Cigref
RÉUSSIR
LE NUMÉRIQUE

# Géopolitique et stratégie numérique

## Défis et leviers d'actions pour les directions du numérique

Février 2025

Cigref

# Géopolitique et stratégie numérique

*Défis et leviers d'actions pour les directions du numérique*

*Février 2025*

**Droit de propriété intellectuelle**
Toutes les publications du Cigref sont mises gratuitement à la disposition du plus grand nombre mais restent protégées par les lois en vigueur sur la propriété intellectuelle.

# ÉDITO

Traditionnellement, la géopolitique était absente des stratégies numériques. Nos décisions reposaient surtout sur des critères métiers, techniques, financiers ou juridiques. Mais depuis quelques années, les enjeux géopolitiques se sont invités dans le domaine du « *Hardware* », avec, dans certains cas, des contraintes imposant le choix d'équipements ou de composants selon de nouveaux critères.

En ce qui concerne les logiciels et les services numériques, il devient actuellement indispensable d'intégrer la géopolitique. Certains acteurs l'ont déjà pris en compte, d'autres s'interrogent sur la nécessité de le faire, et d'autres enfin n'y ont pas encore réfléchi.

Prenons un exemple concret : lors du choix d'un cloud pour héberger nos données, nous analysons généralement les aspects sécuritaires et financiers, et réalisons parfois une étude *make-or-buy*. Malgré tout, des questions comme « *où se situe le datacenter* ? » et « *quel est le risque de coupure de connexion entre nos bureaux et ce datacenter* ? » sont souvent négligées.

Pour les logiciels, la question se pose de savoir si l'*Inner Source* et *l'Open Source* seront mieux adaptés, non pour des raisons financières, mais parce qu'un produit édité est toujours associé à son pays d'origine, alors que l'Open Source ou l'*Inner Source* échappent à cette notion d'appartenance nationale.

Jusqu'à présent, nos stratégies en « *follow-the-sun* » reposaient sur la sélection de trois pays ayant un décalage horaire d'environ 8 heures, souvent déterminés par les implantations géographiques existantes. Allons-nous bientôt devoir choisir ces pays en fonction de critères géopolitiques, voire réduire ces activités organisées en « *follow-the-sun* » pour favoriser le travail de nuit en local ?

Nous observons déjà des politiques de substitution progressive de l'*off-shoring* par du *near-shoring* et à présent par du *reshoring*. Il existe également des cas où des décisions d'externalisation prises par un partenaire conduisent à l'internalisation des équipes en raison des risques géopolitiques liés aux nouvelles localisations des services.

Nous avons jugé utile d'aborder ces sujets et de partager nos expériences récentes. Nous espérons que le rapport qui suit servira à alimenter les discussions internes au sein de chaque organisation membre.

**Marc-Michel STACK**, *Head of Group IT Technology Intelligence*, chez BNP Paribas et
**Taras VELIKOROUSSOV**, Directeur de la performance financière et technique ITN, chez Orange.

## SYNTHÈSE

Les tensions entre grandes puissances, États-Unis, Chine, Russie, Europe, ainsi que les conflits régionaux (Russie-Ukraine, Moyen-Orient), affectent les chaînes d'approvisionnement technologiques et renforcent la polarisation de l'espace numérique mondial. Face à ces bouleversements géopolitiques, la Direction des Systèmes d'Information (DSI) doit intégrer une compréhension fine de ses enjeux pour renforcer sa résilience numérique. Ainsi, ces tensions globales influencent les stratégies IT à travers quatre axes principaux : l'autonomie stratégique, la cybersécurité, la gestion des talents et des fournisseurs, et la gouvernance.

1. Les DSI doivent développer leur **autonomie stratégique**, en réduisant leur dépendance aux technologies et fournisseurs étrangers, et en privilégiant des solutions locales ou européennes dans des secteurs sensibles (cloud, semi-conducteurs). Ainsi, la diversification des partenaires et des fournisseurs devient une stratégie clé pour limiter les risques de rupture d'approvisionnement.
2. L'anticipation des DSI doit également porter sur la **cybersécurité.** L'augmentation des cybermenaces liées aux tensions géopolitiques impose aux DSI de renforcer leurs défenses. Cela inclut des audits de sécurité, des protocoles rigoureux, et une surveillance des cyber-risques géopolitiques. La coopération avec des partenaires de cybersécurité locaux est également essentielle.
3. Enfin, la pénurie de **compétences IT** en Europe encourage les DSI à recruter à l'international, mais les risques géopolitiques et réglementaires liés aux recrutements à l'étranger compliquent ces démarches. Cependant, la diversification géographique des équipes IT contribue aussi à une meilleure résilience des opérations globales.
4. Ainsi, pour aller vers plus d'autonomie, de sécurité et une meilleure gestion des talents numériques à l'international, une **gouvernance IT** proactive est cruciale. En renforçant la collaboration entre la DSI, la direction juridique, la direction RH et les affaires publiques, les entreprises peuvent mieux anticiper les fluctuations géopolitiques. Une cellule dédiée à la prospective IT peut permettre d'accompagner cette réflexion et de favoriser une anticipation continue des risques et des opportunités.

En conclusion, l'approche géopolitique devient indispensable dans la gouvernance IT pour une résilience accrue face aux crises mondiales. La DSI doit s'affirmer comme un pilier stratégique de l'organisation, capable de naviguer dans un contexte numérique fragmenté et polarisé.

