NEXIALOG
CONSULTING

RISQUES GÉOPOLITIQUES :

QUELS IMPACTS SUR LE RISQUE OPÉRATIONNEL DES BANQUES ?

JUIN 2026

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 la résilience des banques à travers le risque de crédit, le risque de marché, le risque de modèle d'activité, le risque de gouvernance et avant tout le risque opérationnel.

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 à l'instar des mesures prises durant le 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 catégories 1 (CET1). Pour aller plus loin, notre one pager dédié « Risque géopolitique » détaille les principes de ce stress test inversé présenté dans ce communiqué de presse de la BCE du 12 décembre 2025.

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 établissements bancaires constituent des cibles stratégiques pour des cyberattaques, souvent menées ou soutenues par des États. Ces offensives visent à perturber les infrastructures, à collecter des informations sensibles ou encore à exercer des pressions économiques, avec à la clé des pertes financières et des atteintes à la réputation.

L'exemple de La Banque Postale est particulièrement révélateur. Le 22 décembre 2025, l'établissement a été la cible d'une attaque par déni de service distribué DDoS (Distributed Denial of Service) menée par des hackers pro-russes rendant le site internet et l'application mobile indisponibles pendant plusieurs jours.

Cette perturbation a affecté les paiements, l'accès aux comptes et les services clients. Une seconde attaque, survenue le 1er janvier 2026, a entraîné à nouveau une indisponibilité des services en ligne. Toutefois, ces incidents n'ont entraîné « aucune intrusion, aucune altération, aucune fuite de données », aucune volonté de « pénétrer nos systèmes internes » (Zakari Moursli, Directeur général adjoint de la Banque Postale, Cyberattaque contre La Banque Postale, le 22/01/2026). Ces événements soulèvent des interrogations quant à leurs motivations : sont-elles purement malveillantes ou à caractère politique ? Ces attaques mettent en lumière la vulnérabilité d'un acteur central du service public français, avec des répercussions sur l'ensemble de l'écosystème du Groupe La Poste (Colissimo, Digiposte, services en ligne de La Banque Postale).

Un autre cas marquant concerne Jaguar Land Rover (JLR), filiale de Tata Motors cotée en Inde. Le 31 août 2025, une cyberattaque a entraîné l'arrêt de la production dans trois usines britanniques, avec un retour à la normale seulement à la mi-novembre. Les conséquences ont été significatives : au troisième trimestre 2025, les ventes en gros ont chuté de 43 % (59 200 véhicules) et les ventes au détail de 25 % (79 600 unités) par rapport à la même période en 2024. À la suite de la publication de ces résultats, le 6 janvier, la capitalisation de Tata Motors Passenger Vehicles a reculé de 4% (MoneyControl et investing.com). Si une reprise est observée au quatrième trimestre 2025 (+61% pour les ventes en gros et +16% pour les ventes

en détail par rapport au trimestre précédent) les niveaux restent inférieurs à ceux du quatrième trimestre 2024 (-14 %) (publication JLR du 6 avril 2026). Selon Cyber Monitoring Center, cet épisode constitue une 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.

Dans ce contexte, ces incidents illustrent le caractère crucial de la résilience numérique. Celle-ci a été renforcée en Europe par Digital Operational Resilience Act (DORA), entré en application le 17 janvier 2025. Face à des tensions géopolitiques qui amplifient le risque opérationnel, les enjeux sont multiples : financiers, réputationnels, mais aussi liés à la continuité d'activité et à la confiance des investisseurs.

LES RISQUES LIÉS AUX TIERS

Les banques dépendent fortement de prestataires externes pour leurs services, leurs données et leurs infrastructures technologiques (centres de services externalisés, fournisseurs IT, acteurs du cloud). Cette dépendance les expose à plusieurs vulnérabilités : restrictions d'accès aux ressources technologiques, limitations d'accès à certains marchés ou encore indisponibilité de prestataires situés dans des zones géopolitiquement instables.

