


ANNA DIMITROVA

CHARBEL KANAAN

NATHALIE BELHOSTE

Conflit armé sur un marché export : 12 recommandations pour protéger l'entreprise, ses salariés et sa réputation

Un conflit armé peut transformer en quelques jours un marché porteur en environnement incontrôlable. Les routes deviennent impraticables, des infrastructures sont détruites, les administrations cessent parfois de fonctionner et de nouveaux acteurs cherchent à imposer leurs propres règles. Dans d'autres situations, l'État résiste et l'activité économique continue, mais au prix d'alertes permanentes, de pénuries de personnel, de coupures énergétiques et de traumatismes humains durables.

Pour une **entreprise exportatrice**, le véritable enjeu n'est donc pas seulement de prévoir une guerre. Il est de construire une organisation capable de détecter rapidement la rupture, de qualifier le type de conflit et de prendre une décision avant que les événements ne la lui imposent.

Les expériences analysées pendant la Masterclass de La Fabrique de l'Exportation font apparaître douze recommandations essentielles.

1. Distinguer le risque politique d'une véritable zone de conflit

Une entreprise habituée aux marchés difficiles peut être tentée de considérer un conflit comme une aggravation du **risque pays**. Cette approche est insuffisante. Dans une zone de conflit, l'entreprise ne fait pas seulement face à une monnaie instable, à une administration lente ou à un changement de réglementation. Elle peut être confrontée à une violence organisée, à une fragmentation territoriale et à la disparition de ses interlocuteurs institutionnels.

La première étape consiste donc à déterminer si l'entreprise opère encore dans un État fonctionnel ou dans un territoire où plusieurs acteurs se disputent le pouvoir. Cette distinction influence toutes les décisions suivantes. Dans un pays où l'État continue de fonctionner, une activité peut parfois être maintenue moyennant une adaptation logistique, énergétique et humaine. Dans un territoire où les institutions sont remplacées par des groupes armés, la possibilité même d'exercer une activité légale et responsable peut disparaître.

2. Cartographier les acteurs et les territoires en temps réel

Une cartographie réalisée au début de la crise devient rapidement obsolète. Les groupes armés changent de nom, de chef, d'alliance et de zone d'influence. Une route sûre le lundi peut être contrôlée par un autre acteur le vendredi.

L'entreprise doit mettre en place une **cartographie dynamique des risques**. Celle-ci doit identifier les autorités officielles, les groupes présents, les infrastructures critiques, les axes logistiques, les zones d'affrontement et les évolutions réglementaires. Elle doit aussi distinguer les informations confirmées des rumeurs. En situation de guerre, la circulation de fausses informations peut conduire à des décisions dangereuses.

Cette cartographie ne doit pas être confiée à un seul intermédiaire. L'entreprise doit croiser plusieurs sources, notamment ses équipes locales, les autorités diplomatiques, les organisations internationales, les associations professionnelles, les prestataires de sécurité et les entreprises présentes dans la région. Le recours à plusieurs sources permet de réduire la dépendance à un interlocuteur qui pourrait minimiser les risques, induire des biais dans ses remontées d'informations ou défendre ses propres intérêts.

3. Créer une cellule de crise disposant d'un véritable pouvoir de décision

Une **cellule de crise** purement consultative ne suffit pas. Elle doit avoir accès aux dirigeants capables de suspendre une activité, de débloquer des moyens financiers et d'ordonner une évacuation. Sa composition doit associer la direction générale, les ressources humaines, la sécurité, le juridique, la conformité, la finance, les opérations et la communication.

Les responsabilités doivent être définies à l'avance. Qui peut fermer un site ? Qui décide l'évacuation ? Qui contacte les familles ? Qui valide un paiement exceptionnel ? Qui conserve les documents susceptibles d'être demandés ultérieurement par une autorité judiciaire ?

Les entreprises internationales doivent également clarifier la répartition des responsabilités entre le siège et la filiale. Le siège ne peut pas se contenter de déléguer la gestion de crise au terrain, puis prétendre qu'il ne connaissait pas les décisions prises localement. À l'inverse, les équipes locales ne doivent pas être paralysées par l'attente d'une validation située à plusieurs milliers de kilomètres.