## REMERCIEMENTS

Nos remerciements vont à **Marc-Michel STACK,** *Head of Group IT Technology Intelligence*, chez BNP Paribas et **Taras VELIKOROUSSOV**, Directeur de la performance financière et technique ITN, chez Orange qui ont piloté ce travail, ainsi qu'à toutes les personnes qui ont participé et contribué à ce groupe de travail Cigref (ordre alphabétique) :

François BANOS - RENAULT

Xavier BENMOUSSA - GROUPE SAVENCIA

Dorra BOUGHANEM - AXA

Olivier BURGAUD - SERVIER

Jean-Philippe CAILLAT - GROUPE 3M

Claudio CIMELLI - MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

Danièle COHEN - STELLANTIS

Clément DAILLY - SUEZ

Anne DESLANDES - LA POSTE

Jean-Marc DO LIVRAMENTO - ENEDIS

Etienne DOCK - HAGER GROUP

Sylvain GERON - CARREFOUR

Didier LAVOIGNAT - GROUPE SEB

Julien MARTINO - MICHELIN

Pascal MOREUIL - AIR FRANCE-KLM

Laurent MOUTY - FAYAT

Laurent POUPON - BNP PARIBAS

Franck REGNIER - ACCOR

Benjamin ROCHARD - TRANSDEV GROUP

Sébastien SCHNEIDER - BPI FRANCE

Nous remercions également vivement tous les intervenants qui ont nourri la réflexion de notre groupe de travail :

- Jean-Joseph BOILLOT, Professeur agrégé de sciences économiques et sociales et Docteur en économie, spécialiste des grandes économies émergentes, notamment la Chine et l'Inde,
- Fayçal BOUJEMAA, *Technology Strategist*, chez ORANGE,
- Stéphane DEMARTIS, *VP Cloud Infrastructure Solutions and Services*, chez Orange
- Eric FICHOT, *Head of HR for CIB functions*, chez BNP Paribas,
- Martin PAILHES, responsable de la Plateforme Digital & IP de la Fonction Juridique du Groupe BNP PARIBAS,
- Nicolas ROUX, *Chief Procurement Officer - IT Technology and Services*, chez BNP PARIBAS
- Sandip WADJE, *Managing Director- Global Head of Emerging Technology Operational Risks & Intelligence*, chez BNP PARIBAS.

Ce document a été construit et rédigé par Aurélie CHOTARD, Directrice de mission au Cigref.

# TABLE DES MATIÈRES


**1 INTRODUCTION : POURQUOI LA DSI DOIT-ELLE S'INTÉRESSER AUX ÉVOLUTIONS GÉOPOLITIQUES ? ..... 6**

1.1 Panorama des principales tendances géopolitiques .....6

1.1.1 Les États-Unis : entre incertitude politique et influence internationale .....6

1.1.2 La Chine : stabilisation économique et tensions stratégiques .....7

1.1.3 Conflit russo-UKRAINIEN : une impasse prolongée .....7

1.1.4 Israël-Palestine et le GOLFE : une escalade régionale .....7

1.1.5 La France : une crise politique interne sans précédent .....7

1.2 Le numérique, un enjeu central dans les relations internationales .....8

1.3 Les enjeux de la DSI dans ce contexte géopolitique .....10

**2 PARTENARIATS ET ACHATS DE LA DSI : ATOUTS ET VULNÉRABILITÉS GÉOPOLITIQUES ..... 12**

2.1 Les principaux partenariats et les enjeux géopolitiques associés .....12

2.2 Le retour au local : une stratégie de résilience numérique ? .....16

2.2.1 Le concept de « *make or buy* » .....17

2.3 Anticiper grâce à une meilleure connaissance des fournisseurs .....17

2.3.1 Les bonnes pratiques pour anticiper les risques de nature géopolitique .....17

2.3.2 Mieux situer et mieux connaître les risques .....18

2.4 Faire les bons choix stratégiques .....19

2.4.1 Conception d'architectures résilientes .....19

2.4.2 Résilience opérationnelle dans les choix IT .....19

2.4.3 Gestion des fournisseurs .....19

**3 POLITIQUES RH-IT DANS UN CONTEXTE INTERNATIONAL TROUBLÉ ..... 21**

3.1 Pénurie des compétences : seule raison du recrutement IT à l'international ? .....21

3.2 Les risques liés aux recrutements internationaux .....23

3.3 Perspectives futures du recrutement à l'international et nouveaux enjeux .....24

**4 INTÉGRER LA DIMENSION GÉOPOLITIQUE À LA GOUVERNANCE DE LA DSI ..... 28**

4.1 Pourquoi est-ce compliqué d'intégrer la dimension géopolitique à la DSI ? .....28

4.2 Prendre en compte la dimension géopolitique : une nécessaire collaboration au sein de l'entreprise ....28

4.2.1 Mettre en place la bonne gouvernance .....28

4.2.2 Collaborer avec les bons outils .....30

4.2.3 Limites et pérennité de l'approche .....31

**5 CONCLUSION : VERS UNE DSI PROACTIVE FACE AUX FLUCTUATIONS GÉOPOLITIQUES ..... 34**

## TABLE DES ILLUSTRATIONS

**Matrice des risques et opportunités sur les partenariats d'innovation .....13**

**Schéma de gouvernance pour intégrer la dimension géopolitique aux activités IT .....30**

## TABLE DES [ENCARTS]

**Tensions géopolitiques et cybersécurité, avec BNP Paribas..... 9**

**La géopolitique des intelligences artificielles.....15**

**Stratégies d'implantation RH-IT : REX des entreprises .....23**

**Perspectives économiques, politiques et culturelles sur l'Inde.....26**

**Travailler avec la direction juridique : une nécessité pour la DSI .....32**

# 1 INTRODUCTION : POURQUOI LA DSI DOIT-ELLE S'INTÉRESSER AUX ÉVOLUTIONS GÉOPOLITIQUES ?

*NB : Ce rapport est issu d'un groupe de travail dont les réflexions se sont tenues entre janvier et septembre 2024. Ainsi, la vision de la scène géopolitique, telle que proposée dans le rapport, ne prend pas en compte les évènements advenus après octobre 2024. Cette première partie, cependant, explore les conséquences de l'élection américaine* ***telles que nous les percevions au moment de la rédaction, en novembre 2024.***

La direction du numérique se retrouve aujourd'hui au carrefour des enjeux technologiques et des enjeux géopolitiques, dans un monde où les équilibres entre nations sont de plus en plus instables et où les pressions et les tensions sur les infrastructures numériques se multiplient. La compréhension des dynamiques géopolitiques devient indispensable pour être en mesure d'anticiper les menaces et les opportunités qui en découlent, et ainsi renforcer la résilience des organisations. Cet intérêt pour les évolutions géopolitiques permet à la DSI d'ajuster ses stratégies pour mieux protéger les systèmes d'information, assurer la continuité opérationnelle et s'aligner sur les objectifs d'autonomie stratégique dans le domaine du numérique. Elle est également une opportunité de dialogue régulier et nourri, entre les directions métiers et les fonctions support d'une part et la DSI d'autre part, sur l'évolution des services et des marchés.

