'impact sur la croissance des ventes et la gestion des risques avant l'attaque.

L'étude souligne également que les cyberattaques ont un impact sur l'appétit pour le risque des entreprises touchées, les incitant à adopter des stratégies plus conservatrices. De plus, les prix des actions des entreprises de l'industrie ciblée sont affectés négativement, témoignant de la perception du marché quant à la vulnérabilité de ces entreprises aux cybermenaces. En somme, cette revue de littérature met en avant l'importance cruciale pour les institutions financières en ligne d'investir dans des mesures de cybersécurité solides afin de protéger les données de leurs clients et de prévenir les conséquences dévastatrices des cyberattaques.

L. Parthiban (2014) examine les conséquences des cybercrimes sur le secteur bancaire. Les résultats principaux de l'étude révèlent que les cybercrimes ont eu un impact significatif sur le secteur bancaire, entraînant diverses formes de fraude et de pertes financières. L'impact financier des cybercrimes sur le secteur bancaire est considérable, nécessitant des ressources importantes pour lutter contre les cyber-attaques et développer des systèmes de prévention efficaces.

Nikoleta Musiał (2019) explore les implications de la gestion des risques cybernétiques dans le contexte des institutions financières. Les principales conclusions de l'étude révèlent que les risques cybernétiques représentent une menace significative pour les institutions financières, pouvant entraîner des dommages à la réputation et des pertes financières. Les petites et grandes entreprises sont également exposées à des risques similaires, et il est crucial pour les entreprises de comprendre et de se protéger contre les risques cybernétiques en constante évolution. Une gestion efficace des risques cybernétiques peut permettre aux entreprises de se démarquer de leurs concurrents et de développer des relations durables avec leurs clients.

Delroy A. Chevers (2019) examine l'impact de la cybercriminalité sur la banque en ligne et propose un modèle pour évaluer cette influence. Les principales conclusions de l'étude mettent en lumière la croissance continue des cybercrimes, caractérisée par une fréquence, un danger et une sophistication croissants des attaques. L'article souligne également les défis à relever pour contrer la complexité de la cybercriminalité et met en évidence les répercussions potentiellement négatives sur les entreprises et les économies nationales. Le modèle de recherche proposé vise à inciter d'autres chercheurs à mener des recherches empiriques dans leurs propres contextes, afin de mieux comprendre et contrer les effets de la cybercriminalité dans le secteur bancaire en ligne.

O. Akinbowale et al. (2020) se penchent sur les effets de la cybercriminalité sur le secteur bancaire et proposent une approche novatrice pour atténuer ces impacts négatifs. Les principales conclusions de l'étude mettent en évidence l'impact négatif de la cybercriminalité sur la réputation des institutions financières et sur la croissance économique. Pour contrer ces effets néfastes, les auteurs recommandent le développement d'un système d'alerte utilisant la technologie du big data. Ce système vise à sensibiliser à la fois les banques et les clients en intégrant efficacement la technologie du big data dans leurs systèmes. En outre, l'étude utilise le tableau de bord équilibré (BSC) pour analyser la cybercriminalité dans le secteur bancaire, une approche novatrice qui n'est pas suffisamment mise en avant dans la littérature existante.

2.4. Mécanismes Financiers des Prêts Syndiqués

Un prêt syndiqué est un prêt consenti à un emprunteur par un groupe de prêteurs, appelé syndicat, plutôt que par une seule institution financière. Ce type de prêt est généralement utilisé pour financer des projets ou des entreprises qui nécessitent des sommes importantes de capital importants, répartissant ainsi le risque entre plusieurs institutions. Selon Sufi (2007), le prêt syndiqué permet aux prêteurs de diversifier leur exposition au risque tout en offrant à l'emprunteur un accès à une somme d'argent plus importante que ce qu'un seul prêteur pourrait offrir.

Dans le cadre des prêts syndiqués, la sécurisation de l'information est essentielle. En raison de la complexité et de l'implication de plusieurs parties prenantes dans ce type de financement, les informations échangées, souvent sensibles, doivent être protégées. Une fuite d'informations ou une cyberattaque pourrait avoir des conséquences graves, à la fois financières et en termes de réputation pour les prêteurs, les arrangeurs et les emprunteurs. La protection de ces données permet de maintenir la confiance des parties impliquées et assure la stabilité des opérations.

L'article de Focarelli, Pozzolo et Casolaro (2008) explore l'effet du processus de certification sur les prix des prêts syndiqués. Cette étude s'inscrit dans un contexte où la certification joue un rôle crucial dans l'évaluation de la qualité des emprunteurs et des instruments financiers. En outre, la réputation des prêteurs et des agences de certification joue un rôle dans la détermination des prix des prêts syndiqués. Comme le montrent Focarelli, Pozzolo et Casolaro (2008), une institution financière bénéficiant d'une solide réputation obtient des conditions de prêt plus favorables, car elle réduit les coûts d'information et de gestion des risques pour les prêteurs. Cela explique pourquoi la certification, en tant que signal de qualité, peut influencer de manière significative les montants d'emprunt dans le cadre des prêts syndiqués.

Une étude antérieure importante dans ce domaine est celle de Diamond (1984), qui a souligné l'importance de la certification dans le marché de la dette et son rôle dans la réduction de l'asymétrie d'information entre les emprunteurs et les prêteurs. Cependant, l'article de Focarelli, Pozzolo et Casolaro (2008) se concentre spécifiquement sur les prêts syndiqués et examine comment la certification affecte leurs prix.

Les auteurs soutiennent que la certification peut agir comme un signal de qualité pour les prêteurs, réduisant ainsi les coûts d'information et permettant des prix plus bas pour les emprunteurs. Ils examinent également comment la réputation des agences de certification et la qualité de l'information divulguée peuvent influencer cet effet.

En conclusion, l'article de Focarelli, Pozzolo et Casolaro (2008) offre des insights précieux sur l'impact de la certification sur les prix des prêts syndiqués. Leur analyse théorique et empirique enrichit la compréhension des mécanismes sous-jacents à ce phénomène, ce qui est crucial pour les praticiens financiers et les décideurs politiques dans leur évaluation des risques et de la valeur des prêts syndiqués.

La recherche menée par Sufi (2007) explore l'impact de l'asymétrie de l'information sur les arrangements de financement, en se concentrant spécifiquement sur les prêts syndiqués. En examinant comment cette asymétrie influe sur les décisions de financement, l'étude met en évidence l'importance cruciale pour les prêteurs de développer des mécanismes efficaces de gestion des risques dans ce contexte complexe. Les résultats de cette étude fournissent des insights précieux pour les praticiens de la finance, en offrant des perspectives sur la manière dont les institutions financières peuvent mieux gérer les risques associés à l'asymétrie de l'information dans leurs activités de prêt.

En mettant en lumière les défis spécifiques posés par l'asymétrie de l'information dans le contexte des prêts syndiqués, la recherche de Sufi contribue également à enrichir la compréhension académique des mécanismes de fonctionnement des marchés financiers. En identifiant les implications pratiques de ces résultats, l'étude fournit un éclairage précieux sur la manière dont les institutions financières peuvent améliorer leurs pratiques de gestion des risques pour atténuer les effets de l'asymétrie de l'information et promouvoir des décisions de financement plus efficaces et éclairées.

En résumé, l'étude de Sufi offre une contribution significative à la fois pour la pratique de la finance et pour la recherche académique en fournissant des insights sur la manière dont les prêteurs gèrent les risques liés à l'asymétrie de l'information dans le contexte des prêts syndiqués. Ses conclusions éclairent les praticiens sur la nécessité de développer des stratégies de gestion des risques adaptées et offrent une base solide pour de futures recherches visant à approfondir notre compréhension des mécanismes de fonctionnement des marchés financiers.

L'étude menée par Acharya et al. (2018) explore les impacts concrets de la crise de la dette souveraine en Europe en utilisant des données de prêts syndiqués comme source d'analyse. Cette recherche offre un éclairage précieux sur les effets réels de la crise, en examinant comment elle a influencé l'accès au crédit pour les emprunteurs européens ainsi que les comportements d'investissement des entreprises. En se concentrant sur les prêts syndiqués, qui sont un élément crucial du financement des entreprises, l'étude permet de mieux comprendre les répercussions économiques de la crise sur l'économie réelle.

Les résultats de cette recherche fournissent des données tangibles sur la manière dont la crise de la dette souveraine a affecté les marchés financiers européens et contribuent ainsi à enrichir la compréhension globale des interactions complexes entre la politique économique, les marchés financiers et les entreprises. En résumé, cette étude constitue une contribution significative à la littérature en fournissant des preuves empiriques sur les véritables implications de la crise de la dette souveraine en Europe, ce qui peut avoir des implications importantes pour les décideurs politiques, les investisseurs et les praticiens de la finance.

La recherche menée par Giannetti et Yafeh (2012) explore l'impact des différences culturelles entre les parties contractantes sur les prêts bancaires syndiqués. Les prêts bancaires syndiqués sont une forme de financement où un groupe de banques travaille ensemble pour fournir un prêt à un emprunteur commun. Cette étude examine comment les différences culturelles entre les parties impliquées dans ces transactions influent sur

les termes du prêt, les performances financières des emprunteurs et la stabilité des prêts. Les auteurs utilisent des données empiriques pour évaluer ces effets et fournir des insights sur l'importance des facteurs culturels dans le domaine financier.

La recherche de Giannetti et Yafeh (2012) contribue à la compréhension des interactions entre la culture et les décisions financières, en mettant en évidence l'importance des différences culturelles dans le processus de prêt syndiqué. Leur analyse offre des perspectives sur la manière dont les facteurs culturels peuvent influencer les dynamiques de négociation, les niveaux de confiance entre les parties et les résultats financiers globaux. En identifiant ces mécanismes, l'étude fournit des informations précieuses pour les praticiens de la finance internationale, en soulignant l'importance de prendre en compte les aspects culturels lors de la conclusion de transactions financières transfrontalières. Cette recherche offre une analyse approfondie des effets des différences culturelles sur les prêts bancaires syndiqués. Leur étude éclaire les mécanismes sous-jacents par lesquels la culture peut influencer les décisions financières et fournit des recommandations importantes pour les praticiens et les décideurs dans le domaine de la finance internationale.