4. Définir des lignes rouges avant d'être soumis à la pression

Les **lignes rouges** doivent être suffisamment précises pour déclencher automatiquement une réévaluation de la présence de l'entreprise. Elles peuvent comprendre la perte du contrôle étatique sur la zone d'implantation, l'enlèvement d'un salarié, la fermeture de l'ambassade, la rupture durable des communications, l'apparition d'un groupe sanctionné, la multiplication des demandes de paiement ou l'impossibilité de garantir un traitement équitable aux salariés.

Chaque ligne rouge doit être associée à une conséquence. Il peut s'agir d'une suspension de la production, d'une réduction des effectifs, d'une évacuation ou d'un retrait. Sans cette préparation, l'entreprise risque de déplacer continuellement ses propres limites. Un incident exceptionnel devient une nouvelle normalité, puis sert de référence pour accepter l'incident suivant. La question à poser n'est pas seulement de savoir combien de temps l'entreprise peut continuer. Il faut déterminer à **partir de quel moment elle ne doit plus continuer**.

5. Préparer plusieurs scénarios plutôt qu'un plan unique

Un plan de crise doit intégrer **plusieurs niveaux de dégradation**. L'entreprise peut prévoir un scénario de tension politique, un scénario de violences localisées, un scénario de guerre ouverte et un scénario d'effondrement institutionnel. Pour chacun, elle doit définir les conséquences sur les salariés, les stocks, la trésorerie, les contrats, les transports, les systèmes informatiques et la communication.

La planification doit aussi distinguer plusieurs options stratégiques. L'entreprise peut maintenir l'activité, la réduire, la suspendre, transférer certaines opérations, quitter une région ou sortir entièrement du pays.

Cette approche évite de réduire la décision à une opposition entre rester et partir. Une **stratégie hybride** permet parfois de préserver une présence commerciale sans maintenir un site industriel fortement exposé. Les scénarios doivent être testés au moyen d'exercices réguliers. Une liste de procédures non testée peut se révéler inutilisable lorsque les communications sont coupées ou que les personnes responsables sont absentes.

6. Placer la protection des personnes avant la protection des actifs

En situation de guerre, l'entreprise doit résister à la tentation de protéger une usine, un stock ou un réseau commercial au détriment des personnes. Le **plan de sécurité doit couvrir tous les salariés**, y compris les collaborateurs locaux, les intérimaires et, lorsque cela est pertinent, les familles.

Les entreprises doivent éviter une protection à deux vitesses. L'évacuation rapide des expatriés, accompagnée du maintien des salariés locaux sur un site dangereux, crée un risque humain, éthique et réputationnel considérable. L'entreprise doit connaître la localisation de ses collaborateurs, disposer de plusieurs moyens de contact et prévoir des solutions de transport, d'hébergement et d'assistance financière.

Elle doit également prendre en compte les contraintes individuelles. Certains salariés ne peuvent pas quitter le pays. D'autres doivent s'occuper de parents ou d'enfants. Certains peuvent être soumis à des obligations militaires. La protection des personnes ne se limite pas à l'évacuation. Elle inclut le maintien des salaires, l'accès aux soins, l'assistance psychologique et l'accompagnement dans la durée.

7. Sécuriser les relations avec les intermédiaires

Dans les environnements instables, les entreprises ont souvent besoin d'intermédiaires. Ceux-ci connaissent le terrain, parlent la langue et peuvent résoudre des difficultés opérationnelles. Mais leur utilisation peut créer une **dépendance dangereuse**. L'entreprise peut ignorer leurs méthodes, leurs relations ou la destination finale des fonds versés.

Tout intermédiaire doit faire l'objet d'une vérification renforcée. Son identité, ses bénéficiaires effectifs, ses liens politiques et ses éventuelles relations avec des groupes sanctionnés doivent être examinés. Les contrats doivent définir précisément les services rendus, les paiements autorisés et les justificatifs exigés. Les versements en espèces doivent être limités et contrôlés.

Lorsqu'un intermédiaire affirme qu'un paiement est indispensable pour franchir un barrage ou garantir la sécurité d'un site, la décision ne doit jamais être laissée à une seule personne. Elle doit être examinée par les fonctions juridique et conformité. Une entreprise ne doit pas confondre la nécessité opérationnelle avec l'autorisation juridique.

8. Contrôler chaque paiement lié à la sécurité

Les paiements présentés comme des **frais de protection**, des **droits de passage** ou des **dépenses de sécurité** sont particulièrement risqués. Ils peuvent financer directement ou indirectement un groupe armé, une organisation sanctionnée ou une activité criminelle. Ils peuvent également encourager de nouvelles demandes et renforcer la dépendance de l'entreprise. Une procédure spécifique doit imposer l'identification du bénéficiaire, la justification du paiement, la validation par plusieurs responsables et la conservation des documents.