## 1.1 PANORAMA DES PRINCIPALES TENDANCES GÉOPOLITIQUES

L'année 2024 s'est déroulée sous un climat international d'incertitudes géopolitiques, avec des dynamiques changeantes entre les principales puissances mondiales, des conflits exacerbés dans des zones déjà tendues, et des bouleversements politiques en France qui ajoutent une dimension unique à la scène européenne. Chaque année, le Cigref dresse un panorama de la scène internationale dans la note de contexte de son rapport d'orientation stratégique.

Les cinq grands enjeux géopolitiques, proposés ci-dessous, décrivent un contexte global dans lequel les alliances, la stabilité économique et la sécurité régionale se révèlent interdépendantes et volatiles, influençant l'équilibre des relations internationales et des marchés mondiaux pour les années à venir.

### 1.1.1 LES ÉTATS-UNIS : ENTRE INCERTITUDE POLITIQUE ET INFLUENCE INTERNATIONALE

En novembre 2024, l'élection présidentielle américaine occupe une place centrale dans l'agenda international, car elle influence les relations des États-Unis avec leurs alliés, particulièrement en Europe et dans l'Indo-Pacifique. La compétition entre Kamala Harris et Donald Trump a révélé deux visions distinctes. Harris incarnant une continuité dans l'approche multilatéraliste et les alliances internationales, avec une volonté de soutenir les partenariats en Asie et en Europe, tandis que Trump défend un repli sur des politiques protectionnistes et une vision transactionnelle du monde. À présent que Trump a été réélu à la tête des USA, une hausse des tarifs douaniers va vraisemblablement diviser

davantage l'économie mondiale en blocs économiques, affaiblissant les échanges mondiaux et exacerbant les tensions commerciales, notamment avec la Chine.

### 1.1.2 LA CHINE : STABILISATION ÉCONOMIQUE ET TENSIONS STRATÉGIQUES

La Chine connaît un ralentissement économique marqué par des problèmes structurels dans les secteurs de la consommation et de l'immobilier. Malgré ses efforts pour relancer la croissance par des investissements publics, son PIB devrait continuer de stagner en 2025. Sur le plan géopolitique, la Chine renforce son influence en Asie-Pacifique où les tensions avec les États-Unis restent vives. Les alliés asiatiques de Washington surveillent de près les conséquences de l'élection américaine, car la victoire de Trump pourrait aggraver les frictions commerciales avec Pékin, avec un regain de la concurrence sur le plan technologique et économique.

### 1.1.3 CONFLIT RUSSO-UKRAINIEN : UNE IMPASSE PROLONGÉE

La guerre en Ukraine s'enlise, sans avancée décisive d'un côté ou de l'autre. Le soutien occidental demeure crucial pour l'Ukraine, et l'élection américaine devrait en redéfinir les contours. La future administration Trump devrait envisager une réduction des aides, privilégiant une approche isolationniste. Cette perspective inquiète les alliés européens, pour qui le soutien américain est essentiel pour contenir les ambitions russes dans un contexte d'absence relative de leadership clair en Europe.

### 1.1.4 ISRAËL-PALESTINE ET LE GOLFE : UNE ESCALADE RÉGIONALE

La montée des tensions au Moyen-Orient, exacerbée par les récentes hostilités entre Israël, le Hamas et le Hezbollah soutenu par l'Iran, pourrait déstabiliser toute la région. Les alliances américaines dans le Golfe pourraient être mises à l'épreuve à l'issue de l'élection américaine : Trump pourrait en effet intensifier le soutien militaire unilatéral à Israël. Cette situation augmente le risque d'escalade à long terme dans la région, affectant également les relations des États-Unis avec des acteurs clés comme l'Arabie saoudite.

### 1.1.5 LA FRANCE : UNE CRISE POLITIQUE INTERNE SANS PRÉCÉDENT

La France traverse une crise politique marquée par des divisions internes et une instabilité gouvernementale. Le manque de majorité claire et les difficultés budgétaires renforcent les tensions, tandis que le gouvernement fait face à une dette publique en hausse. Cette situation soulève des préoccupations au sein de l'UE, où la France joue un rôle stabilisateur crucial. Le pays pourrait être contraint de réformer son budget pour assurer la soutenabilité de sa dette, tout en naviguant entre les exigences de l'UE et celles des citoyens français.

## 1.2 LE NUMÉRIQUE, UN ENJEU CENTRAL DANS LES RELATIONS INTERNATIONALES

Le numérique est aujourd'hui le théâtre d'une **fragmentation croissante de l'espace mondial**. Cette tendance s'accentue sous l'effet de rivalités technologiques et économiques entre grandes puissances, exacerbées par des stratégies protectionnistes et d'autosuffisance technologique.

La **rivalité entre les États-Unis et la Chine**, particulièrement visible dans l'industrie des semi-conducteurs, est emblématique de cette fragmentation. Les États-Unis s'efforcent de réduire leur dépendance aux semi-conducteurs asiatiques en rapatriant la production sur leur sol et en imposant à la Chine des restrictions d'accès aux technologies avancées, tandis que celle-ci poursuit sa quête d'autonomie technologique malgré ces barrières. De son côté, l'Union européenne, consciente de son retard, investit dans son propre *Chips Act* pour tenter de combler le fossé technologique, bien qu'elle demeure dépendante des acteurs asiatiques et américains (dans un contexte où 60% des semi-conducteurs mondiaux et plus de 90% des semi-conducteurs les plus avancés sont encore produits à Taïwan, et que la Chine manifeste une capacité croissante à établir un blocus de cette île).

**L'intensification de cette dynamique protectionniste** entraîne la formation de blocs technologiques fermés, où chaque région tente de protéger et de développer ses capacités numériques. Cette fragmentation impacte également l'industrie de l'intelligence artificielle (IA) générative, un secteur en pleine effervescence mais dont le modèle économique reste fragile. Les grands acteurs de l'IA générative, majoritairement basés aux États-Unis, investissent massivement dans ces technologies, mais peinent à rendre les opérations profitables. Le secteur pose en outre des défis pour la gouvernance des données et des infrastructures nécessaires, que chaque bloc tente de maîtriser avec des politiques industrielles et régulatoires parfois opposées, pour limiter sa dépendance.

