Interruption numérique prolongée : quels enjeux pour le secteur financier ?
Janvier 2026

FICHE SCÉNARIO — INTERRUPTION NUMERIQUE PROLONGEE

Résumé

La présente fiche explore les conséquences pour la place financière française et le Groupe de Place Robustesse (GPR) d'une interruption numérique prolongée (supérieure à 24 heures).

Description de la menace

La Place financière est aujourd'hui dépendante de la disponibilité continue de réseaux (Internet, voix, mobile) et de l'accès à des solutions-clés opérées par des prestataires extérieurs (cloud, messagerie, authentification, outils collaboratifs). **Cette dépendance est structurelle et croissante**, portée par la dématérialisation intégrale des opérations et la concentration de nombreux services stratégiques entre les mains d'un nombre réduit d'*hyperscalers*, principalement américains. **Le contexte géopolitique** (cyber-hostilités étatiques, fragmentation technologique) **et climatique** (tempêtes, incendies, inondations, affectant data centers et réseaux fibre) renforce la plausibilité d'une telle coupure.

Matérialité et impacts sur la Place financière et le GPR

Comme dans le cas d'une interruption électrique (cf. fiche dédiée), un incident d'ampleur – panne télécom massive, attaque cyber sur des infrastructures critiques, indisponibilité d'un grand fournisseur cloud… – pourrait **affecter simultanément l'ensemble des processus financiers critiques** : marchés, paiements de détail et de gros montants, gestion de liquidité, accès aux données, etc. À très court terme, **les premiers impacts** pour les établissements, infrastructures et autorités membres du GPR **concerneraient les personnes** (capacité des collaborateurs à travailler sans outils numériques) **et la communication**, condition essentielle au maintien du pilotage de crise.

Interruption numérique prolongée : quels enjeux pour le secteur financier ?

Groupe de Place Robustesse – Banque de France
Groupe de travail « Panorama de la menace »

Avertissement

La présente note est le fruit de travaux menés au sein du Groupe de travail « Panorama de la menace » du GPR. Les échanges et contributions des membres du groupe de travail ont constitué un socle déterminant pour l'élaboration des constats et propositions présentés dans ce document.

Les analyses et conclusions présentées dans cette note n'engagent que leurs auteurs et ne reflètent pas nécessairement les positions des organisations auxquelles les contributeurs sont affiliés.

Date

Janvier 2026

1. Description de la menace

1.1 Définitions et périmètre retenu

Dans le cadre de ces travaux, le terme « **interruption numérique** » recouvre **toute perte partielle ou totale d'accès aux infrastructures numériques critiques (réseaux télécoms, data centers, solutions cloud, services numériques tiers…) sur une zone géographique donnée ou pour une communauté d'utilisateurs**.

Deux formes ont été retenues comme prioritaires pour cette analyse, en raison de leurs impacts potentiels pour la continuité des activités financières :

- **La perte prolongée (>24 heures) d'accès aux réseaux de télécommunications** (voix et données, y compris 3G/4G/5G et accès fixe) ;
- **La perte prolongée (>24 heures) d'accès aux services numériques critiques fournis par des prestataires externes**, incluant notamment les services cloud (IaaS/PaaS/SaaS), la messagerie, les solutions d'authentification et les plateformes collaboratives.

Ce double périmètre reflète les deux vecteurs de rupture jugés les plus pertinents pour le secteur financier : l'un affectant la capacité à communiquer, l'autre touchant directement l'exécution opérationnelle et le traitement des données.