Les tensions observées depuis février 2026, autour du détroit d'Ormuz, par lequel transite près de 20% du pétrole mondial et du gaz naturel liquéfié (selon l'Agence internationale de l'Énergie), illustrent concrètement ce risque. Elles ont provoqué une hausse du prix de l'énergie, des perturbations dans les chaînes d'approvisionnement ainsi que des surcoûts logistiques. Ces déséquilibres affectent directement les prestataires de services dont dépendent les banques, renforçant ainsi leur exposition au risque opérationnel.

Bien que cette analyse se concentre sur ce dernier, ces tensions ont également des répercussions sur d'autres types de risques, notamment le risque de crédit. En effet, pour les entreprises fortement dépendantes de l'énergie ; l'augmentation des prix pèse sur les marges, alourdit les coûts d'exploitation et fragilise la trésorerie. Cela détériore leur solvabilité et leur capacité de remboursement, ce qui accroît mécaniquement le risque de crédit pour les établissements bancaires. À lire aussi, un article dédié qui analyse l'impact des risques géopolitiques au-delà du risque opérationnel.

LES RISQUES DE NON-CONFORMITÉ

Les évolutions géopolitiques s'accompagnent des mises à jour fréquentes des cadres réglementaires, notamment des listes officielles (sanctions, gels des avoirs, personnes politiquement exposées, restrictions sectorielles, etc.). Les banques s'exposent à un risque de non-conformité si leurs dispositifs internes — bases de données et systèmes de filtrage — ne sont pas actualisés en continu.

Chaque nouveau paquet de sanctions illustre cet enjeu. Le 19e paquet adopté en octobre 2025 contre la Russie a, par exemple, entraîné l'ajout de 69 entités à la liste des gels d'avoirs, le renforcement des restrictions visant les entreprises énergétiques finançant la guerre, l'interdiction de transactions avec cinq banques russes et l'intégration de 45 entités de pays tiers impliquées dans le contournement des sanctions (communiqué de presse du Conseil de l'UE du 23 Octobre 2025). Par ailleurs, un 20e paquet a été annoncé le 6 février 2026 à Bruxelles par Ursula von der Leyen.

Dans ce contexte, l'intelligence artificielle constitue un levier clé pour assurer une mise à jour continue et automatisée des dispositifs de conformité.

RISQUE OPÉRATIONNEL ET GÉOPOLITIQUE : IMPLICATIONS PRUDENTIELLES ET ATTENTES DU SUPERVISEUR

COMMENT MESURER LE RISQUE OPÉRATIONNEL SELON BÂLE ?

La mesure du risque opérationnel repose désormais sur la méthode SMA (Standardised Measurement Approach), définie par le Comité de Bâle, appelée à devenir l'unique approche pour le calcul du capital réglementaire minimal.

Elle combine deux composantes :

- le Business Indicator (BI), fondé sur le compte de résultat ;
- le Loss Component (LC), basé sur les pertes opérationnelles historiques sur une période de dix ans.

Les autorités de surveillance porteront une attention particulière à l'implémentation de la méthode SMA pour le calcul des exigences de fonds propres conformément au paquet CRR III/CRD VI, en application depuis le 1er janvier 2025. L'accent sera notamment mis sur la fiabilité du Loss Component, tandis que des inspections sur site (On-Site Inspections) viendront contrôler la qualité des données utilisées pour le Business Indicator, afin de garantir une couverture adéquate du risque opérationnel.

RISQUE OPÉRATIONNEL ET CAPITALISATION (CRR III / CRD VI)

Le risque opérationnel est défini par le Comité de Bâle comme « le risque de pertes résultant de processus internes inadéquats ou défaillants, de personnes, de systèmes ou d'événements externes ». Le risque géopolitique, en tant que facteur externe, contribue directement à son augmentation via les pertes opérationnelles observées.

Dans ce contexte, les tensions géopolitiques renforcent l'exposition des banques aux incidents opérationnels (cyberattaques, sanctions, défaillance de tiers, etc.) , ce qui se traduit par une hausse des pertes. Cette augmentation alimente le niveau des actifs pondérés par les risques RWA (Risk-Weighted Assets), et, à capital constant, exerce une pression à la baisse sur le ratio CET1(Common Equity Tier 1), affaiblissant ainsi la solvabilité des établissements.