Enfin, **l'Union européenne fait face à une dépendance structurelle** envers les grandes entreprises technologiques américaines, qui capturent une part croissante de la valeur numérique créée en Europe. Cette situation met en lumière les tensions autour de la souveraineté numérique de l'Europe, qui se trouve fragilisée par une concentration de pouvoir entre les mains de quelques acteurs étrangers, menaçant à long terme la compétitivité et l'autonomie stratégique de ses entreprises.

Nous assistons à la fin d'un cycle de recherche d'universalisme et d'interopérabilité dans l'espace numérique mondial qui se fragmente au rythme des rivalités économiques, technologiques et de gouvernance, chaque bloc tentant de préserver ses intérêts et de limiter sa dépendance aux autres, au risque de compromettre les coopérations et les interopérabilités internationales.

**Tensions géopolitiques et cybersécurité, avec BNP Paribas**

Le secteur financier est une cible majeure pour les cyberattaquants. Au-delà de protéger les données financières, il est indispensable de maintenir stable le système financier et de préserver la confiance dans le système bancaire. Ainsi, une banque comme BNP Paribas se doit de garder un regard permanent sur l'impact que peuvent avoir les tensions géopolitiques sur l'évolution des attaques cyber. Ces attaques cyber peuvent poursuivre des objectifs différents et ont donc des conséquences diverses sur l'activité d'une organisation :

- **Les attaques cyber comme outil dans les conflits géopolitiques** : on constate l'augmentation des cyberattaques comme outils d'influence géopolitique, spécifiquement l'utilisation de stratégies cyber durant le conflit en cours entre la Russie et l'Ukraine. Des acteurs privés et d'autres nations se sont impliqués dans ces opérations cyber. Les cyberattaques sont utilisées comme des moyens de pression par les acteurs géopolitiques. L'évolution de la situation géopolitique a une incidence directe sur l'évolution des risques cyber (exemple des nombreuses attaques contre Israël après le 7 octobre).
- **Les attaques cyber pour perturber la chaîne d'approvisionnement IT** : les institutions financières et leurs chaînes d'approvisionnement sont particulièrement vulnérables aux attaques cyber. Les attaquants ciblent généralement les parties les moins sécurisées de la chaîne d'approvisionnement, mais ces attaques peuvent aussi être instrumentalisées dans la cadre de conflits géopolitiques pour affecter des industries plus globales, comme celle des semi-conducteurs dans le cas d'un conflit régional en Asie.
- **Les attaques cyber comme moyen de pression et d'influence entre états** : certains pays, notamment la Russie et la Corée du Nord, soutiennent des activités cybercriminelles comme moyen de contourner les sanctions et de mener une guerre indirecte. Ces activités incluent des attaques de *ransomware* et des campagnes de désinformation, qui sont payées en cryptomonnaies pour contourner les sanctions.
- **Les attaques cyber comme outil de déstabilisation des populations** : ces attaques cyber ont des impacts plus larges sur les systèmes financiers et la confiance sociale, elles sont utilisées de façon stratégique pour instiller une méfiance parmi les populations et pour perturber les services essentiels.

Pour faire face à cette évolution du paysage cyber et au contexte de tensions mondiales, les organisations doivent mieux se préparer et anticiper les menaces cyber de toute nature. Cela inclut l'amélioration des défenses en cybersécurité, la compréhension des motifs derrière les cyberattaques et la préparation aux crises potentielles telles qu'un conflit potentiel en Asie susceptible d'affecter violemment les chaînes d'approvisionnement mondiales.

**Sandip WADJE,** *Managing Director- Global Head of Emerging Technology Operational Risks & Intelligence*, chez BNP PARIBAS

## 1.3 LES ENJEUX DE LA DSI DANS CE CONTEXTE GÉOPOLITIQUE

Dans un contexte géopolitique marqué par la fragmentation de l'espace numérique et la rivalité technologique croissante entre grandes puissances, la Direction des Systèmes d'Information (DSI) fait face à des enjeux stratégiques majeurs. En plus de s'adapter aux contraintes locales, elle doit également envisager des formes de régionalisation afin de saisir des opportunités et de renforcer sa résilience. Voici les enjeux principaux auxquels la DSI doit répondre dans ce cadre :

- **Autonomie stratégique et maîtrise des dépendances** : la DSI est confrontée au défi de réduire sa dépendance vis-à-vis des fournisseurs étrangers, particulièrement américains et asiatiques, dans des domaines stratégiques comme le cloud, les semi-conducteurs, et les services numériques. Face à la fragmentation de l'espace numérique, elle doit diversifier ses sources d'approvisionnement pour limiter les risques de rupture, que ce soit en matière de données, de compétences, ou de technologies critiques. Cela implique notamment de privilégier des solutions locales ou européennes, alignées avec les politiques de souveraineté numérique.
- **Cybersécurité et résilience des infrastructures** : Dans un environnement international de plus en plus polarisé, les cybermenaces s'intensifient. La DSI doit garantir la sécurité des données et la résilience de ses infrastructures en adoptant des protocoles de cybersécurité robustes, des audits réguliers, et des partenariats de cyberdéfense renforcés. L'expansion internationale peut contribuer à cette résilience en offrant une diversification géographique des ressources, assurant une continuité des opérations en cas de crises locales ou de cyberattaques.
- **Accélération de l'innovation et adaptation aux régulations internationales** : pour rester compétitive, la DSI doit surveiller et adopter les innovations émergentes dans les marchés étrangers, tout en naviguant dans un cadre réglementaire de plus en plus complexe et fragmenté. En effet, les régulations sur les données, la protection de la vie privée, et l'IA varient d'une région à l'autre, forçant la DSI à adapter rapidement ses pratiques pour respecter les lois locales, comme le RGPD en Europe, tout en suivant les réglementations américaines ou asiatiques. Cette veille technologique et réglementaire lui permet non seulement de rester conforme mais aussi de tirer parti des écosystèmes technologiques locaux.
- **Optimisation des coûts opérationnels et recherche de talents** : La DSI peut aussi chercher à réduire ses coûts en tirant parti des économies d'échelle permises par une implantation internationale. Cela lui permet d'optimiser ses achats de ressources critiques, de standardiser ses processus et d'accéder à des talents qualifiés dans des régions clés. Ces talents, parfois rares localement, sont essentiels pour soutenir des domaines critiques tels que la cybersécurité et l'IA. L'internationalisation facilite donc l'accès à des compétences variées tout en renforçant la compétitivité de l'organisation.
- **Facilitation du changement organisationnel et soutien 24/7** : Dans un environnement mondial instable, la DSI doit développer une culture d'adaptabilité et d'agilité. Une présence internationale régionale permet d'impulser une culture d'adaptabilité, essentielle pour faire face aux évolutions rapides du secteur numérique. En outre, la DSI peut fournir un support continu aux clients grâce à un modèle « *follow the sun* », en s'appuyant sur des équipes

réparties sur plusieurs fuseaux horaires. Une telle organisation garantit la disponibilité des services critiques 24/7, répondant ainsi aux exigences de performance et de satisfaction client.