1.2 Évaluation du risque d'interruption numérique en France

L'exposition du secteur financier au risque d'interruption numérique découle d'un ensemble de facteurs structurels et conjoncturels qui définissent la manière dont les institutions conçoivent, opèrent et sécurisent leurs activités numériques. Ces facteurs forment un **ensemble de déterminants qui rendent un épisode d'interruption numérique plausible en France.**

Sur le plan structurel, le premier facteur déterminant réside dans la numérisation quasi-intégrale des activités financières. La plupart des opérations bancaires, de marché ou de paiement reposent désormais sur des systèmes informatiques interconnectés et sur des échanges en temps réel, ce qui accentue la dépendance à la disponibilité continue des réseaux et des services informatiques. Pour le Financial Stability Board (2022)[1], la pandémie de COVID-19 a accéléré cette mutation, rendant les services financiers plus agiles mais aussi plus sensibles aux pannes informatiques et aux cyberattaques.

De plus, **la croissance rapide des besoins numériques** — alimentée par la hausse des volumes de traitement, l'essor du cloud et le développement de l'intelligence artificielle — exerce une pression croissante sur les infrastructures physiques (data centers, câbles sous-marins, réseaux de transport de données). Cette dynamique d'expansion crée un environnement en constante évolution, dans lequel les capacités doivent être régulièrement renforcées pour absorber la hausse de la demande.

Le deuxième facteur tient à l'externalisation croissante vers des prestataires spécialisés, qu'il s'agisse d'opérateurs de cloud, de fournisseurs de messagerie ou de solutions d'authentification. Le secteur financier dépend aujourd'hui d'un écosystème complexe de prestataires tiers couvrant la quasi-totalité de ses fonctions critiques — de la communication interne à la gestion des paiements, de la cybersécurité à la

[1] Financial Stability Board, FinTech and Market Structure in the COVID-19 Pandemic - Implications for financial stability, 21 March 2022 - https://www.fsb.org/uploads/P210322.pdf

conformité réglementaire. De plus, un nombre restreint d'acteurs mondiaux assure aujourd'hui l'hébergement et la fourniture d'une part très importante des services essentiels utilisés par le secteur financier. Cette concentration crée un risque de dépendance collective : une défaillance unique peut avoir un effet systémique, du fait de l'homogénéité des prestataires utilisés dans tout le secteur.

L'incident mondial lié à une mise à jour défectueuse de **la solution de cybersécurité CrowdStrike en 2024**[2] en a fourni une illustration saisissante : en quelques heures, des millions de postes de travail ont été rendus inopérants dans des secteurs critiques, y compris la finance, les transports et la santé. L'incident a illustré le risque inhérent aux défaillances de solutions de sécurité ou de composants logiciels diffusés à large échelle.

Un enjeu connexe majeur est celui de **la souveraineté numérique**[3], ces acteurs tiers étant pour la plupart non européens, principalement américains. Cette dépendance crée ainsi une asymétrie stratégique, la continuité et la confidentialité des activités critiques du secteur reposant sur des prestataires soumis à des juridictions étrangères[4]. Au-delà du risque juridique, cette dépendance pose un enjeu de maîtrise technologique et d'autonomie décisionnelle : en cas de tension géopolitique ou de mesures coercitives unilatérales, l'accès à des services essentiels pourrait être compromis ou soumis à des conditions extérieures au cadre européen.[5]

Un troisième facteur structurel réside dans l'interdépendance des systèmes critiques. Les infrastructures télécoms, énergétiques et numériques sont en effet étroitement liées : un incident sur le réseau électrique peut compromettre le fonctionnement des data centers ; une panne de télécommunications peut empêcher l'accès à des systèmes cloud ; une défaillance logicielle peut paralyser des équipements physiques. Ces chaînes d'interdépendance accroissent le risque d'effet domino et complexifient la gestion de crise.

La vague de froid exceptionnelle ayant frappé le Texas en février 2021 a provoqué une panne massive du réseau électrique, entraînant la mise à l'arrêt de centres de données, d'antennes mobiles et de réseaux de télécommunication. Plusieurs services bancaires, distributeurs et plateformes de paiement ont été rendus inaccessibles pendant plusieurs jours. Cet épisode illustre concrètement la vulnérabilité en chaîne entre les infrastructures énergétiques, télécoms et numériques, une défaillance sur un maillon critique pouvant rapidement paralyser l'ensemble du système.