Dans sa déclaration de 2018, la Loan Market Association (LMA) met en garde contre les effets néfastes d'un Brexit difficile sur les marchés des prêts syndiqués et sur l'économie européenne. Cette déclaration souligne les préoccupations de l'industrie financière quant aux répercussions potentielles d'un Brexit sans accord sur la stabilité et le fonctionnement des marchés de prêts syndiqués, qui sont essentiels au financement des entreprises européennes. La LMA met en avant les risques de perturbation des flux de capitaux, d'incertitude juridique et de volatilité des marchés financiers qui pourraient découler d'un Brexit sans accord, et souligne l'importance pour les décideurs politiques de prendre des mesures pour atténuer ces risques.

Cette déclaration de la LMA met en lumière les préoccupations spécifiques de l'industrie financière concernant les conséquences d'un Brexit sans accord sur les marchés de prêts syndiqués. Elle fournit une perspective importante sur les défis potentiels auxquels les entreprises européennes pourraient être confrontées en termes de financement et de stabilité financière dans un tel scénario. En mettant en avant ces préoccupations, la déclaration de la LMA contribue au débat public sur les implications économiques du Brexit et souligne l'importance d'une approche prudente et coordonnée de la part des décideurs politiques pour atténuer les risques pour les marchés financiers européens.

La recherche menée par Berg et al. (2017) revisite le "puzzle de tarification des prêts syndiqués", mettant en lumière les écarts de prix observés dans ces types de prêts. Les prêts syndiqués sont des prêts accordés par un groupe de prêteurs à un emprunteur commun, et la tarification de ces prêts peut varier de manière significative malgré des caractéristiques similaires des emprunteurs, cette étude analyse les facteurs sous-jacents contribuant à cette disparité de tarification et propose des explications pour comprendre le phénomène.

Les résultats de cette recherche soulignent l'importance de prendre en compte divers facteurs, tels que la qualité du crédit de l'emprunteur, les conditions macroéconomiques et les caractéristiques spécifiques du prêt, pour expliquer les variations de prix observées dans les prêts syndiqués. En identifiant ces facteurs et en les intégrant dans un cadre analytique, l'étude de Berg et al. offre des insights précieux pour les praticiens de la finance et les chercheurs dans le domaine de la tarification des prêts syndiqués.

L'étude de Maskara (2010) se penche sur la valeur économique de la tranchée dans les prêts syndiqués, où un prêt est subdivisé en tranches vendues à divers investisseurs. Cette recherche évalue comment cette structuration affecte la valeur économique des prêts syndiqués en analysant des données empiriques pour évaluer ses avantages et inconvénients pour les emprunteurs, prêteurs et investisseurs. Les résultats de l'étude fournissent des perspectives sur les implications de la structuration des prêts en termes de partage des risques, de montants de financement et de répartition de la valeur économique entre les parties prenantes, contribuant ainsi à une meilleure compréhension des pratiques de structuration des prêts syndiqués et de leur impact sur les marchés financiers. En résumé, cette recherche offre une analyse approfondie de la tranchée dans les prêts syndiqués, apportant des informations précieuses pour les praticiens de la finance, les décideurs politiques et les chercheurs intéressés par la structuration des prêts et son impact sur l'allocation des ressources financières.

L'étude de Nini (2004) se concentre sur l'évaluation de la valeur des intermédiaires financiers à travers l'analyse des prêts syndiqués aux emprunteurs des marchés émergents. En examinant ces transactions financières, qui impliquent un groupe de prêteurs fournissant un prêt à un emprunteur commun, l'étude vise à déterminer le rôle et l'impact des intermédiaires financiers dans ces marchés spécifiques. Les résultats de l'étude mettent en lumière l'importance cruciale des intermédiaires financiers dans la facilitation de ces transactions, soulignant notamment leur capacité à réduire les montants de transaction et à fournir une expertise en matière de crédit.

Cette recherche offre ainsi des insights précieux sur le rôle des intermédiaires financiers dans les marchés de prêts syndiqués aux emprunteurs des marchés émergents. En soulignant les avantages qu'ils apportent, tels que la réduction des coûts et l'expertise, elle contribue à une meilleure compréhension de leur valeur ajoutée dans le fonctionnement global des marchés financiers internationaux. En résumé, cette étude offre une analyse empirique approfondie qui peut avoir des implications importantes pour les praticiens de la finance internationale ainsi que pour les décideurs politiques cherchant à comprendre le rôle des intermédiaires financiers dans ces marchés spécifiques.

Ferreira et al. en (2012), explorent l'impact des banques universelles sur la gouvernance d'entreprise via le marché des prêts syndiqués. Les banques universelles, qui offrent des

services bancaires tant commerciaux qu'investissement, jouent un rôle crucial dans le financement des entreprises. Ferreira et Matos analysent comment ces banques, grâce à leur capacité à structurer et à diriger des prêts syndiqués, influencent les décisions des entreprises emprunteuses et imposent des conditions de prêt strictes, protégeant ainsi leurs propres intérêts.

Les auteurs démontrent empiriquement que la présence de banques universelles dans les syndicats de prêts conduit à des conditions de prêt plus rigoureuses et à une meilleure performance des entreprises emprunteuses. Utilisant des données globales sur les prêts syndiqués, ils montrent que les entreprises bénéficiant de prêts de banques universelles présentent une réduction des risques de défaut, ce qui souligne l'effet positif de ces banques sur la gouvernance d'entreprise. Cette étude se positionne dans la continuité de recherches antérieures sur le rôle historique des banques universelles en Allemagne et leurs effets sur la structure de financement des entreprises.

En situant leur recherche dans un cadre plus large, Ferreira et Matos (2012) enrichissent la littérature existante sur la gouvernance d'entreprise et les prêts syndiqués. Ils confirment les théories selon lesquelles les banques universelles, en raison de leur pouvoir de marché et de leurs capacités de contrôle, jouent un rôle déterminant dans la surveillance et l'amélioration de la performance des entreprises. Leur travail s'ajoute aux contributions de chercheurs comme Gerschenkron, Fohlin (2000), et plus récemment Sufi et Ivashina (2009), qui ont étudié les impacts des prêts syndiqués sur la performance des entreprises et les conditions de financement.

Ekkehart Boehmer et William L. Megginson, (1990), analyse les facteurs influençant les prix des prêts syndiqués des pays en développement sur le marché secondaire. En examinant ces déterminants, les auteurs cherchent à comprendre comment les risques et les rendements associés à ces prêts se reflètent dans leurs prix de revente. Cette recherche est particulièrement pertinente pour les investisseurs et les décideurs politiques qui cherchent à optimiser la gestion des risques financiers dans les marchés émergents. Les auteurs identifient plusieurs facteurs clés qui influencent les prix sur le marché secondaire des prêts syndiqués, tels que la solvabilité des pays emprunteurs, les conditions économiques mondiales, et les termes spécifiques des prêts, incluant les taux d'intérêt et les garanties.

Par une analyse empirique détaillée, Boehmer et Megginson (1990) montrent que les variations des prix des prêts sont principalement attribuables aux différences de risques de crédit et de marché des pays en développement. Leur étude démontre que des facteurs comme la stabilité économique et la politique économique des pays emprunteurs jouent un rôle crucial dans la détermination des prix de ces prêts.

En situant leur travail dans le contexte des recherches existantes, Boehmer et Megginson (1990) enrichissent la littérature sur les marchés des prêts syndiqués et le risque souverain. Ils complètent les études antérieures en fournissant des insights sur les implications pratiques pour les investisseurs et les décideurs politiques, soulignant l'importance de la stabilité macroéconomique pour améliorer l'accès au financement international. Leur recherche offre une base solide pour les analyses futures sur la gestion des risques et la détermination des prix des actifs financiers dans les pays en développement.

Steven Dennis et Donald Mullineaux (2000) analysent les différents aspects du marché des prêts syndiqués, qui sont des prêts accordés par un groupe de banques à un emprunteur unique. Les auteurs examinent les motivations des banques à participer à ces syndicats, la structure de ces prêts, ainsi que leurs implications pour les institutions financières et les emprunteurs. Cette recherche est fondamentale pour comprendre comment ces prêts facilitent le financement des grandes entreprises et des projets d'infrastructure tout en permettant une gestion efficace des risques pour les banques.

Dennis et Mullineaux (2000) identifient plusieurs motivations pour les banques à participer à des prêts syndiqués, notamment la diversification des risques, l'accès à de nouveaux clients, et les revenus supplémentaires générés par les frais de syndication. Ils montrent que la participation à des syndicats de prêts permet aux banques de partager les risques associés à des prêts de grande envergure et d'améliorer leurs relations avec d'autres institutions financières.

Les auteurs analysent également la structure des prêts syndiqués, y compris la répartition des parts de prêt entre les membres du syndicat et les rôles spécifiques des banques leaders et participantes, révélant que cette structure dépend de la taille et de la complexité du prêt, ainsi que de la réputation des banques impliquées.

Les implications des prêts syndiqués sont significatives tant pour les emprunteurs que pour les banques. Pour les emprunteurs, ces prêts offrent des conditions de financement plus flexibles et souvent à des coûts réduits grâce à la concurrence entre les banques du syndicat. Pour les banques, les prêts syndiqués représentent une opportunité de renforcer leur position sur le marché et d'améliorer leur gestion du risque de crédit. Cet article enrichit la littérature sur la finance intermédiée en fournissant des perspectives détaillées sur les mécanismes et les avantages des prêts syndiqués, offrant ainsi des insights précieux pour les chercheurs et les praticiens du domaine financier.

Y. Chen, M. Hu, et S. Kim (2019) mettent en lumière les menaces telles que le phishing, les logiciels malveillants et les violations de données, qui exposent les vulnérabilités uniques des transactions syndiquées, notamment la transmission électronique d'informations sensibles entre les parties prenantes. Ces risques menacent la stabilité des processus de prêt et la confidentialité des données, ce qui peut entraîner une perte de confiance des investisseurs et des emprunteurs dans le système financier.