- **Gouvernance éthique et responsabilité environnementale** : enfin, la DSI doit intégrer des pratiques responsables et éthiques dans sa gestion, notamment en matière de qualité des données, d'utilisation de l'IA, et d'impact environnemental. La dépendance aux données et aux infrastructures numériques exige une gouvernance rigoureuse, notamment face à l'émergence des IA génératives, pour éviter les biais algorithmiques et minimiser les effets négatifs sur l'environnement.

# 2 PARTENARIATS ET ACHATS DE LA DSI : ATOUTS ET VULNÉRABILITÉS GÉOPOLITIQUES

Dans un monde où les tensions géopolitiques influencent de plus en plus les décisions d'affaires, les partenariats et achats de la DSI se révèlent être des leviers stratégiques, mais également des sources de vulnérabilité. Les collaborations internationales, qu'elles s'exercent dans le domaine de l'innovation, de la conformité ou de l'approvisionnement de services critiques, doivent être envisagées avec prudence pour anticiper les risques de rupture et assurer la continuité des opérations. En intégrant les dimensions géopolitiques aux stratégies d'achats et de partenariats, la DSI peut non seulement renforcer la résilience de l'organisation face aux crises mondiales, mais aussi maximiser les avantages d'un écosystème diversifié de fournisseurs et de partenaires, tout en minimisant les dépendances critiques.

## 2.1 LES PRINCIPAUX PARTENARIATS ET LES ENJEUX GÉOPOLITIQUES ASSOCIÉS

La conclusion de partenariats à l'international, qu'ils soient de nature commerciale ou non, concerne plusieurs domaines clés :

- Pour **l'innovation,** collaborer avec des acteurs étrangers permet à une entreprise internationale d'accéder à des technologies disruptives, sur des domaines spécifiques comme avec Israël dans le domaine de la cybersécurité, ou auprès d'acteurs de pointe situés aux États-Unis. Ces partenariats peuvent également soutenir l'incubation d'acteurs émergents (start-ups) dans une logique de recherche industrielle et académique et permettre la mise en relation avec des partenaires industriels pour le déploiement à grande échelle des solutions développées. Enfin, travailler avec des *think tanks* et des universités sur ces questions d'innovation participe à faire émerger une compréhension et une vision commune autour de l'évolution des technologies.
- Dans le **domaine monétaire**, ces partenariats impliquent la gestion des transactions financières à l'international, notamment en dollars, une connaissance approfondie de la fiscalité applicable dans chaque région du monde et une prise en compte des implications extraterritoriales des lois américaines dans le cadre de ces transactions en dollars.
- La **compliance** est un autre domaine critique, nécessitant une connaissance des juridictions locales pour garantir la conformité. Identifier des partenaires maîtrisant les spécificités juridiques locales, comme en Argentine, au Venezuela, en Chine ou en Russie, est essentiel. Par ailleurs, ces collaborations sont nécessaires pour le dépôt de brevets et pour effectuer une veille sur les brevets locaux.
- Pour la **fourniture des services vitaux** à l'entreprise, dans les domaines du cloud, des solutions SaaS et des télécoms, les fournisseurs locaux sont parfois incontournables dans certaines régions, notamment en Chine, où l'état oblige chaque entreprise étrangère à recourir à des

prestataires locaux si elle souhaite bénéficier de ces services. La diversité des régions où une entreprise opère rend parfois impossible ou compliqué de travailler avec un partenaire unique.

- Sur le plan de **l'accès aux marchés locaux**, ou « *go to market* », il est indispensable de comprendre la culture locale et, souvent, de collaborer avec des entreprises sur place. En Chine, par exemple, des partenariats locaux sont requis pour accéder au marché. Ces collaborations permettent également de bénéficier d'un support en matière d'acculturation, d'éducation et de formation dans les pays où l'organisation est active, tout en évitant une vision trop franco-centrique.
- La **standardisation** constitue une priorité pour certaines organisations, qui cherchent à uniformiser leurs procédures à l'échelle mondiale afin de faciliter leur déploiement. Cela peut se traduire par une participation à des consortiums multipartenaires pour établir des standards et des normes applicables à l'international.
- Enfin, la **gestion des ressources humaines IT** à l'international, dans le cadre de stratégie d'*offshoring* ou de *nearshoring*, peut nécessiter la conclusion de partenariats avec des agences locales pour faciliter l'accès à des compétences rares ou peu disponibles en Europe. Ces partenariats peuvent aussi se faire avec des entreprises françaises disposant d'implantations à l'étranger, notamment dans l'Union européenne, en Afrique du Nord ou en Inde.

Les partenariats d'innovation doivent être étudiés avec un regard attentif, car ils nécessitent souvent que l'entreprise allège ses procédures pour permettre des expérimentations nouvelles. Dans le cadre d'un travail collaboratif, il faut bien définir la propriété de chacun pour éviter toute concurrence par la suite.

| **Les partenariats d'innovation** | |
|---|---|
| Opportunités | Menaces |
| • Augmenter la clientèle de l'entreprise, grâce à l'acquisition de nouveaux marchés, et à l'évolution de son *business model.*<br>• Gagner en maîtrise technologique.<br>• Innover plus rapidement à des coûts moindres.<br>• Bénéficier d'un bassin d'expertise.<br>• Anticiper les besoins en compétences.<br>• Anticiper les investissements nécessaires.<br>• Se rapprocher des fournisseurs et faire évoluer la relation vers un dispositif partenarial.<br>• S'aligner sur les standards technologiques du marché. | • Concernant les partenariats avec les startups, la question de la propriété intellectuelle et le poids de l'entreprise dans le CA (risques de dépendance) doivent être consciencieusement évalués et monitorés.<br>• Risque de fuite de savoir-faire métier dans certains cas.<br>• Complexité des structures d'innovations dans l'Union Européenne.<br>• Difficulté d'intégration des nouvelles solutions dans le « *SI legacy* ».<br>• Risque de rachat des startups françaises par des acteurs étrangers.<br>• Risques de fuite de données sensibles. |

*Matrice des risques et opportunités sur les partenariats d'innovation*

Ainsi, en ce qui concerne les stratégies d'achat et de partenariat à l'international, les entreprises font face à des risques géopolitiques qui peuvent être directs (sanctions, conflits) ou indirects (effets en chaîne). Par exemple, un événement comme une guerre entre Taïwan et la Chine aurait des répercussions globales. Ce n'est pas uniquement le lieu d'achat qui importe, mais la globalité des facteurs géopolitiques qui doit être prise en compte.