Sur le plan conjoncturel, l'intensification des tensions géopolitiques et la montée en puissance des menaces cyber exposent directement les infrastructures numériques. Les dernières années ont montré

[2] https://www.cert.ssi.gouv.fr/actualite/CERTFR-2024-ACT-032/

[3] Le rapport du Conseil de l'Union européenne sur la sécurité économique (2023) définit la souveraineté numérique comme la « capacité de l'Union à agir de manière indépendante dans le cyberespace, à protéger ses infrastructures critiques et à garantir la maîtrise de ses données ».

[4] Le Clarifying Lawful Overseas Use of Data Act (CLOUD Act), adopté par les États-Unis en 2018, autorise les autorités judiciaires américaines à contraindre les entreprises de droit américain à fournir des données stockées à l'étranger. Selon la Commission européenne (Communication « A European Strategy for Data », COM(2020) 66), plus de 90 % des données industrielles européennes sont hébergées par des prestataires basés aux États-Unis.

[5] L'ENISA (European Union Agency for Cybersecurity), dans son Threat Landscape Report 2022, identifie la concentration des services cloud auprès de trois fournisseurs américains (AWS, Microsoft Azure, Google Cloud) comme un risque de dépendance stratégique. Le récent blocage des accès aux services Microsoft du président de la Cour Pénale Internationale a pu montrer les conséquences directes d'une telle dépendance (cf. La Cour pénale internationale abandonne Microsoft pour une solution européenne, après les tensions répétées avec l'administration Trump)

que les réseaux satellitaires, les câbles sous-marins et les opérateurs d'infrastructures peuvent devenir des cibles stratégiques.

L'attaque par wiper menée contre le réseau KA-SAT de Viasat en février 2022, à la veille de l'invasion de l'Ukraine, a entraîné la mise hors service de dizaines de milliers de modems satellites en Europe, illustrant la capacité d'une action ciblée à produire des effets géographiques étendus. De même, plusieurs ruptures de câbles sous-marins dans la mer Baltique ou en mer Rouge en 2023- 2024, parfois d'origine malveillante, ont mis en évidence la vulnérabilité physique de ces infrastructures vitales pour la connectivité internationale.

Enfin, le changement climatique constitue un facteur aggravant. L'augmentation de la fréquence et de l'intensité des événements extrêmes — tempêtes, inondations, canicules — expose directement les infrastructures physiques : inondation de sites d'hébergement, surchauffe des data centers, rupture de câbles aériens, incendies liés à des surcharges électriques. Ces événements peuvent causer des interruptions prolongées, parfois sur plusieurs jours, malgré les dispositifs de redondance et de sauvegarde.

Le risque d'interruption numérique prolongée s'inscrit donc dans une dynamique où les aléas naturels, techniques et humains tendent à se conjuguer. Sa probabilité de survenue justifie une approche collective et prospective pour le renforcement de la résilience du secteur.

2. Impacts sur le secteur financier[6]

2.1. Matérialité[7] du risque d'interruption numérique pour le secteur financier

Dans cette fiche, **les impacts sont évalués à partir d'un scénario d'interruption numérique prolongée — supérieure à 24 heures — affectant une zone étendue (échelle régionale ou nationale).**

La matérialité du risque d'interruption numérique pour le secteur financier est élevée. La quasi-totalité des opérations financières — paiements, marché, post-marché, reporting réglementaire, contrôle des risques, décisionnel interne — repose sur l'accès à des infrastructures numériques distribuées et interconnectées. Une perte d'accès aux réseaux télécoms prive immédiatement les organisations de leur capacité à coordonner leurs opérations, tandis qu'une indisponibilité des services numériques tiers empêche l'accès à certains systèmes applicatifs critiques, emportant un risque de paralysie rapide.