Pour atténuer ces risques, l'article propose des stratégies axées sur des mesures de sécurité renforcées, la formation du personnel et une collaboration étroite entre les acteurs du marché financier. En développant des pratiques robustes de cybersécurité et en renforçant la sensibilisation aux menaces numériques, les institutions financières peuvent mieux protéger les transactions syndiquées contre les attaques cybernétiques et maintenir la confiance dans l'intégrité des transactions financières.

L'impact négatif sur la réputation des banques, mesuré par la rétention des prêts au sein des syndicats, est également confirmé. Nous mesurons la réputation par la capacité d'une banque à maintenir sa position en tant que chef de file ou membre principal des syndicats de prêt. Une baisse de cette rétention, ainsi qu'une diminution du rôle de la banque dans les nouveaux syndicats formés, témoigne d'une détérioration de sa réputation.

La certification est cruciale sur le marché financier car elle permet de réduire les asymétries d'information entre les prêteurs et les emprunteurs. Sur les marchés où les informations sur la solvabilité d'une entreprise peuvent être incomplètes ou incertaines, le fait qu'une banque chef de file accepte d'organiser un prêt syndiqué envoie un signal fort aux autres prêteurs potentiels et aux investisseurs. Cela agit comme une forme de garantie implicite de la qualité de l'emprunteur, car les banques participantes comptent sur l'expertise de la banque chef de file pour évaluer les risques associés à l'emprunteur.

Dans ce contexte, les prêts syndiqués jouent un rôle clé, car ils sont souvent arrangés par des banques bien établies qui jouissent d'une solide réputation. La participation de ces banques à la structuration et à la coordination des prêts aide à rassurer les autres membres du syndicat sur la solidité financière de l'emprunteur, renforçant ainsi la confiance. En outre, les banques chefs de file subissent une pression importante pour maintenir leur réputation, ce qui renforce leur diligence dans l'évaluation des risques, d'où l'importance de la certification.

3. Hypothèses et prédictions empiriques

Cette section expose les trois hypothèses principales qui structurent notre étude.

3.1. Hypothèse 1

Notre première hypothèse stipule que les cyberattaques subies par les emprunteurs entraînent une réduction du montant des prêts syndiqués accordés par les banques. En effet, les cyberattaques augmentent les risques opérationnels et financiers perçus, ce qui peut réduire la volonté des prêteurs de participer à des transactions de grande envergure. Les prêts syndiqués reposent sur la confiance des participants envers l'arrangeur principal et les capacités de l'emprunteur à honorer ses engagements (Ivashina, 2009; Sufi, 2007). Les études antérieures (Kamiya et al., 2021) suggèrent que les événements augmentant la perception du risque, tels que les cyberattaques, conduisent à des ajustements dans la taille des prêts octroyés, car les prêteurs cherchent à limiter leur exposition financière.

3.2. Hypothèse 2

Notre deuxième hypothèse explore l'impact des cyberattaques sur la structure des prêts syndiqués, en particulier le nombre des participants. Nous supposons que lorsqu'un emprunteur subit une cyberattaque, le nombre de participants à un prêt syndiqué diminue, entraînant une structure de prêt plus concentrée.

Dans le cadre de notre étude sur l'impact des cyberattaques, nous faisons un parallèle avec l'hypothèse de réputation de Gopalan et al. (2011). De la même manière que les faillites peuvent nuire à la réputation des chefs de file et réduire leur capacité à attirer des participants, les cyberattaques pourraient également affecter la réputation des banques leaders en suggérant une faiblesse dans leur cybersécurité, ce qui pourrait décourager d'autres banques de participer à des prêts syndiqués avec elles. Cela entraînerait une concentration accrue des prêts et potentiellement des coûts plus élevés pour l'emprunteur.

3.3. Hypothèse 3

Les cyberattaques affectent la réputation des banques, mesurée par une augmentation des exigences de fonds propres des prêteurs, notamment à travers une hausse du ratio de fonds propres de catégorie 1 (Tier One). Le ratio Tier One, bien qu'il soit principalement un indicateur de stabilité financière et de gestion des risques, a également une dimension réputationnelle importante. Dans un secteur bancaire où la confiance est cruciale, un ratio Tier One élevé est perçu comme un signal de fiabilité et de solidité financière, renforçant

ainsi la réputation de la banque auprès des investisseurs et des parties prenantes. Après une cyberattaque, qui fragilise cette confiance, les prêteurs peuvent percevoir un besoin d'accroître ce ratio pour signaler leur résilience face aux risques accrus. En réponse à cette menace, les banques peuvent augmenter leurs réserves de capital, ce qui est interprété comme une stratégie visant à rassurer le marché sur leur capacité à absorber les chocs financiers. Ainsi, un ratio Tier One élevé après une cyberattaque devient un moyen pour les banques de maintenir ou restaurer leur réputation en montrant qu'elles sont suffisamment solides pour gérer les perturbations, ce qui peut également se traduire par des exigences plus strictes en matière de prêt et de garanties de la part des prêteurs.

4. Base de données et description des variables

4.1. Base de données

Les données de cette étude proviennent de Dealscan, une source reconnue fournissant des informations complètes sur les prêts syndiqués, y compris le montant des prêts, la structure et les conditions de financement, ainsi que les caractéristiques des emprunteurs et des prêteurs. Cette base de données est largement utilisée dans les études académiques portant sur les prêts syndiqués (Gopalan et al., 2011 ; Chu et al., 2019 ; Shin, 2021 ; Newton et al., 2022). En complément, UpGuard fournit des informations fiables sur les cyberincidents majeurs, en particulier dans le secteur financier. En nous concentrant sur les emprunteurs ayant subi des cyberattaques, nous avons construit notre variable « profil cyberattaque » à partir des informations recueillies sur le site UpGuard.

4.2. Analyse descriptive

Nos variables explicatives sont l'indicateur de cyberattaque, les années et les caractéristiques regroupées en trois catégories différentes. Les caractéristiques des prêts incluent log(montant des prêts), court terme, moyen terme, long terme, fonds de roulement, refinancement et garantie. Les caractéristiques des emprunteurs comprennent log(actifs), log(taille), ROA emprunteur et valeur de marché. Enfin, les caractéristiques des prêteurs sont composées du nombre de prêteurs, log(taille des prêteurs), ROA prêteurs, log_Prêteurs_PartN, total des prêts sur total des actifs et nombre de chefs de file. Cette classification nous permet d'analyser l'impact des cyberattaques sur les prêts syndiqués en prenant en compte les variables de contrôle liées aux prêts, aux emprunteurs et aux prêteurs.

4.2.1. Description des variables

Nous allons définir les variables utilisées dans notre étude, et expliquer en détail chacune des variables dépendantes et explicatives :

Variables Dépendantes:

Log (Montant du prêt) : Le logarithme est utilisé pour réduire la variabilité et atténuer l'impact des valeurs extrêmes. Cela facilite les analyses statistiques, notamment en rendant la distribution des montants de prêts plus proche d'une distribution normale.

Log (Nombre des participants) : Le logarithme est utilisé pour réduire la skewness (asymétrie) de la distribution, ce qui permet une analyse plus robuste, surtout lorsque la variable présente une forte dispersion. Cela aide aussi à interpréter les résultats en termes de pourcentage de variation.

Log (Ratio de fonds propres de catégorie 1 des prêteurs) : Le ratio de fonds propres de catégorie 1 reflète la capacité des banques à absorber les pertes sans compromettre leur solvabilité. Un ratio plus élevé indique que la banque dispose de capitaux de haute qualité, renforçant ainsi sa résilience financière.

Variables Explicatives:

Indicateur Cyberattaque : Cette variable binaire permet de capturer l'impact des cyberattaques sur les prêts syndiqués. Une valeur de 1 indique que l'emprunteur a subi une cyberattaque, ce qui permet de tester si ces événements influencent négativement les décisions des prêteurs.

Taille des prêteurs (Log des actifs totaux) : Cette variable mesure la capacité des banques à diversifier leurs risques et supporter de plus grands engagements financiers, souvent associée à une meilleure stabilité.

ROA Prêteurs et Emprunteurs : Le ROA (Return on Assets) indique l'efficacité avec laquelle une entité utilise ses actifs pour générer des bénéfices. Un ROA plus élevé reflète une rentabilité accrue.

Valeur de marché : La valeur de marché des capitaux propres par rapport à la valeur comptable indique comment les investisseurs perçoivent la performance future et le risque de l'emprunteur.

Garantie : Cette variable binaire (1 = garantie fournie, 0 = pas de garantie) est importante pour évaluer si la présence d'une garantie impacte les décisions des prêteurs, surtout après une cyberattaque.

Fonds de roulement : Il reflète la capacité de l'emprunteur à financer ses opérations quotidiennes et à faire face à des obligations à court terme.

Refinancement: Un indicateur important pour différencier entre les prêts pour de nouvelles opérations et ceux visant à restructurer une dette existante.

Nombre de chefs de file : Un nombre élevé de chefs de file peut indiquer une diversification du risque et un partage des responsabilités accrues dans la syndication.

Court terme : Cette variable binaire identifie les prêts dont l'échéance est inférieure ou égale à un an. Elle permet de mesurer la proportion de prêts à court terme dans l'échantillon et leur impact sur les décisions des prêteurs.

Long terme : Cette variable binaire identifie les prêts dont l'échéance est supérieure à cinq ans. Elle permet d'étudier l'impact des prêts à long terme sur les caractéristiques des emprunteurs et des prêteurs dans les syndications.

4.2.2 Statistique descriptive

L'analyse descriptive des variables utilisées dans cette étude nous permet de mieux comprendre la distribution et la variabilité des données avant d'entreprendre les analyses économétriques. (Le Tableau 1) présente les statistiques descriptives des principales variables de l'étude, qui constituent une base essentielle pour examiner l'impact des cyberattaques sur les montants et les conditions des prêts syndiqués.