La conformité ne doit pas être considérée comme une formalité administrative. Elle doit être capable d'arrêter une opération. Les responsables locaux doivent savoir qu'ils peuvent refuser un paiement sans être tenus pour responsables d'une interruption de l'activité. Dans le cas contraire, la pression des objectifs commerciaux peut les conduire à accepter des arrangements qu'ils savent dangereux. La continuité de l'activité ne peut jamais justifier le financement d'acteurs interdits ou la violation de sanctions internationales.

9. Organiser une remontée directe des signaux critiques

La **myopie organisationnelle** apparaît lorsque l'information existe, mais ne modifie pas la décision. Pour l'éviter, certains événements doivent être transmis directement à la direction générale et au conseil d'administration. Un enlèvement, une demande de rançon, une menace contre le responsable de la sécurité ou la prise de contrôle d'une route ne doivent pas être noyés dans un rapport opérationnel. L'entreprise doit créer un canal de remontée indépendant de la ligne hiérarchique habituelle. Les salariés et les responsables locaux doivent pouvoir signaler une situation sans craindre d'être accusés d'alarmisme.

Il est également nécessaire d'organiser la contradiction. Une personne ou une équipe doit avoir pour mission de remettre en cause les hypothèses dominantes.

10. Ne pas laisser les investissements passés dicter l'avenir

Un **actif industriel coûteux** ne doit pas devenir un piège décisionnel. Les sommes déjà investies sont perdues, que l'entreprise reste ou parte, lorsqu'elles ne peuvent pas être récupérées. La décision doit donc se fonder sur les risques et les bénéfices futurs, et non sur la volonté de justifier les dépenses passées.

Pour réduire ce biais, l'évaluation doit être conduite par une équipe qui n'est pas directement responsable de l'investissement initial. Les dirigeants qui ont porté le projet peuvent avoir des difficultés à reconnaître qu'il faut l'abandonner. Le conseil d'administration doit recevoir une analyse complète comprenant les risques humains, juridiques, éthiques et réputationnels. Une comparaison limitée aux pertes financières liées à la fermeture donnerait une vision trompeuse. Le maintien d'un actif ne constitue pas une réussite lorsque l'entreprise perd sa réputation, fait l'objet de poursuites ou expose ses salariés.

11. Renforcer la résilience opérationnelle et énergétique

Dans un pays où l'État continue de fonctionner, la priorité peut être d'adapter les opérations plutôt que de quitter le marché. L'entreprise doit **diversifier ses fournisseurs**, ses **itinéraires** et ses **moyens de transport**. Elle doit prévoir des stocks

de sécurité, des capacités de production alternatives et des solutions de travail à distance.

La résilience énergétique est devenue essentielle. Les générateurs, batteries et systèmes de secours doivent être dimensionnés pour des coupures longues, et non pour une interruption de quelques heures. Les équipements doivent être testés dans des conditions réelles. Il faut vérifier les stocks de carburant, la maintenance, la disponibilité des pièces détachées et la capacité à fonctionner par grand froid.

La résilience numérique est tout aussi importante. Les données critiques doivent être sauvegardées dans plusieurs pays et accessibles même lorsque les systèmes locaux sont indisponibles.

12. Préparer un retrait responsable et une éventuelle réentrée

Le plan de sortie doit être élaboré dès l'entrée sur un marché à risque. Attendre la dernière phase de la crise expose l'entreprise à un départ chaotique. Le **retrait responsable** doit couvrir les salariés, les équipements dangereux, les données, les contrats, les stocks et les obligations envers les partenaires. L'entreprise doit prévoir comment informer ses clients, sécuriser les installations et conserver les documents nécessaires à de futures procédures.

Elle doit également déterminer les conditions d'une éventuelle réentrée. Quitter un marché ne signifie pas nécessairement l'abandonner pour toujours. Une entreprise peut suspendre ses activités, maintenir une veille et revenir lorsque la sécurité et le cadre institutionnel sont rétablis. La décision de retour doit être aussi rigoureuse que la décision de départ. Elle ne peut pas reposer uniquement sur les perspectives de reconstruction ou sur l'espoir de prendre une avance commerciale. Le potentiel économique d'un marché post-conflit ne doit jamais conduire à minimiser les risques encore présents.