À titre d'illustration, en mars 2026, Citigroup et HSBC ont décidé de fermer temporairement certaines agences aux Émirats arabes unis en raison du conflit opposant les États-Unis et Israël à l'Iran. Ces fermetures alimentent le Loss Component : 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). Ces éléments sont intégrés dans les scénarios internes de pertes opérationnelles, conduisant à une hausse du RWA opérationnel et une pression à la baisse du ratio CET1 pour un niveau de capital CET1 constant.

INTÉGRATION DES TESTS INVERSÉS DANS ICAAP

Dans le cadre de leur ICAAP (Processus Interne d'Evaluation de l'Adéquation du Capital) 2026, les banques devront intégrer des tests de résistance inversés portant sur des scénarios géopolitiques. L'objectif est d'identifier des situations extrêmes plausibles, d'en mesurer les impacts, de définir des mesures de prévention et de remédiation, et de s'assurer de la robustesse du dispositif de gouvernance et de résilience opérationnelle.

Bien que ces exercices n'aient pas d'impact direct sur les exigences en fonds propres (P2R) ni sur les recommandations prudentielles (P2G), ils enrichissent l'analyse qualitative dans le cadre du processus SREP (Supervisory Review and Evaluation Process).

NOTRE VISION : RENFORCER LA RÉSILIENCE FACE AUX RISQUES GÉOPOLITIQUES

- Cartographier précisément les expositions géopolitiques propres à chaque banque et en évaluer la criticité à partir de scénarios experts, afin de prioriser les dispositifs de contrôle (analyse des tiers, chaînes d'approvisionnement, risques de concentration, indicateurs dédiés, etc.).
- Mobiliser l'intelligence artificielle pour améliorer les contrôles : les modèles de machine learning permettent d'optimiser la détection des transactions à risque, de prioriser les alertes et de réduire les faux positifs. Couplés à des technologies de traitement du langage naturel (NLP-Natural Language Processing), ils facilitent l'intégration continue des mises à jour des listes de surveillance, garantissant une veille et un filtrage continuellement actualisés.

- Renforcer l'analyse des pertes opérationnelles historiques et leur traduction en capital réglementaire : l'étude des incidents passés liés à des chocs géopolitiques permet d'alimenter le Loss Component pour le calcul du RWA. Elle pose toutefois la question de la capacité des données historiques à refléter des risques émergents, notamment à l'intersection des risques géopolitiques, cyber et 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.

- Intégrer pleinement les risques cyber dans un contexte géopolitique, en cohérence avec le règlement européen Digital Operational Resilience Act(DORA).

- Répondre aux attentes des superviseurs, notamment via la mise en œuvre de reverse stress tests géopolitiques et l'application des exigences de capital prévues par CRR III / CRD VI.

- Activer des leviers stratégiques : réallocation des investissements, adaptation des modèles opérationnels, diversification géographique, sécurisation des chaînes d'approvisionnement et renforcement des plans de continuité d'activité (sites de repli, diversifications géographiques, tests réguliers de résistance).

BIBLIOGRAPHIE

Banque de France : La BCE va évaluer la capacité des banques à intégrer le risque géopolitique dans leurs tests de résistance | Banque de France
https://www.banque-france.fr/fr/communiques-de-presse/la-bce-va-evaluer-la-capacite-des-banques-integrer-le-risque-geopolitique-dans-leurs-tests-de

Banque Centrale Européennes – Supervision bancaire : Limiter les effets du risque géopolitique
https://www.bankingsupervision.europa.eu/framework/priorities/html/geopolitical-risk.fr.html#:~:text=Les%20bouleversements%20g%C3%A9opolitiques%20peuvent%20g%C3%A9n%C3%A9rer,l%27imposition%20de%20sanctions%20internationales

BCE : Priorités prudentielles pour 2026-2028
https://www.bankingsupervision.europa.eu/framework/priorities/html/ssm.supervisory_priorities202511.fr.html

BCE : Priorités et risques
https://www.bankingsupervision.europa.eu/framework/priorities/html/index.fr.html