La variable Log (Montant de la transaction), qui représente la transformation logarithmique des montants des transactions, affiche une moyenne de 6,55 avec un écart-type de 1,05. Cela indique une certaine variation autour de cette moyenne, mais à un niveau modéré. L'utilisation du logarithme vise à réduire l'impact des valeurs extrêmes, facilitant ainsi la comparaison entre prêts de différentes tailles. En parallèle, Log (Montant des prêts), qui suit une transformation similaire, présente une moyenne de 6,20 et une médiane de 6,21, suggérant une distribution relativement symétrique des montants de prêts dans l'échantillon. Les données montrent ainsi que la plupart des prêts sont relativement proches en termes de montants, avec peu de valeurs aberrantes.

L'Indicateur Cyberattaque, une variable binaire mesurant la présence ou l'absence d'une cyberattaque associée à un prêt, a une moyenne de seulement 0,06. Cela révèle que, dans la majorité des cas, les prêts ne sont pas liés à des cyberattaques, avec une fréquence de 6% pour ces événements. Cette rareté des cyberattaques dans l'échantillon est importante pour comprendre leur potentiel impact sur les prêts syndiqués.

Concernant les caractéristiques des prêteurs, la variable Taille des prêteurs, mesurée par la valeur totale des actifs, affiche une moyenne de 22,32 avec un écart-type de 1,55. Cela montre que les prêteurs dans l'échantillon sont globalement de grande taille, ce qui peut avoir une influence sur leur capacité à structurer et à supporter de grands prêts syndiqués. Cette caractéristique est renforcée par le Ratio de fonds propres des prêteurs, qui, avec une moyenne de 0,14, suggère une certaine variabilité dans la solidité financière des prêteurs, certains ayant des fonds propres relativement faibles par rapport à leurs actifs totaux.

Du côté des emprunteurs, la variable ROA Emprunteur (Return on Assets) affiche une moyenne de 0,11, avec des valeurs allant de -1,19 à 2,54. Cela indique une grande diversité dans la rentabilité des emprunteurs, avec certains enregistrant des résultats financiers très faibles voire négatifs, et d'autres ayant des performances bien au-dessus de la moyenne. Ce type de variation peut affecter la capacité des emprunteurs à honorer leurs engagements financiers.

En ce qui concerne la Valeur de Marché des emprunteurs, cette variable présente une moyenne de 1,25 et un écart-type élevé de 9,95. Cette grande dispersion dans les valeurs de marché des emprunteurs suggère qu'il existe une hétérogénéité significative dans la taille et la valeur des entreprises emprunteuses, ce qui peut influencer la perception du risque associé aux prêts qu'elles contractent.

D'autres variables clés, telles que la Garantie, le Fonds de roulement et le Refinancement, permettent de mieux comprendre la structuration des prêts syndiqués. Par exemple, la variable Garantie a une moyenne de 0,34, indiquant que dans environ un tiers des prêts, une garantie est fournie, ce qui peut jouer un rôle dans la sécurisation du crédit. La variable Fonds de roulement, avec une moyenne de 0,21, montre que la majorité des prêts ne sont pas spécifiquement utilisés pour financer le fonds de roulement des emprunteurs. Enfin, Refinancement, qui mesure si le prêt est destiné à refinancer une dette existante, affiche une moyenne de 0,23, ce qui suggère que près d'un quart des prêts dans l'échantillon servent à cette fin.

Enfin, la Diversité des prêteurs est mesurée par la variable Nombre de chefs de file qui, avec une moyenne de 2,21, montre une gestion relativement concentrée des syndications de prêts, bien que le nombre de chefs de file puisse varier considérablement entre les prêts. De plus, la variable Log (Nombre de prêteurs), qui mesure le nombre total de prêteurs impliqués dans un prêt syndiqué, a une moyenne de 2,60, suggérant une structure de syndicat de prêts dominée par un petit nombre de prêteurs principaux dans la plupart des cas.

4.3. Matrice de corrélation

Les résultats présentés dans (les tableaux 2, 3, 4 et 5) illustrent les corrélations entre les différentes variables de l'étude, fournissant des insights précieux sur la dynamique des prêts syndiqués. La matrice de corrélation révèle des relations significatives entre plusieurs variables clés, fournissant des aperçus précieux sur la dynamique des prêts syndiqués. Par exemple, Log (montant de la transaction) et Log (montant des prêts) présentent une corrélation très élevée de 0,836*, ce qui suggère une forte association entre le montant total du prêt et le montant individuel des prêts. Cela indique que lorsque le montant total des transactions augmente, les montants des prêts individuels tendent également à augmenter.

De plus, une corrélation notable de 0,731* entre Log (actifs) et Log (taille) souligne que la taille des emprunteurs est directement liée à leurs actifs, ce qui peut avoir des implications sur leur capacité à obtenir des financements.

Les résultats montrent également que le nombre de prêteurs présente une corrélation positive avec Log (montant de la transaction) (0,635*) et Log (montant des prêts) (0,627*). Cela indique que les prêts impliquant un plus grand nombre de prêteurs tendent à avoir des montants plus élevés, ce qui pourrait être interprété comme une augmentation de la confiance des prêteurs dans les emprunteurs lorsque plusieurs d'entre eux sont impliqués.

Concernant les variables liées aux cyberattaques, indicateur cyberattaque présente des corrélations positives avec Log (montant de la transaction) (0,144*) et Log (montant des prêts) (0,109*), suggérant que les prêts associés à des cyberattaques sont souvent de plus grande envergure. Toutefois, il est important de noter les corrélations négatives significatives observées avec des variables telles que Log des prêteurs PartN (-0,058*) et ROA prêteurs (-0,231*), indiquant que les cyberattaques pourraient avoir des effets délétères sur certaines mesures de performance des prêteurs.

5. Méthodologie économétrique

5.1. Modèle de moindres carrés ordinaires

Dans cette section, nous présentons le modèle économétrique basé sur la méthode des moindres carrés ordinaires (MCO), qui nous permet d'évaluer l'impact des cyberattaques sur le montant des prêts syndiqués. Nous avons choisi d'appliquer une régression linéaire multiple, en nous inspirant des travaux antérieurs tels que ceux de Gopalan et al. (2011), Chu et al. (2019), et Newton et al. (2021), qui ont également utilisé cette méthode pour analyser des dynamiques similaires dans le contexte des prêts.

Pour estimer nos équations, nous avons utilisé le logiciel RStudio Desktop (<https://posit.co/download/rstudio-desktop/>), en raison de sa flexibilité et de ses capacités d'analyses statistiques avancées. La décision d'utiliser RStudio repose sur sa large adoption dans les analyses économétriques récentes.

En nous appuyant sur la littérature existante, nous modélisons la relation entre nos variables dépendantes et un ensemble de variables explicatives. Parmi celles-ci, l'indicateur cyberattaque est une variable clé, mesurant l'impact des incidents de cyberattaques sur les conditions des prêts. Cet indicateur prend la valeur de 1 si une entreprise a subi une cyberattaque dans les 12 mois précédant l'émission du prêt, et 0 dans le cas contraire.

L'équation de base de notre modèle est formulée comme suit :

Log(montant des prêts syndiqués)

$$\begin{aligned} &= \beta_0 + \beta_1 * \text{Indicateur Cyberattaque} + \beta_2 * \text{Taille des prêteurs} \\ &+ \beta_3 * \text{Ratio de fonds propres première catégorie prêteurs} + \beta_4 \\ &* \text{ROA PRÊTEURS} + \beta_5 * \text{Log Actifs emprunteur} + \beta_6 \\ &* \text{ROA emprunteur} + \beta_7 * \text{Valeur de Marche emprunteur} + \beta_8 \\ &* \text{Garantie} + \beta_9 * \text{Fonds de Roulement} + \beta_{10} * \text{Refinancement} \\ &+ \beta_{11} * \text{Nombre de chefs de file} \end{aligned} \quad (1)$$

L'équation (1) nous permet de tester l'impact des cyberattaques sur le montant des prêts syndiqués, conformément à notre première hypothèse. Cette régression inclut diverses variables explicatives. L'indicateur cyberattaque prend la valeur de 1 si l'emprunteur a été victime d'une cyberattaque, et 0 sinon. Nous intégrons également des caractéristiques des prêteurs, telles que la taille des prêteurs, le Ratio de fonds propres de première catégorie, et le ROA des prêteurs, qui mesurent leur solidité financière. Du côté des emprunteurs, nous considérons le Log des actifs, le ROA, et la valeur de marché pour évaluer leur stabilité financière et leur capacité de remboursement. Enfin, nous prenons en compte plusieurs caractéristiques des prêts, y compris la garantie, le fonds de roulement, le refinancement, et le nombre de chefs de file, qui reflètent la structure et la répartition du risque dans les prêts syndiqués.

Toutefois, pour tester notre deuxième hypothèse, nous reprenons notre échantillon de la manière suivante :

$$\begin{aligned}
 & \text{Log}(\text{Nombre de participants}) \\
 &= \beta_0 + \beta_1 * \text{Indicateur Cyberattaque} + \beta_2 * \text{Taille des prêteurs} \\
 &+ \beta_3 * \text{Ratio de fonds propres première catégorie des prêteurs} \\
 &+ \beta_4 * \text{ROA prêteurs} + \beta_5 * \text{Log Actifs emprunteur} + \beta_6 \\
 &* \text{ROA emprunteur} + \beta_7 * \text{Valeur de Marche emprunteur} + \beta_8 \\
 &* \text{Garantie} + \beta_9 * \text{Fonds de Roulement} + \beta_{10} \\
 &* \text{Refinancement} \tag{2}
 \end{aligned}$$

Pour évaluer cette hypothèse, nous avons construit un modèle économétrique où la variable dépendante est le logarithme du nombre de prêteurs participants. Les variables explicatives incluent un indicateur de cyberattaque, ainsi que des variables de contrôle telles que les actifs de l'emprunteur et sa rentabilité.

Enfin, pour approfondir notre analyse, nous proposons une troisième hypothèse, décrite par l'équation suivante :

$$\begin{aligned}
 & \text{Log}(\text{Ratio de fonds propres première catégorie prêteurs}) \\
 &= \beta_0 + \beta_1 * \text{Indicateur Cyberattaque} + \beta_2 \\
 &* \text{Log actifs emprunteur} + \beta_3 * \text{Garantie} + \beta_4 \\
 &* \text{Fonds de Roulement} + \beta_5 * \text{Refinancement} \tag{3}
 \end{aligned}$$

Cette dernière équation nous permet d'analyser l'impact des cyberattaques sur le ratio de fonds propres des prêteurs, en tenant compte des caractéristiques des emprunteurs et des garanties associées.