- **Les risques de rupture dans la chaîne d'approvisionnement sont critiques**, notamment pour le matériel (*hardware*). Les difficultés de livraison entraînent des problématiques d'approvisionnement qui peuvent impacter la disponibilité des équipements. Les entreprises doivent influencer leurs fournisseurs pour être parmi les premiers à être livrés, afin de minimiser ces risques.
- **Les risques liés à la régulation** sont dus aux lois sur la protection des données (parfois utilisées par les gouvernements pour réguler les activités des entreprises) et aux lois sur la propriété intellectuelle, surtout dans les marchés où la réglementation peut varier significativement selon les pays.
- **Les risques de cybersécurité** se manifestent par des attaques ciblées sur des entreprises spécifiques, et sont souvent difficiles à gérer. Ces risques intègrent l'espionnage industriel qui est parfois complexe à détecter. Les fuites de données peuvent également provenir de pays alliés et ne sont pas uniquement les conséquences de menaces cyber, mais peuvent provenir de manipulation humaine, de la part de partenaires ou de fournisseurs ayant accès aux données.
- Certaines régions, comme le Venezuela ou la Turquie, présentent des **risques financiers** liés à la volatilité des taux de change. Les fluctuations peuvent en particulier entraîner des pertes importantes pour les entreprises entre le moment de la facturation et celui du paiement.
- **Les risques RSE** (responsabilité sociétale des entreprises) incluent la réputation, par exemple la gestion des employés dans des pays en conflit interne, comme au Myanmar. Les risques RH concernent la protection des employés et des sous-traitants dans des zones à risque, comme la Russie ou l'Ukraine. Les entreprises doivent également surveiller les sous-traitants pour éviter des incidents internes, comme des actions menées par des activistes au profit d'une cause de nature politique ou militante.

Pour le *software*, l'un des principaux enjeux est le maintien opérationnel de la solution. Il est souvent préférable d'acheter des solutions en Europe ou aux États-Unis pour en conserver l'expertise locale. Enfin, la juridiction spécifiée dans les contrats est également essentielle, car en cas de rachat d'un fournisseur européen par une entreprise d'un autre pays, le contrat pourrait changer de juridiction.

**La géopolitique des intelligences artificielles**

L'intégration d'outils d'intelligence artificielle au sein des organisations devient de plus en plus nécessaire pour rester compétitifs sur un marché mondial et faire évoluer les manières de travailler. Pour mener à bien cette intégration, il faut d'abord identifier les cas d'usages les plus pertinents, puis résoudre certains défis techniques liés au SI historique. Ces différentes préoccupations empêchent les directions du numériques de regarder vers d'autres conséquences du déploiement massif de ces outils, et ces conséquences sont de nature géopolitique, environnementale et réglementaire :

- **Consommation d'énergie et capacité de calcul** : l'IA est très énergivore et exigeante en termes de puissance de calcul.
- **Europe et autonomie stratégique** : l'Europe a davantage mis l'accent sur la réglementation que sur l'autonomie stratégique dans le domaine de l'IA. Le continent est ainsi absent sur le marché des systèmes d'exploitation (OS) et des moteurs de recherche. Par exemple, 75% des requêtes des citoyens européens sont effectuées sur Google. Google pratique l'économie de l'intention : en compilant les requêtes d'une entreprise, ils sont capables de reconstruire son plan stratégique. De même, les acteurs européens sont absents sur le marché du cloud. Enfin, en termes de *hardware*, l'Asie est leader, notamment sur le marché des semi-conducteurs.
- **Défis réglementaires** : les réglementations évoluent rapidement mais risquent de ne pas suivre le rythme des avancées technologiques. La réglementation américaine se positionne toujours au-dessus de la réglementation européenne. Cependant, en quoi la réglementation ne pourrait-elle pas être une force d'innovation, comme le RGPD qui a inspiré de nombreux pays dont les USA par la suite ?
- **Fuite des talents et des données** : la réglementation stricte sur la protection des données en France peut entraver le développement d'IA performantes. De plus, les chercheurs français migrent vers les entreprises américaines en raison de meilleurs investissements et salaires.
- **Financement et modèles économiques** : des investissements massifs dans l'IA sont effectués par des géants technologiques américains. La question du modèle économique européen pour l'IA est cruciale.
- **Fragmentation et centralisation des IA** : la fragmentation des IA pose des défis pour leur intégration dans les entreprises. Les petits modèles de langage (SLM) et les solutions open source sont des alternatives viables.

Face à ces différents défis, les directions du numérique disposent de plusieurs leviers d'actions :

- **Stratégies industrielles et géopolitiques** : des réflexions *by design* sont nécessaires pour faire face aux défis géopolitiques. Des approches visant à réduire la dépendance à certains fournisseurs sont à considérer.

- **Acteurs clés et alliances** : des alliances stratégiques et des investissements sont observés dans le secteur, comme l'acquisition d'ARM par NVIDIA.
- **Enjeux de fermeture et d'ouverture** : des débats sur la fermeture ou l'ouverture du marché pour favoriser l'émergence d'acteurs forts sont en cours.

**Fayçal BOUJEMAA**, *Technology Strategist*, chez ORANGE

## 2.2 LE RETOUR AU LOCAL : UNE STRATÉGIE DE RÉSILIENCE NUMÉRIQUE ?

Pour la sélection des fournisseurs, le choix se pose entre une stratégie de ***local sourcing*** ou une stratégie de ***global sourcing***. Par exemple, si un contrat monde avec un éditeur américain peut offrir certains avantages en termes de gestion, il présente des risques en cas de tensions géopolitiques. Une approche locale pourrait permettre de mieux répartir certains risques face à la fragmentation géopolitique croissante qui s'accentue avec la politique de la Chine et le conflit russo-ukrainien. Cette fragmentation remet en question la viabilité de certaines décisions d'*offshoring*, pour lesquelles les risques géopolitiques n'ont pas toujours été pris en compte initialement.

