Risques géopolitiques : Quels impacts sur le risque opérationnel des banques ?

Entre la guerre russo-ukrainienne, les cyberattaques étatiques, la rivalité entre les États-Unis et la Chine, les annonces des droits de douane sur les importations par les États-Unis ou encore les instabilités au Moyen-Orient ; le monde évolue désormais dans un contexte marqué par des **tensions géopolitiques**. Ces tensions affectent les banques à travers le risque de crédit, le risque de marché, le risque de liquidité et de financement, le risque de modèle d'activité, le risque de gouvernance et avant tout **le risque opérationnel** et la **résilience** qui déterminent leur capacité à traverser ces crises.

La résilience des banques face aux risques géopolitiques : une priorité majeure pour la BCE

La BCE alerte : l'endettement public pourrait réduire la capacité des États à soutenir les banques en cas de crise ; comme cela avait été possible lors du Covid-19 ; renforçant l'enjeu de résilience. Dans sa publication du 18 novembre 2025 définissant ses priorités pour les années 2026-2028, la BCE place la résilience des banques face aux risques géopolitiques comme la **1ère priorité majeure**. Elle prévoit également, dans son communiqué de presse du 12 décembre 2025, d'évaluer 110 banques sous sa supervision directe, représentant près de 75 % des actifs du système bancaire européen, sur leur capacité à résister aux chocs géopolitiques dans le cadre d'un **stress test inversé**. Les banques devront définir des scénarios géopolitiques pouvant conduire à une diminution d'au moins 300 points de base de leurs fonds propres de catégorie 1 (CET1).

Chocs géopolitiques : quels impacts sur le risque opérationnel des banques ?

Les tensions géopolitiques dépassent aujourd'hui le seul cadre macroéconomique. Elles exposent les banques à des risques opérationnels, impactant leur **continuité d'activité** et leur **résilience**. Trois principaux risques opérationnels sont identifiés :

Les risques cyber : Les banques sont des cibles stratégiques de cyberattaques et de cybermenaces orchestrées par des États. Ces attaques visent à perturber les infrastructures, espionner et exercer des pressions économiques, pouvant entraîner des pertes financières et un impact réputationnel négatif. Un exemple récent, l'attaque contre Jaguar Land Rover (JLR), filiale de Tata Motors Passenger Vehicles cotée en Inde, montre qu'un incident cyber peut affecter directement ses résultats et son cours boursier. Le 31 août 2025, JLR a subi une cyberattaque qui a stoppé la production dans 3 usines britanniques, avec retour à la normale mi-novembre. Au T3 2025, cet arrêt a fait chuter les ventes en gros de -43% (59 200 véhicules) et au détail de -25% (79 600 unités) par rapport au T3 2024 (publication JLR du 5 janvier 2026). Le 6 janvier, au lendemain de la publication, la capitalisation de Tata Motors Passenger Vehicles a chuté de 4% (MoneyControl et investing.com). Au T4 2025, les ventes rebondissent (+61% pour les ventes en gros et +16% pour les ventes en détail vs. T3 2025) mais restent en retrait par rapport au T4 2024 (-14 %) (publication JLR du 6 avril 2026). Selon Cyber Monitoring Center, il s'agit de la cyberattaque la *« plus dommageable financièrement jamais arrivée au Royaume-Uni »* coûtant environ 1,9Md£ (2,5Md€) à l'économie britannique et perturbant plus de 5000 organisations.

Ainsi, la résilience numérique, renforcée en Europe par DORA (*Digital Operational Resilience Act*) depuis le 17 janvier 2025, est essentielle face aux tensions géopolitiques compte tenu des impacts opérationnels, financiers, réputationnels et sur la confiance des investisseurs.

Les risques liés aux tiers : Les banques dépendent de prestataires externes (IT, cloud, services), ce qui peut entraîner des restrictions d'accès aux technologies, aux marchés et aux services, notamment lorsque ces prestataires sont situés dans des zones instables. Depuis février 2026, les tensions autour du détroit d'Ormuz, où passe près de 20% du pétrole mondial et du gaz naturel liquéfié (selon l'Agence internationale de l'Énergie), illustrent ce risque de tiers. Ces tensions ont entraîné une hausse du prix de l'énergie, des retards dans les chaînes d'approvisionnement et des surcoûts dans la logistique. Ces perturbations touchent les fournisseurs de services dont dépendent les banques impactant leur risque opérationnel, mais pas seulement. On pourra citer le risque de crédit, et autres risques financiers.