5.2. Tests de Diagnostics

Les tests de diagnostics sont essentiels pour vérifier la validité des hypothèses sous-jacentes du modèle de régression par moindres carrés ordinaires (MCO). Si ces hypothèses ne sont pas respectées, les résultats du modèle peuvent être biaisés ou inefficaces, ce qui affecterait la robustesse de nos conclusions.

5.2.1. Test de Breusch-Pagan pour l'hétéroscédasticité

Pour vérifier la présence d'hétéroscédasticité, nous avons appliqué le test de Breusch-Pagan. L'hypothèse nulle (H_0) de ce test stipule que la variance des erreurs est constante (homoscédasticité), tandis que l'hypothèse alternative (H_1) indique la présence d'hétéroscédasticité.

Dans notre analyse (Tableau 6), le test de Breusch-Pagan a donné une statistique de 2994,9 avec une p-value inférieure à $2,2e-16$. Étant donné que la p-value est bien en dessous du seuil de signification de 5 %, nous rejetons l'hypothèse nulle d'homoscédasticité. Cela signifie que notre modèle présente des signes d'hétéroscédasticité, indiquant que la variance des erreurs n'est pas constante à travers les observations. Pour corriger ce problème, des méthodes robustes, telles que des erreurs standard robustes, seront utilisées pour garantir la validité des estimations.

5.2.2. Test de Multi colinéarité à l'aide du VIF (Variance Inflation Factor)

La multicolinéarité est un phénomène qui survient lorsque deux ou plusieurs variables indépendantes dans un modèle de régression sont fortement corrélées entre elles. Cela peut poser des problèmes en régression, car cela rend les estimations des coefficients moins fiables et peut rendre l'interprétation des résultats plus difficile. En outre, la multicolinéarité peut augmenter la variance des coefficients estimés, ce qui les rend sensibles aux petites variations des données.

Pour détecter la multicolinéarité, nous utilisons le facteur d'inflation de la variance (VIF), qui mesure dans quelle mesure la variance d'une variable explicative est amplifiée par sa corrélation avec les autres variables. En règle générale, un VIF supérieur à 5 ou 10 indique une multicolinéarité problématique.

Les résultats de ce test sont présentés dans (le tableau 7), montrent que les VIF des variables explicatives dans notre modèle sont tous bien inférieurs à 2.5, ce qui indique qu'il n'y a pas de multicolinéarité significative. En conséquence, les coefficients estimés sont stables et les variables explicatives ne sont pas fortement corrélées entre elles, garantissant ainsi la fiabilité de notre modèle.

6. Description du modèle de régression linéaire multiple avec des données de panel et des effets fixes

Dans cette étude, nous utilisons un modèle de régression linéaire multiple avec des effets fixes, appliqué sur un panel de 984 entités comprenant des prêteurs et des emprunteurs, couvrant la période de 2001 à 2021, avec un total de 65 863 observations. Ce type de modèle est particulièrement adapté aux analyses longitudinales où les mêmes entités sont suivies sur plusieurs périodes. L'approche des données de panel est efficace pour traiter les dépendances non observées entre les variables explicatives et la variable dépendante, réduisant ainsi les biais potentiels que l'on rencontre dans les modèles de régression linéaire classiques.

Les données de panel, par définition, sont bidimensionnelles : elles combinent des observations sur plusieurs entités (comme les entreprises) à travers différentes périodes. Cette double dimension permet d'intégrer à la fois des caractéristiques transversales et des séries chronologiques. Contrairement aux données transversales, qui ne capturent qu'un instantané, ou aux séries chronologiques, qui se concentrent sur une seule unité dans le temps, les données de panel offrent une meilleure compréhension des dynamiques sous-jacentes en tenant compte des variations individuelles et temporelles. Cette approche enrichit notre analyse en incorporant des effets fixes qui contrôlent les caractéristiques inobservées et constantes dans le temps des entités étudiées.

L'utilisation d'un modèle à effets fixes s'avère cruciale pour notre étude sur l'impact des cyberattaques sur les prêts syndiqués. Cette méthode permet de contrôler les effets non observés propres à chaque entité en utilisant des variables indicatrices pour chaque unité. Cela est particulièrement utile lorsque ces effets non observés sont corrélés avec les variables explicatives, ce qui pourrait autrement biaiser les estimations des coefficients. En adoptant les effets fixes, nous isolons ainsi l'effet des variables explicatives sur notre variable dépendante tout en éliminant les biais dus aux variables omises qui restent constantes dans le temps pour chaque emprunteur ou prêteur.

Pour estimer notre modèle, nous avons appliqué la méthode des moindres carrés ordinaires (MCO). Cette technique minimise la somme des carrés des écarts entre les valeurs observées et celles prédites par le modèle, produisant ainsi des estimations efficaces des coefficients. L'application de cette méthode sur des données de panel permet de tirer parti des avantages des observations multiples sur des périodes variées, ce qui améliore la précision des résultats obtenus.

6.1. Utilisation des effets fixes pour `année` et `l'identifiant de l'emprunteur`

L'intégration des effets fixes pour l'année et l'identifiant de l'emprunteur permet de contrôler les facteurs temporels (comme les chocs économiques globaux) et les attributs spécifiques à chaque emprunteur (comme la stabilité financière), améliorant ainsi la robustesse de nos estimations.

6.2. Prise en compte des facteurs temporels et des caractéristiques des emprunteurs

Dans le cadre de notre analyse, nous intégrons des effets fixes pour les années et pour l'identifiant des emprunteurs. Cette approche permet de contrôler les fluctuations temporelles globales (telles que les chocs macroéconomiques) ainsi que les attributs spécifiques à chaque emprunteur, qui peuvent influencer les résultats. De plus, nous tenons compte des caractéristiques des emprunteurs en incluant des variables explicatives telles que le logarithme des actifs, le ratio de rentabilité des actifs (ROA), ainsi que d'autres indicateurs financiers. Cette démarche garantit que nous isolons au mieux l'impact des cyberattaques sur les conditions de prêt en prenant en compte les différences inhérentes entre les emprunteurs.

Enfin, les effets fixes appliqués aux années nous permettent de capturer les variations temporelles qui affectent l'ensemble des emprunteurs, comme les changements dans le contexte macroéconomique ou les évolutions réglementaires. Cette stratégie améliore la robustesse de nos résultats en distinguant les influences exogènes des effets spécifiques aux entités étudiées.

7. Résultats du modèle à effets fixes

Cette section présente les résultats du modèle à effets fixes appliqué à l'étude de l'impact des cyberattaques sur les prêts syndiqués. Nous mettons l'accent sur les effets des cyberattaques sur le montant des prêts, la structure des prêts syndiqués et les exigences en capital des prêteurs.

7.1. Analyse des résultats de la régression : effets des cyberattaques sur les montants des prêts syndiqués

Les résultats des régressions économétriques, présentés dans le tableau 8, montrent une relation significative entre les cyberattaques et les montants des prêts syndiqués, conformément à l'hypothèse 1 de l'étude. Selon cette hypothèse, les banques ayant subi des cyberattaques tendent à accorder des montants de prêts plus faibles en raison d'une perte de confiance des investisseurs dans leur solidité financière. Les résultats confirment cette hypothèse, puisque l'indicateur de cyberattaque présente un coefficient estimé de -0,1071 ($p < 0,001$), ce qui suggère que les banques affectées par des cyberattaques réduisent le montant des prêts syndiqués de 10,71 % en moyenne. Cela reflète un impact négatif des cyberattaques sur la réputation des banques, incitant les prêteurs à ajuster leurs conditions de financement pour minimiser le risque perçu.

D'autres variables explicatives jouent également un rôle significatif dans la détermination du montant des prêts. La taille des prêteurs (Taille des prêteurs) a un effet positif sur le montant des prêts, avec un coefficient de 0,0374642 ($p < 0,001$). Cela signifie que les banques de plus grande taille ont tendance à accorder des prêts plus élevés. Ce coefficient suggère que, toutes choses égales par ailleurs, les prêteurs plus grands sont capables de proposer des montants de prêts plus importants, probablement en raison de leur solidité financière et de leur réputation plus robuste.

Le ratio de fonds propres première catégorie (Ratio de fonds propres) a également un effet positif sur les montants des prêts, avec un coefficient de 0,0130207 ($p < 0,001$). Cela suggère qu'une augmentation du ratio de fonds propres des prêteurs est associée à une augmentation significative des montants de prêts accordés. Cette relation positive indique que les prêteurs avec un capital plus élevé sont plus enclins à accorder des prêts importants, probablement en raison de leur plus grande stabilité financière.

Les autres variables, telles que le ROA des prêteurs, la valeur de marché des emprunteurs, et le refinancement, ont également montré des effets significatifs, contribuant à la variation des montants des prêts syndiqués, mais c'est principalement la cyberattaque et la taille des prêteurs qui expliquent la plus grande part de cette variation.

Ces résultats, détaillés dans le tableau 8, confirment l'hypothèse 1 et mettent en évidence que, bien que les cyberattaques aient un impact négatif sur la capacité des banques à

accorder des prêts importants, d'autres caractéristiques financières des prêteurs et des emprunteurs influencent également les montants accordés. Les prêteurs ajustent leurs engagements en fonction de l'ensemble des facteurs de risque perçus, incluant non seulement l'impact des cyberattaques, mais aussi les caractéristiques spécifiques de chaque transaction.

7.2. Analyse des résultats de la régression : effets des cyberattaques sur la structure des prêts syndiqués

Dans cette section, nous analysons l'impact des cyberattaques sur la structure des prêts syndiqués, en particulier sur le nombre de prêteurs participants. Pour ce faire, un modèle économétrique a été élaboré, où la variable dépendante est le logarithme du nombre de participants. Les résultats obtenus à partir du modèle de régression à effets fixes, présentés dans (le tableau 9), montrent un effet significatif des cyberattaques sur cette structure, mesurée par la variation du nombre de prêteurs participants.