Lors de cette réflexion, il faut préciser ce que l'on entend par « local » : cela fait-il référence à une localisation en France, ou au contraire à une localisation en Inde ? Le choix des *hyperscalers*, qui ne couvrent pas certaines zones géographiques, peut être problématique pour les entreprises cherchant à se déployer à l'international. Il est donc nécessaire de bien évaluer les risques liés à chaque fournisseur.

Le développement d'une approche locale induit le plus souvent une fragmentation du SI d'un point de vue technique. Les entreprises se trouvent donc face à un dilemme en matière de stratégie de *sourcing* : est-il préférable de développer une approche la plus globale possible, et de faire face aux risques de dépendance à un fournisseur, ou bien est-il préférable de multiplier les partenaires et fournisseurs locaux, quitte à complexifier l'agencement du système d'information ? De manière générale, il est compliqué pour une entreprise de partir complètement sur un chemin ou sur un autre. Certaines stratégies IT sont pourtant mieux gérées quand elles s'inscrivent dans une dimension locale, au niveau de l'entreprise. La gestion de ses données au niveau local permet en effet à l'entreprise de conserver la maîtrise de son patrimoine informationnel, en garantissant la compatibilité de celui-ci avec son architecture technique globale. Par ailleurs, une stratégie plus locale implique généralement de développer des architectures IT agnostiques aux fournisseurs, notamment pour des questions de conformité aux différentes réglementations locales. Dans ce type de stratégie, il est tout de même nécessaire de développer une taxonomie et une gouvernance commune pour conserver une certaine homogénéité et une cohérence globale au niveau de l'organisation.

### 2.2.1 LE CONCEPT DE « *MAKE OR BUY* »

Le concept de *make or buy* est souvent mal compris, et encore limité à des considérations purement financières. Chez certaines entreprises, ce concept évolue néanmoins pour intégrer des aspects stratégiques. Ainsi, une approche open source peut répondre à la question du *make or buy* dans certains cas, notamment pour rapprocher la chaîne de valeur des activités critiques. Cependant, l'open source ne convient pas toujours. Pour des applications standards comme un ERP par exemple, le développement interne n'apporterait sans doute pas de valeur ajoutée. Construire un ERP en interne pour répondre aux risques géopolitiques pourrait être une solution, mais serait-elle viable à long terme ?

Certains pays, comme la Chine, développent leurs propres solutions pour se protéger des dépendances étrangères (par exemple, en construisant leur propre alternative à Salesforce). Toutefois, cette approche pose la question des ressources disponibles : tous les pays ou entreprises ont-ils les moyens de développer leurs propres CRM ou applications critiques ?

Le « *make* » n'est pas toujours nécessaire pour avoir un contrôle total. L'option *on-premise* peut être une première étape pour réduire les risques géopolitiques, bien que certains fournisseurs refusent cette solution. OVH Cloud, par exemple, vise à développer un ensemble de solutions entièrement en open source. Cela montre qu'une **stratégie hybride entre « *make* », « *buy* » et « *open source* »** peut offrir des avantages dans certains contextes.

## 2.3 ANTICIPER GRÂCE À UNE MEILLEURE CONNAISSANCE DES FOURNISSEURS

Dans l'organisation des achats, il existe deux approches distinctes : d'une part, la gestion des relations fournisseurs (*Vendor Management*) et, d'autre part, la fonction « achats » opérationnelle. Un enjeu important est de déterminer où intégrer le risque géopolitique dans cette structure. Il ne suffit pas de se contenter d'une simple matrice de risques. Il faut aller plus loin en adoptant une réflexion globale sur les bonnes pratiques organisationnelles, qui doivent inclure des éléments de gestion proactive des risques.

### 2.3.1 LES BONNES PRATIQUES POUR ANTICIPER LES RISQUES DE NATURE GÉOPOLITIQUE

Les bonnes pratiques à adopter incluent notamment la mise en place, dans les contrats fournisseur, de **clauses contractuelles spécifiques**, adaptées aux risques géopolitiques et conformes aux régulations en vigueur. Il est important de ne pas se limiter à une approche théorique, mais d'intégrer des mécanismes concrets dans l'organisation. Cela permet de mieux préparer l'entreprise à faire face à des situations imprévues. Le **partage des bonnes pratiques** à l'échelle de la réglementation et des contrats est également essentiel pour la gestion de ces risques.

En termes de stratégie, il est crucial de définir des éléments de consensus au sein de l'organisation, mais également de mettre en lumière les divergences qui peuvent exister. Cela permet d'avoir une vue

équilibrée et nuancée des risques, tout en favorisant des discussions constructives sur les orientations à suivre.

Dans un contexte où tout devient géopolitique, il est essentiel de fournir aux entreprises des éléments d'appréciation précis. Par exemple, la **signature des contrats sous une juridiction locale** peut s'avérer une bonne pratique pour réduire certains risques. Il est donc primordial de suivre les évolutions réglementaires et de s'y adapter pour mieux gérer les impacts des tensions géopolitiques.

Un autre point important concerne les **stratégies cloud**. Certains fournisseurs attirent leurs clients en limitant les options de réversibilité, captant ainsi une partie importante de la valeur. Cela pose un problème en matière d'autonomie stratégique et de risques géopolitiques. Le choix des services cloud est souvent dicté par la régulation : certains secteurs sont fortement encadrés, tandis que d'autres estiment que leurs données ne sont pas soumises à des risques géopolitiques et peuvent donc minimiser cette dimension dans leurs choix technologiques.

### 2.3.2 MIEUX SITUER ET MIEUX CONNAÎTRE LES RISQUES

Il est crucial de faire une **sélection des applications critiques** pour lesquelles il est nécessaire de répartir les risques géopolitiques. Les équipes doivent être formées à ces enjeux et comprendre la différenciation entre ce qui est « cœur de métier » et ce qui ne l'est pas. Cette réflexion doit s'inscrire dans une stratégie de résilience globale.