Les incidents récents — CrowdStrike (2024), Amazon Web Services (2025)[8], Microsoft Azure (2025)[9], défaillances de Slack, Teams ou Salesforce (2022-2024) — démontrent qu'une indisponibilité massive peut

[6] L'analyse menée privilégie l'évaluation de l'impact net, c'est-à-dire des conséquences résiduelles après activation des mesures de contingence. Cette approche permet d'identifier précisément les lacunes de couverture et les efforts prioritaires de renforcement à mener.
[7] La matérialité du risque renvoie à son potentiel d'impact significatif et durable sur le fonctionnement d'un secteur. Dans le cas du secteur financier, un risque est dit matériel lorsqu'il est susceptible de produire des conséquences substantielles sur la continuité d'activité, la réputation ou la stabilité financière dans son ensemble.
[8] https://www.franceinfo.fr/internet/snapchat-signal-zoom-l-acces-a-de-nombreux-sites-perturbe-en-raison-d-une-panne-du-service-de-cloud-d-amazon_7564207.html
[9] https://www.lemonde.fr/pixels/article/2025/10/29/microsoft-azure-deuxieme-plateforme-cloud-au-monde-touche-par-une-panne_6650216_4408996.html

se diffuser mondialement en quelques minutes à cause du modèle SaaS centralisé. Ces précédents renforcent l'hypothèse d'un événement global, affectant simultanément plusieurs institutions, sans distinction géographique.

2.2. Impacts pour le secteur financier

Une interruption numérique prolongée affecterait l'ensemble des processus critiques du secteur financier. Les systèmes de paiement, les plateformes de marché, la gestion de la liquidité, les activités de conformité, les infrastructures de sécurité et la relation client reposent tous sur l'accès aux télécommunications et aux services numériques.

Comme dans le cas d'une interruption électrique, **les deux impacts immédiats et transverses sont :**

- **Les personnes (organisation du travail et continuité humaine) :** une perte d'accès à la messagerie, aux annuaires, aux VPN ou aux solutions d'authentification rend le travail collaboratif immédiatement difficile. En quelques heures, l'organisation interne se fragmente, et la chaîne décisionnelle s'affaiblit, même si les infrastructures techniques restent partiellement disponibles.
- **La communication interne et externe** : sans réseaux télécoms, la cellule de crise ne peut plus coordonner la réponse opérationnelle, transmettre des consignes ou escalader les incidents. Sans accès aux solutions collaboratives (Teams, Zoom, Outlook), les mécanismes d'information traditionnels se figent. L'impact le plus aigu survient donc non sur la technique elle-même, mais sur la capacité collective à agir**.**

À l'inverse d'une interruption électrique qui désactive l'ensemble des infrastructures, une interruption numérique peut laisser une partie du système fonctionnelle mais inutilisable, faute de coordination. **Le risque clé n'est donc pas seulement la panne, mais la désorganisation qu'elle entraîne**.

L'entrée en application **du règlement européen DORA (Digital Operational Resilience Act)**[10] en 2025 marque une évolution majeure dans la gestion des risques numériques du secteur financier.

Ce texte impose à l'ensemble des institutions financières — banques, assurances, infrastructures de marché, prestataires de services de paiement — un **niveau homogène et élevé de résilience opérationnelle**, incluant des exigences strictes en matière de gestion de crise, de continuité d'activité, de tests de résilience informatique (TLPT) et de cartographie des dépendances critiques.

De plus, DORA introduit pour la première fois **un cadre de supervision directe des prestataires tiers critiques (Critical ICT Third-Party providers - CTPPs),** en particulier les grands fournisseurs cloud et de services IT, dont l'interruption pourrait avoir un effet systémique.

Ce cadre offre une première base structurante de sécurisation, mais il ne supprime pas le risque : en cas de défaillance simultanée ou prolongée touchant plusieurs CTPPs, la capacité du secteur financier à maintenir ses fonctions essentielles dépendra encore largement de ses propres mécanismes de continuité et de l'efficacité des protocoles de coordination de Place.

[10] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R2554