L'hypothèse 2 postule que les cyberattaques conduisent à une réduction du nombre de participants aux prêts syndiqués, induisant une structure de financement plus concentrée. Nos résultats confirment cette hypothèse, avec un coefficient estimé de $-0,3642$ ($p < 0,001$) pour l'indicateur de cyberattaque. Cela suggère qu'après une cyberattaque, le nombre de prêteurs participants à un prêt syndiqué diminue de manière significative, ce qui peut être interprété comme une perte de confiance dans la stabilité des banques affectées, diminuant ainsi l'attractivité de ces prêts pour les investisseurs.

D'autres variables explicatives montrent également des effets significatifs sur la structure des prêts. La taille des prêteurs (Taille des prêteurs) a un effet positif sur le nombre de participants, avec un coefficient de $0,0348$ ($p < 0,001$). Cela indique que les prêteurs plus grands ou ayant une plus grande capacité financière attirent davantage de participants, possiblement en raison de leur perception comme plus sûrs ou stables. En revanche, le ratio de fonds propres première catégorie des prêteurs (Ratio de fonds propres première catégorie) a un effet négatif, avec un coefficient de $-0,0103$ ($p < 0,001$), suggérant que des prêteurs avec un capital plus élevé attirent moins de participants. Cela pourrait refléter la perception que ces prêteurs, mieux capitalisés, sont plus prudents et limitent donc le nombre de participants dans leurs prêts.

Les autres variables de contrôle, telles que le ROA des prêteurs, les actifs des emprunteurs, ainsi que la rentabilité et la valeur de marché des emprunteurs, ont également montré des effets significatifs. Le ROA des prêteurs (coefficient de $2,415$) et les actifs des emprunteurs (coefficient de $0,2515$) ont des effets positifs et significatifs, suggérant que des prêteurs plus rentables et des emprunteurs plus solides financièrement attirent davantage de participants. En revanche, la rentabilité des emprunteurs (ROA emprunteur) et la valeur de marché des emprunteurs ont des effets significatifs, bien que moins marqués.

En conclusion, les résultats confirment l'hypothèse 2 selon laquelle les cyberattaques entraînent une réduction du nombre de participants aux prêts syndiqués, suggérant ainsi une concentration accrue de la structure des prêts. Cette diminution du nombre de participants pourrait résulter de la réduction de la confiance des investisseurs, qui deviennent plus prudents après un événement de cyberattaque. En outre, des caractéristiques financières des prêteurs, comme la taille du prêteur et le ratio de fonds propres, influencent également cette structure, avec des prêteurs plus grands attirant plus de participants et ceux ayant un capital plus élevé attirant moins de participants.

7.3. Analyse des résultats de la régression : effets des cyberattaques sur le ratio de fonds propres des prêteurs

Enfin, les résultats pour l'hypothèse 3, présentés dans le Tableau 10, montrent l'impact des cyberattaques sur le ratio de fonds propres de première catégorie (Tier 1) des prêteurs dans le cadre des prêts syndiqués. Nous avons construit un modèle économétrique où la variable dépendante est le logarithme du ratio de fonds propres des prêteurs. Les résultats du modèle de régression à effets fixes, présentés dans le tableau 10, montrent un impact positif significatif des cyberattaques sur le ratio de fonds propres des prêteurs, suggérant que les cyberattaques entraînent une augmentation de ce ratio.

L'indicateur de cyberattaque présente un coefficient estimé de 8,756 ($p < 2,2e-16$), ce qui indique qu'après une cyberattaque, les prêteurs augmentent substantiellement leur ratio de fonds propres de première catégorie. Cette augmentation peut être interprétée comme une réponse des prêteurs visant à se prémunir contre les risques accrus de réputation et les pertes financières associés à de tels événements. Ainsi, les prêteurs, en augmentant leur capital, cherchent probablement à maintenir la confiance des investisseurs et à limiter leur exposition au risque perçu après une cyberattaque.

Les autres variables explicatives montrent également des effets significatifs. La taille des actifs de l'emprunteur (Log (Actifs de l'emprunteur)) a un coefficient positif de 1,751, indiquant que des emprunteurs plus grands ou plus solides financièrement entraînent une augmentation du ratio de fonds propres des prêteurs, ce qui peut refléter une plus grande sécurité pour les prêteurs dans ces cas. De plus, la garantie fournie (Nouvelle Garantie) a un effet positif, avec un coefficient de 0,2201, suggérant que la présence de garanties supplémentaires incite également les prêteurs à augmenter leur ratio de capital, afin de mieux se protéger contre les risques de réputation.

En revanche, la variable Fonds de roulement présente un coefficient négatif de -0,4720, ce qui suggère qu'un fonds de roulement plus élevé chez l'emprunteur est associé à une réduction du ratio de fonds propres de première catégorie des prêteurs. Ce résultat pourrait indiquer que les prêteurs perçoivent un emprunteur avec un fonds de roulement plus élevé comme moins risqué, réduisant ainsi la nécessité pour eux d'augmenter leur capital. Enfin, le refinancement (Refinancement) a également un effet positif sur le ratio de capital, avec

un coefficient de 0,1145, ce qui peut être vu comme un signe de prudence accrue de la part des prêteurs dans des situations de refinancement, où les risques sont souvent perçus comme plus élevés.

En conclusion, les résultats confirment que les cyberattaques ont un impact positif sur le ratio de fonds propres des prêteurs dans les prêts syndiqués. Cette augmentation des réserves de capital peut être interprétée comme une stratégie de protection contre les risques accrus de réputation et les pertes financières liés aux cyberattaques. Ces ajustements dans le capital des prêteurs sont également influencés par la taille des emprunteurs et les garanties, ainsi que par des éléments financiers comme le fonds de roulement et le refinancement.

8. Conclusion

Cette étude a examiné l'impact des cyberattaques sur la réputation des banques, en se concentrant sur les conditions de financement dans le cadre des prêts syndiqués. En utilisant une approche économétrique à effets fixes sur un échantillon de 65 863 observations provenant de 50 banques, les données de DealScan ont permis de tirer plusieurs conclusions significatives.

Les résultats montrent que les banques victimes de cyberattaques accordent des montants de prêts syndiqués plus faibles, ce qui indique une perte de confiance des prêteurs dans leur solidité financière. Cette baisse des montants de prêts accordés confirme notre hypothèse principale selon laquelle les cyberattaques entraînent une détérioration de la réputation des banques emprunteuses et chefs de file, ce qui se traduit par des conditions de financement plus strictes.

En outre, l'analyse révèle que les cyberattaques modifient la structure des prêts syndiqués en augmentant la concentration des prêteurs principaux et en réduisant le nombre de participants. Cette réduction de la diversité des prêteurs reflète une prudence accrue face au risque, affectant négativement les interactions entre banques de différentes tailles et profils.

Enfin, en cas de cyberattaques, les emprunteurs subissent une perte de réputation, car la situation demande une augmentation du capital de première catégorie des prêteurs, ce qui confirme un impact négatif sur leur perception de risque. Cela correspond à notre hypothèse supplémentaire, soulignant que les cyberattaques ne se contentent pas d'affecter les conditions immédiates des prêts, mais ont aussi des implications plus larges sur la réputation bancaire.

Cependant, notre étude présente certaines limites, notamment l'absence de prise en compte des stratégies spécifiques de gestion des risques mises en œuvre par les banques après une cyberattaque. De plus, les données disponibles sur les incidents de cybersécurité peuvent être partielles ou biaisées, ce qui pourrait affecter la précision de nos résultats.

Des recherches futures pourraient examiner les effets à long terme des cyberattaques sur la réputation bancaire et explorer l'efficacité des différentes mesures de cybersécurité pour atténuer ces impacts. Une analyse plus approfondie des politiques de gestion des risques et de la cybersécurité pourrait fournir des recommandations pratiques pour les banques cherchant à protéger leur réputation sur le marché des prêts syndiqués.

9. Bibliographie

1. Acharya, V., Eisert, T., Eufinger, C., & Hirsch, C. (2018). Real effects of the sovereign debt crisis in Europe: Evidence from syndicated loans. *Review of Financial Studies*, 31, 2855–2896.
2. Akinbowale O., & al. (2020). Analysis of cyber-crime effects on the banking sector using the balanced scorecard: A survey of literature. *Journal de la criminalité financière*, 27(3), 945-958.
3. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks in the financial sector.
4. Ali L., & al. (2017). The effects of cyber threats on customer behavior in e-banking services.
5. Amir, E., Levi, S., & Livne, T. (2019). Insider trading and disclosure: The case of cyberattacks. Available at SSRN 3355978.
6. Barakat, A., Ashby, S., Fenn, P., & Bryce, C. (2019). Operational risk and reputation in financial institutions: Does media tone make a difference? *Journal of Banking & Finance*, 98, 1-24.
7. Bayle de Jessé, M. (2019). The Eurosystem's cyber resilience strategy for financial market infrastructures. *Cyber Security: A Peer-Reviewed Journal*, 2(4), 294-302.
8. Berg, T., Saunders, A., Steffen, S., & Streit, D. (2017). Mind the gap... syndicated loan pricing puzzle revisited. *Review of Financial Studies*, 30, 948–987.
9. Bianchi, D., & Tosun, O. (2018). Cyberattacks and stock market activity. University of Warwick Unpublished working paper.
10. Boehmer, E., & W.L. Megginson (1990). Determinants of secondary market prices for developing country syndicated loans. *Journal of Finance*, 45(5), 1517–1540.
11. Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund.
12. Cebula, J. J., & Young, L. R. (2010). A taxonomy of operational cyber security risks. CMU/Software Engineering Institute, Pittsburgh, PA.
13. Chen, Y., Hu, M., & Kim, S. (2019). Cybersecurity risks in the financial sector: Implications for syndicated loans.