Les risques de non-conformité : Les évolutions géopolitiques entraînent des mises à jour fréquentes des listes officielles (sanctions, registre des gels des avoirs, Personnes Politiquement Exposées, restrictions sectorielles, etc.) exposant les banques à un risque de non-conformité si leurs listes internes et leur système de filtrage ne sont pas actualisés. Chaque nouveau paquet de sanctions entraîne des mises à jour des listes de surveillance. Par exemple le 19ème paquet adopté en octobre 2025 contre la Russie a conduit à 69 nouvelles inscriptions sur la liste des gels des avoirs, des restrictions renforcées contre les entreprises énergétiques russes finançant la guerre, l'interdiction de transactions avec 5 banques russes et l'ajout de 45 entités de pays tiers participant au contournement des sanctions (communiqué de presse du Conseil de l'UE du 23 octobre 2025).

Risque opérationnel et géopolitique : Implications prudentielles et attentes du superviseur

Quels sont les points de vigilance pour le calcul du risque opérationnel selon SMA ?

Les autorités de surveillance accorderont une attention particulière à l'implémentation de la méthode SMA *(Standardised Measurement Approach)* pour le calcul des exigences de fonds propres conformément au paquet CRR III/CRD VI, en application depuis le 1er janvier 2025. Pour le risque opérationnel, l'attention portera notamment sur le ***Loss Component*** (basé sur les pertes opérationnelles historiques sur 10 ans) ; tandis que des revues ciblées et des OSI (*On-Site Inspections*) vérifient la fiabilité des données comptables utilisées pour le ***Business Indicator***, garantissant que le capital réglementaire couvre correctement le risque opérationnel.

Risque opérationnel et capitalisation sous CRRIII / CRD VI

Les tensions géopolitiques accroissent l'exposition des banques aux risques opérationnels (par exemples liés aux cyberattaques, sanctions, défaillance de tiers, etc.) en augmentant les pertes opérationnelles. La hausse du risque opérationnel augmente alors le RWA *(Risk-Weighted Assets)*, diminuant en conséquence le ratio CET1 *(Common Equity Tier 1)* pour un niveau de capital CET1 constant, réduisant ainsi la solvabilité des banques.

Par exemple, en mars 2026, Citigroup et HSBC ont fermé des agences aux Émirats arabes unis en raison de la guerre américano-israélienne contre l'Iran. Ces fermetures génèrent des coûts : coûts de continuité d'activité (bascule sur des canaux alternatifs), coûts liés aux ressources humaines et à la sécurité (évacuation, protection du personnel), coûts liés aux interruptions de services (transactions non exécutées et pénalités contractuelles) ; augmentant le Loss Component, le RWA opérationnel et exerçant une pression à la baisse du ratio CET1.

Intégration des tests inversés dans ICAAP

Les tests de résistance inversés sur le risque géopolitique seront menés dans le cadre de l'ICCAP (*Processus Interne d'Evaluation de l'Adéquation du Capital*) 2026 des banques. Sans impact direct sur les exigences de fonds propres (P2R) et les recommandations (P2G), ces tests apportent des éléments qualitatifs pour l'évaluation l'ICAAP et le SREP *(Supervisory Review and Evaluation Process)*.

Notre vision : Renforcer la résilience des banques face aux risques géopolitiques

Les banques doivent d'abord **cartographier leurs risques géopolitiques** et en évaluer leur criticité à partir de scénarios d'experts, afin de prioriser les dispositifs de contrôle à déployer (tels que la cartographie des tiers, l'analyse de la chaîne d'approvisionnement et du risque de concentration, indicateurs de risques géopolitiques). Les contrôles peuvent ensuite **être renforcés par l'Intelligence Artificielle.** Par exemple, pour les contrôles de transaction, le machine learning permet une détection plus intelligente et dynamique en priorisant des alertes et en réduisant les faux positifs. Couplé au NLP *(Natural Language Processing)*, il garantit une veille et un filtrage continuellement actualisés.

Il est aussi essentiel de **renforcer la mesure du *Loss Component* et du RWA opérationnel** via une exploitation des incidents historiques liés à des chocs géopolitiques (tels que cyberattaques, défaillances de prestataires, interruptions de systèmes opérationnels). Cette approche invite toutefois **à s'interroger sur la capacité des données historiques à refléter pleinement des risques géopolitiques émergents.** Les risques géopolitiques sont corrélés aux risques cyber et aux risques liés à l'IA, un triptyque qu'il convient de quantifier conjointement. Cette réflexion alimente déjà notre démarche de quantification des besoins en fonds propres pour les risques cyber.

Enfin, au-delà des enjeux opérationnels, c'est toute la **stratégie qui doit évoluer** : adaptation des modèles opérationnels, réallocation d'investissement, réorganisation de la chaîne d'approvisionnement et renforcement du plan de continuité d'activité (systèmes/sites de repli, diversification géographique, tests réguliers de résistance. L'enjeu est clair : préserver la solvabilité dans un environnement devenu instable**.**