BCE : Résultats des tests de résistance 2025 menés par l'ABE et la BCE | Autorité de contrôle prudentiel et de résolution
https://acpr.banque-france.fr/fr/communiques-de-presse/resultats-des-tests-de-resistance-2025-menes-par-labe-et-la-bce

Ouest France : Une nouvelle cyberattaque russe cible les services en ligne de La Poste et de la Banque Postale
https://www.ouest-france.fr/societe/faits-divers/une-nouvelle-cyberattaque-russe-cible-les-services-en-ligne-de-la-poste-et-de-la-banque-postale-5e10fdee-e6ee-11f0-91a5-1dde61cf54f7

BFMTV : Cyberattaque contre la Banque Postale: l'attaque informatique revendiquée par un groupe pro-russe
https://www.bfmtv.com/tech/cyberattaque-contre-la-banque-postale-l-attaque-informatique-toujours-en-cours-la-dgsi-chargee-de-l-enquete_AV-202512230721.html

La Banque Postale : Cyberattaque contre La Banque Postale - La Banque Postale
https://www.labanquepostale.com/newsroom-publications/actualites/2026/cyberattaque-banque-groupe-la-poste.html

Le Big Data : Banque Postale en panne : une attaque à ne pas négliger
https://www.lebigdata.fr/banque-postale-en-panne-comment-une-cyberattaque-a-frappe-le-service-public

BIBLIOGRAPHIE

Les Echos : Le détroit d'Ormuz, ce verrou contrôlé par l'Iran et qui ferme l'accès au pétrole | Les Echos
https://www.lesechos.fr/monde/afrique-moyen-orient/le-detroit-dormuz-ce-verrou-controle-par-liran-et-qui-ferme-lacces-au-petrole-2220193

Commission Européenne : L'UE adopte un 19 e train de sanctions à l'encontre de la Russie*
https://ec.europa.eu/commission/presscorner/detail/fr/ip_25_2491

La tribune : Pétrole, banques, cryptos : l'UE dévoile un 20e paquet de sanctions contre Moscou et verrouille l'accès aux mers
https://www.latribune.fr/article/economie/international/33778656893483/petrole-banques-cryptos-l-ue-devoile-un-20e-paquet-de-sanctions-contre-moscou-et-verrouille-l-acces-aux-mers

Boursorama : Citi maintient la fermeture de la plupart de ses succursales aux Émirats arabes unis pour une durée indéterminée en raison de la guerre contre l'Iran - 16/03/2026 à 13:11 - Boursorama
https://www.boursorama.com/bourse/actualites/citi-maintient-la-fermeture-de-la-plupart-de-ses-succursales-aux-emirats-arabes-unis-pour-une-duree-indeterminee-en-raison-de-la-guerre-contre-l-iran-0c7eca35d1d4b97f9b9a13f617325ac2

L'Usine Digitale : Le piratage de Jaguar Land Rover aura coûté 2,19 milliards d'euros à l'économie britannique
https://www.usine-digitale.fr/editorial/le-piratage-de-jaguar-land-rover-aura-coute-2-19-milliards-d-euros-a-l-economie-britannique.N2240002

JLR : JLR Q3 SALES IMPACTED BY CYBER INCIDENT AS PREVIOUSLY INDICATED | JLR Corporate Website
https://www.jlr.com/news/2026/01/jlr-q3-sales-impacted-cyber-incident-previously-indicated

JLR : JLR Q4 SALES BOUNCE BACK AFTER CYBER INCIDENT | JLR Corporate Website
https://www.jlr.com/news/2026/04/jlr-q4-sales-bounce-back-after-cyber-incident

Investing.com : Tata Motors Passenger Vehicles (TAMO) Share Price History - Investing.com India
https://in.investing.com/equities/tata-motors-ltd-historical-data

MoneyControl : Tata Motors PV shares fall 4% after JLR wholesales drop 43% in Q3 after cyberattack
https://www.moneycontrol.com/news/business/markets/tata-motors-pv-shares-drop-4-after-jlr-wholesales-drop-43-in-q3-after-cyberattack-13759075.html

NEXIALOG
CONSULTING