14. Chu, Y., Zhang, D., & Zhao, Y. E. (2019). Bank capital and lending: Evidence from syndicated loans. *Journal of Financial and Quantitative Analysis*, 54(2), 667-694.
15. Corbet, S., & Gurdgiev, C. (2020). An incentives-based mechanism for corporate cyber governance enforcement and regulation. In *Ecological, Societal, and Technological Risks and the Financial Sector* (pp. 281-307).
16. Delroy A. Chevers. (2019). The impact of cybercrime on e-banking: A proposed model.
17. Dennis, S., & D. Mullineaux (2000). Syndicated loans. *Journal of Financial Intermediation*, 9, 404–426.
18. Dupont, B. (2012). The cyber security environment to 2022: Trends, drivers, and implications.
19. Dzhaparov, P. (2020). Cyber risks – the big challenge facing banks. *Economics and Computer Science*, (1), 6-18.
20. Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). The impact of cyberattacks on financial institutions: Evidence from the 2020 cyberattack on the U.S. Federal Reserve. *Journal of Financial Stability*, 52, 100826.
21. Ferreira, M. A., & P. P. Matos. (2012). Universal banks and corporate control: Evidence from the global syndicated loan market. *Review of Financial Studies*, 25, 2703–2744.
22. Fiordelisi, F., Soana, M. G., & Schwizer, P. (2013). The determinants of reputational risk in the banking sector. *Journal of Banking & Finance*, 37(5), 1359-1371.
23. Focarelli, D., Pozzolo, A., & Casolaro, L. (2008). The pricing effect of certification on syndicated loans. *Journal of Monetary Economics*, 55(2), 235–349.
24. Fiordelisi, F., Soana, M. G., & Schwizer, P. (2014). Reputational losses and operational risk in banking. *The European Journal of Finance*, 20(2), 105-124.
25. Gennaioli, N., Shleifer, A., & Vishny, R. (2015). Neglected risks: The psychology of financial crises. *American Economic Review*, 105, 310–314.
26. Giannetti, M., & Yafeh, Y. (2012). Do cultural differences between contracting parties matter? Evidence from syndicated bank loans. *Management Science*, 58, 365–383.
27. Gogolin, F., Lim, I., & Vallascas, F. (2021). Cyberattacks on small banks and the impact on local banking markets. Available at SSRN 3823296.

28. Gopalan, R., Nanda, V., & Yerramilli, V. (2011). Does poor performance damage the reputation of financial intermediaries? Evidence from the loan syndication market. *The Journal of Finance*, 66(6), 2083-2120.
29. Grody, A. D. (2020). Addressing cyber risk in financial institutions and in the financial system. *Journal of Risk Management in Financial Institutions*, 13(2), 155-162.
30. Yildirim, İ. (2019). Gestion des risques cyber dans les banques : Assurance risque cyber. In *Global cyber security, pénurie de main-d'œuvre et risque commercial international* (pp. 38-50). IGI Global.
31. Ivashina, V. (2009). Asymmetric information effects on loan spreads. *Journal of Financial Economics*, 92(2), 300-319.
32. Iyer, S. R., Simkins, B. J., & Wang, H. (2020). Cyberattacks and impact on bond valuation. *Finance Research Letters*, 33, 101215.
33. Jamilov, R., Rey, H., & Tahoun, A. (2021). The anatomy of cyber risk (No. w28906). National Bureau of Economic Research.
34. 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.
35. Kaschner, H. (2021). *Cyber crisis management*. New York, NY: Springer Publishing.
36. Kotidis, A., & Schreft, S. (2022). Cyberattacks and financial stability: Evidence from a natural experiment.
37. Linsley, P. M., & Sharif, A. (2006). The role of reputation in the banking sector: A framework for understanding how reputation affects performance. *Journal of Financial Regulation and Compliance*, 14(3), 266-281.
38. Loan Market Association (LMA). (2018). LMA warns against damaging effect on syndicated loan markets and the broader European economy in the event of a hard Brexit, press release.
39. Mazumder M., & al. (2020). The spillover effect of the Bangladesh Bank cyber heist on banks' cyber risk disclosures in Bangladesh.
40. Malik, M. S., & Islam, U. (2019). Cybercrime: an emerging threat to the banking sector of Pakistan. *Journal of Financial Crime*, 26(1), 50-60.
41. Maskara, P. K. (2010). Economic value in tranching of syndicated loans. *Journal of Banking & Finance*, 34(5), 946–955.

42. McLennan, M. (2022). *The Global Risks Report 2022* (17th ed.). Cologny, Switzerland: World Economic Forum.
43. Michael Best, et al. (2019). *Cyber security in the banking sector*.
44. Musiał, N. (2019). Cyber risk in financial institutions: A Polish case. In *Multiple Perspectives in Risk and Risk Management: ERRN 8th European Risk Conference 2018*, Katowice, Poland, September 20-21 (pp. 301-313). Springer International Publishing.
45. Roy, N. C., & Prabhakaran, S. (2022). Sustainable response system building against insider-led cyber frauds in banking sector: a machine learning approach. *Journal of Financial Crime*, 30(1), 48-85.
46. Nguyen, L. (2022). *Cybersecurity and defending critical infrastructure*.
47. Nini, G. P. (2004). The value of financial intermediaries: Empirical evidence from syndicated loans to emerging market borrowers. *International Finance Discussion Papers*, 820. Board of Governors of the Federal Reserve System, U.S.
48. Oliver Gulyas, & al. (2022). *Cybersecurity threats in the banking sector*. IEEE, 2022. p. 1070 à 1075.
49. Perera, S., Jin, X., Maurushat, A., & Opoku, D. G. J. (2022, March). Factors affecting reputational damage to organisations due to cyberattacks. In *Informatics* (Vol. 9, No. 1, p. 28). MDPI.
50. Pollmeier, S., Bongiovanni, I., & Slapnicar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. *Safety Science*, 159, 106022.
51. Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a bank's finances. *International Journal of Current Research & Academic Review*, 2(2), 173-178.
52. Sufi, A. (2007). Information asymmetry and financing arrangements: Evidence from syndicated loans. *Journal of Finance*, 62(2), 629–668.
53. Stanikzai Q., & al. (2021). Evaluation of cyber security threats in banking systems. IEEE, 2021. p. 1 à 4.

10. Tableaux

Tableau 1: Statistiques descriptives :

Ce tableau représente les statistiques sommaires des différentes variables de notre étude qui constituent les caractéristiques de prêts, ceux des emprunteurs et ceux des prêteurs. Avec pour échantillon 65 863 observations concernant 50 différentes banques américaines octroyant des prêts syndiqués entre 2001 et 2021.

	Moyenne	Ecart- type	Min	Max	Nombre d'observations
Caractéristiques de Prêts:					
Log (montant de la transaction)	6,552	1,047	2,996	10,166	65863
Log (montant des prêts)	6,204	1,077	2,704	11,156	65863
Court terme	0,203	0,402	0,000	1,000	65863
Moyen terme	0,767	0,423	0,000	1,000	65863
Long terme	0,030	0,171	0,000	1,000	65863
Fonds de roulement	0,219	0,414	0,000	1,000	65863
Refinancement	0,863	0,344	0,000	1,000	65863
Garantie	0,284	0,451	0,000	1,000	65863
<u>Caractéristiques des</u>					
<u>emprunteurs:</u>					
Log (actifs)	22,321	1,552	18,177	27,501	65863
Log (taille)	22,321	1,552	18,177	27,501	65863
ROA EMPRUNTEUR	0,108	0,115	-1,192	2,545	65863
Valeur de Marché	1,249	9,950	0,000	847,20	65863
<u>Caractéristiques de</u>					
<u>l'arrangeur principal:</u>					
Nombre de prêteurs	15,783	8,817	2,000	80,000	65863
Taille des prêteurs	-2,070	0,329	-2,855	0,123	65863
ROA prêteurs	0,026	0,011	-0,034	0,143	65863
Log_Prêteurs_PartN	2,356	0,558	-2,659	4,075	65863

Total des prêts sur total des actifs	0,554	0,119	0,034	0,849	65863
Nombre de chefs de file	2,199	1,684	1,000	18,000	65863
Indicateur Cyberattaque	0,029	0,168	0,000	1,000	65863

Tableau 2: Coefficients de corrélation des variables.

Ce tableau présente la matrice de corrélation fournissant des coefficients de corrélation entre les différentes variables (indépendante et explicatives). Le caractère étoile (*) indique les degrés de significativité des différents coefficients : lorsqu'il est apposé *** ça signifie un seuil de 1% (0,01), ** traduit un seuil de 5% (0,05) et * explique un seuil de 10% (0,1).

	Log (montant de la transaction)	Log (montant des prêts)	Court terme	Moyen terme
Log (montant de la transaction)	1.000			
Log (montant des prêts)	0.836***	1.000		
Court terme	0.085***	0.126***	1.000	
Moyen terme	-0.078***	-0.097***	-0.915***	1.000
Long terme	-0.006	-0.055***	-0.089***	-0.320***
Fonds de roulement	-0.209***	-0.154***	-0.140***	0.141***
Refinancement	0.009*	-0.008*	-0.157***	0.150***
Garantie	-0.154***	-0.263***	-0.217***	0.152***
Log (actifs)	0.681***	0.731***	0.288***	-0.241***
Log (taille)	0.681***	0.731***	0.288***	-0.241***
ROA Emprunteur	-0.031***	-0.024***	-0.023***	0.038***
Valeur de Marché	0.011**	0.012**	-0.006	0.008*
Nombre de prêteurs	0.635***	0.627***	0.107***	-0.092***
Taille des prêteurs	0.043***	0.018***	-0.003	-0.003
ROA prêteurs	-0.187***	-0.095***	0.115***	-0.121***
Log_Prêteurs_partN	-0.541***	-0.528***	-0.052***	0.056***
Total des prêts sur total des actifs	-0.133***	-0.111***	0.065***	-0.067***

Nombre de chefs de file	0.348***	0.258***	-0.160***	0.150***
Indicateur Cyberattaque	0.144***	0.109***	-0.046***	0.040***

Tableau 3: Coefficients de corrélation des variables (suite)

Ce tableau présente la matrice de corrélation fournissant des coefficients de corrélation entre les différentes variables (indépendante et explicatives). Le caractère étoile (*) indique les degrés de significativité des différents coefficients : lorsqu'il est apposé *** ça signifie un seuil de 1% (0,01), ** traduit un seuil de 5% (0,05) et * explique un seuil de 10% (0,1).

	Long term	Takeover	Fonds de roulement	Refinancement	Garantie
Log (montant de la transaction)					
Log (montant des prêts)					
Court terme					
Moyen term					
Long term	1.000				
Fonds de roulement	-0.017** *	-0.144***	1.000		
Refinancement	-0.001	0.136***	0.061***	1.000	
Garantie	0.134** *	0.143***	0.067***	0.094***	1.000
Log (actifs)	-0.080** *	0.080***	-0.223***	-0.041***	-0.380***
Log (taille)	-0.080** *	0.080***	-0.223***	-0.041***	-0.380***
ROA Emprunteur	-0.039** *	0.030***	0.063***	-0.020***	-0.042***
Valeur de Marché	-0.007	0.001	-0.003	-0.008*	-0.013***

	-				
	0.026**				
Nombre de prêteurs	*	0.019***	-0.157***	0.122***	-0.089***
	0.014**				
Taille des prêteurs	*	0.048***	0.005	-0.000	0.034***
	0.028**				
ROA prêteurs	*	0.032***	0.085***	-0.007	-0.049***
	-				
	0.016**				
Log_Prêteurs_partN	*	-0.007	0.108***	-0.143***	0.093***
	0.014**				
Total des prêts sur total des actifs	*	0.081***	0.022***	-0.018***	-0.002
	0.007				
Nombre de chefs de file		0.060***	-0.115***	0.023***	0.029***
	-				
Indicateur Cyberattaque	0.008*	0.021***	-0.060***	-0.008*	0.002

Tableau 4: Coefficients de corrélation des variables (suite)

Ce tableau présente la matrice de corrélation fournissant des coefficients de corrélation entre les différentes variables (indépendante et explicatives). Le caractère étoile (*) indique les degrés de significativité des différents coefficients : lorsqu'il est apposé *** ça signifie un seuil de 1% (0,01), ** traduit un seuil de 5% (0,05) et * explique un seuil de 10% (0,1).

	Log (actifs)	Log (taille)	ROA Emprunteur	Valeur_de_Marché_Emprunteur
Log(montant de la transaction)				
Log (montant des prêts)				
Court terme				
Moyen terme				
Long terme				
Fonds de roulement				
Refinancement				

Garantie				
Log (actifs)	1.000			
Log (taille)	1.000***	1.000		
ROA Emprunteur	-0.155***	-0.155***	1.000	
Valeur de Marché	-0.018***	-0.018***	0.036***	1.000
Nombre de prêteurs	0.590***	0.590***	-0.062***	-0.011**
Taille des prêteurs	0.056***	0.056***	-0.047***	-0.011**
ROA prêteurs	-0.032***	-0.032***	0.034***	0.012**
Log_Prêteurs_partN	-0.523***	-0.523***	0.075***	0.015***
Total des prêts sur total des actifs	-0.090***	-0.090***	0.007	0.001
Nombre de chefs de file	0.203***	0.203***	-0.055***	-0.008*
Indicateur Cyberattaque	0.105***	0.105***	-0.036***	-0.002

Tableau 5 : Coefficients de corrélation des variables (suite)

Ce tableau présente la matrice de corrélation fournissant des coefficients de corrélation entre les différentes variables (indépendante et explicatives). Le caractère étoile (*) indique les degrés de significativité des différents coefficients : lorsqu'il est apposé *** ça signifie un seuil de 1% (0,01), ** traduit un seuil de 5% (0,05) et * explique un seuil de 10% (0,1).

	Nomb re de prête urs	Taille des prête urs	ROA PRÊTE URS	Log_Prêteurs_ partN	Total des prêts total actifs	des sur e de chefs de file	de Indicateur Cyberatta que
Log(montant de la transaction)							
Log (montant des prêts)							
Court terme							
Moyen terme							
Long terme							
Fonds de roulement							
Refinancement							
Garantie							
Log (actifs)							
Log (taille)							
ROA EMPRUNTEUR							
Valeur de Marché							
Nombre de prêteurs	1.000						
Taille des prêteurs	0.068 ***	1.000					
ROA prêteurs	0.013 **	- 0.047 ***	1.000				
Log_Prêteurs_ partN	- 0.770 ***	- 0.156 ***	-0.012**	1.000			

Total des prêts - sur total des actifs	- 0.052 ***	- 0.003	0.355***	0.049***	1.000	
Nombre de chefs de file	0.181 ***	0.031 ***	- 0.456***	-0.171***	-0.197***	1.000
Indicateur Cyberattaque	- 0.012 **	- 0.058 ***	- 0.231***	-0.032***	-0.065***	0.414** *
						1.000

Tableau 6: Test de Breusch-Pagan

Ce test permet de détecter la présence ou non de l'hétéroscédasticité des termes d'erreurs dans le modèle de régression.

Source	Somme des carres	Degré de liberté	Carré moyen
Modèle	14 585,3192	12	12 15,443267
Résidus	5 918,5714	65 850	0,089887786
Total	20 503,8906	65 862	0,311311943

Statistique	Valeur
Nombre d'observations	65 863
F (12, 65 850)	7 243,555
Prob > F	< 0,0001
Chi2 (1)	2 994,9
p-value	< 2,2e-16
R ²	0,569
R ² ajusté	0,569
Erreur standard résiduelle	0,707

Tableau 7: Test de multicollinéarité

Connu sur le nom de VIF, il est utilisé pour mesurer la multicollinéarité. Ce tableau nous présente les variances d'inflation pour chaque coefficient dans notre équation.

Variabes	VIF	1/VIF
Indicateur Cyberattaque	2.085773	0,479565
Ratio de fonds propres Tier 1	2.397120	0,417210
Log (actifs de l'emprunteur)	1.344604	0,743828
Valeur de marché de l'emprunteur	1.002172	0,997831
Refinancement	1.037417	0,914700
Taille du prêteur	1.025934	0,975287
ROA du prêteur	1.398968	0,714618
ROA de l'emprunteur	1.043666	0,958176
Garantie	1.233817	0,810621
Fonds de roulement	1.096463	0,912074

Tableau 8 : Impact des cyberattaques sur les montants des prêts syndiqués – Avec effets fixes des ‘emprunteurs’ et ‘année’

Ce tableau présente les résultats obtenus après l'application des équations de régression, utilisant la méthode des moindres carrés ordinaires (MCO) avec effets fixes. Les coefficients obtenus reflètent la relation entre les montants des prêts syndiqués et les différentes variables explicatives, notamment les indicateurs financiers des prêteurs et des emprunteurs, ainsi que l'impact des cyberattaques. Les symboles ***, **, * indiquent respectivement des niveaux de significativité statistique de 1%, 5% et 10%. L'estimateur robuste a été utilisé pour ajuster l'analyse aux éventuelles hétéroscédasticités dans les erreurs.

Variable	Coefficient	Erreur standard	t-Statistique
Indicateur Cyberattaque	-0.1070553	0.0167643	-6.3859
Taille des prêteurs	0.0374642	0.0068757	5.4488
Ratio de fonds propres première catégorie	0.0130207	0.0012253	10.6269
ROA prêteurs	-2.5330407	0.2548067	-9.9410
Log (actifs)	0.6437248	0.0074540	86.3596
ROA emprunteur	0.2532575	0.0249364	10.1561
Valeur de Marché emprunteur	0.1913309	0.0040186	47.6110
Nouvelle Garantie	0.0935929	0.0094233	9.9321
Fonds de roulement	0.0103125	0.0075221	1.3710
Refinancement	0.1248815	0.0075186	16.6097
Nombre de chefs de file	0.0334067	0.0021615	15.4551

Tableau 9 : Impact des cyberattaques sur la structure des prêts syndiqués – Avec effets fixes des prêteurs et des emprunteurs

Ce tableau présente les résultats des régressions effectuées pour analyser l'impact des cyberattaques sur la structure des prêts syndiqués, en particulier sur le nombre de participants dans les prêts. Les régressions ont été réalisées avec la méthode des moindres carrés ordinaires (MCO) et incluent les effets fixes des prêteurs et des emprunteurs. Les coefficients indiquent la direction et l'ampleur de la relation entre les variables explicatives et le nombre de participants dans les prêts. Les symboles ***, **, * indiquent respectivement des niveaux de significativité de 1%, 5% et 10%. L'estimateur robuste a été utilisé pour corriger les éventuelles hétéroscédasticités dans les erreurs.

Variable	Coefficient	Erreur standard	t-Statistique
Indicateur Cyberattaque	-0.3642189	0.01083782	-33.6063
Taille des prêteurs	0.03476441	0.00451287	7.7034
Ratio de fonds propres première catégorie	-0.0103019	0.00080721	-12.7624
ROA prêteurs	2.41515571	0.16264537	14.8492
Log (actifs)	0.25155497	0.00486556	51.7012
ROA emprunteur	0.07030445	0.01684546	4.1735
Valeur de Marché emprunteur	0.07229503	0.00265366	27.2435
Nouvelle Garantie	0.03448186	0.00624711	5.5197
Fonds de roulement	0.01919869	0.00501977	3.8246
Refinancement	0.38476237	0.00502723	76.5356

Tableau 10 : Impact des cyberattaques sur la réputation des emprunteurs via le ratio de fonds propres de première catégorie

Ce tableau présente les résultats des régressions effectuées pour analyser l'impact des cyberattaques sur la réputation des emprunteurs, mesurée par le ratio de fonds propres de première catégorie des prêteurs. Les régressions ont été réalisées en utilisant la méthode des moindres carrés ordinaires (MCO) avec des effets fixes des emprunteurs et des années. Les coefficients reflètent la direction et l'ampleur de la relation entre les variables explicatives et le ratio de fonds propres des prêteurs. Les symboles ***, **, * représentent respectivement les niveaux de significativité statistique de 1%, 5% et 10%. L'estimateur robuste a été utilisé pour contrôler les hétéroscédasticités potentielles dans les erreurs.

Variable	Coefficient	Erreur standard	t-Statistique
Indicateur Cyberattaque	8.756439	0.042757	204.7942
Log (actifs de l'emprunteur)	1.751108	0.021529	81.3386
Garantie	0.220127	0.031425	7.0048
Fonds de roulement	-0.472028	0.025008	-18.8750
Refinancement	0.114544	0.024768	4.6247