Trois niveaux peuvent être envisagés pour traiter les risques liés aux fournisseurs. Le premier niveau de risque est **stratégique**, et concerne les décisions globales qui peuvent être prises par le COMEX sur la localisation des applications et services IT. Chaque décision, que ce soit de l'internalisation, du *nearshoring* ou de l'*offshoring,* comporte des risques spécifiques quant à la gestion des fournisseurs. Le deuxième niveau concerne la **situation du fournisseur**, sa conformité aux différentes réglementations, sa localisation et son état financier. Chaque organisation doit avoir une bonne connaissance de ces informations au moment d'effectuer son choix et dans toute la relation avec le fournisseur qui s'ensuit. De manière pragmatique, cela signifie qu'il faut réaliser une *due diligence* à l'*onboarding* de chaque fournisseur et réaliser un suivi continu sur ces différents critères. Enfin, le troisième niveau se concentre sur les **services**, et spécifiquement sur les risques qui peuvent advenir dans le cadre du service rendu par le fournisseur et de son introduction dans le système d'information de l'entreprise (extraction de données, espionnage…).

Il est donc essentiel pour les entreprises d'adopter une pratique de « ***Know Your Supplier*** **» (KYS).** Cela permet de partager une grille de lecture commune et d'intégrer des analyses géopolitiques dans les processus de sélection des fournisseurs.

Le secteur bancaire peut servir d'exemple à cet effet, car il est fortement régulé. La mise en place d'une gouvernance IT structurée en plusieurs niveaux (niveau 1 : raison d'être & stratégie ; niveau 2 : structuration IT ; niveau 3 : déploiement des entités) permet d'assurer une continuité dans les pratiques et de garantir la conformité des opérations dans un environnement géopolitique complexe.

## 2.4 FAIRE LES BONS CHOIX STRATÉGIQUES

La dimension géopolitique doit être intégrée dans toutes les activités de la direction du numérique. Il ne s'agit pas seulement de s'intéresser aux contrats, mais de revoir l'ensemble des processus pour garantir la résilience des systèmes et des choix technologiques.

### 2.4.1 CONCEPTION D'ARCHITECTURES RÉSILIENTES

Il est essentiel de concevoir des architectures de solutions qui tiennent compte des spécificités géographiques et des risques locaux. Chaque plaque géographique doit avoir sa propre solution adaptée aux contextes légaux et géopolitiques.

*Outil recommandé : Une grille de lecture architecturale, similaire aux pratiques éthiques et RSE pourrait être utilisée pour partager les meilleures pratiques avec les équipes. Cela impliquerait de suivre les réglementations locales et de sensibiliser à l'impact de la géopolitique sur les choix IT.*

### 2.4.2 RÉSILIENCE OPÉRATIONNELLE DANS LES CHOIX IT

La résilience doit être pensée dès la conception des systèmes : choix de solutions, architectures robustes, diversification des infrastructures. La résilience devient alors un critère central dans les décisions IT.

*Outil recommandé : Un framework complet qui inclut la gestion des risques géopolitiques, le suivi des fournisseurs et l'adaptation des architectures IT doit être élaboré pour garantir une révision continue des pratiques. Cela inclut également l'intégration d'une culture d'entreprise qui valorise la résilience comme un élément clé de la stratégie.*

### 2.4.3 GESTION DES FOURNISSEURS

Le suivi des fournisseurs ne doit pas se limiter aux aspects commerciaux. Il est essentiel de connaître non seulement leur situation financière, mais aussi leur localisation, les risques géopolitiques associés, et leur conformité avec les réglementations locales. Une stratégie de résilience implique de cartographier les fournisseurs critiques pour les services *business* et de maintenir un monitoring continu des risques géopolitiques. Bien que cela soit coûteux, cette approche permet d'identifier les menaces potentielles avant qu'elles n'affectent l'activité. La diversification du *sourcing* est un élément essentiel de la résilience, qui se heurte souvent à des contraintes de coûts, en particulier lorsque les services achats privilégient la maîtrise des coûts au détriment de la prise en compte des risques.

*Outil recommandé : Une cartographie des fournisseurs critiques, mise à jour régulièrement.*

Il est important d'anticiper les risques liés à la dépendance vis-à-vis d'un fournisseur. Une défaillance ne traduit pas seulement une faillite, mais peut aussi être le résultat d'un rachat ou d'une modification des conditions d'utilisation. Le « *Vendor Management* » doit intégrer cette gestion des risques. Il faut mettre en place des revues périodiques des risques et des pratiques associées, pour intégrer de façon continue la dimension géopolitique dans les stratégies d'achat et de gestion des fournisseurs. Ce *framework* devrait être inclus dans les processus de gouvernance IT.

Il est crucial de diversifier les implantations géographiques pour éviter de concentrer les risques dans un seul pays. Par exemple, dans la mise en place de serveurs, il est recommandé de ne pas centraliser toutes les infrastructures dans une seule région géopolitique sensible, mais d'envisager des alternatives plus sûres.

*Outils recommandés :*

- *Une liste de questions spécifiques à poser lors de l'engagement avec un fournisseur pour évaluer sa résilience et sa capacité à réagir face à des événements imprévus.*
- *Une revue périodique de la résilience des fournisseurs critiques en matière géopolitique.*

La gestion des fournisseurs ne doit pas être uniquement le domaine des achats. Il est nécessaire de redéfinir les missions des équipes en charge du « *Vendor Management* » pour inclure cette dimension de résilience et d'ancrage géopolitique. Un nouveau rôle pourrait être créé, avec des responsabilités spécifiques pour garantir la mise en place des processus résilients, en lien avec les métiers.

*Outil recommandé : Création d'une nouvelle fiche de poste pour un « Vendor Manager » avec une mission de pilotage des processus de résilience.*

# 3 POLITIQUES RH-IT DANS UN CONTEXTE INTERNATIONAL TROUBLÉ

Dans un contexte international instable, les politiques RH-IT sont confrontées à de nombreux enjeux liés aux recrutements et à la gestion des talents dans les différents pays. Si la pénurie de compétences numériques incite les entreprises à recruter au-delà de leurs frontières, des facteurs comme la complexité des réglementations locales, les risques géopolitiques et les particularités culturelles influencent fortement ces choix. L'enjeu est de taille : il s'agit non seulement d'assurer la continuité et la résilience des activités IT, mais aussi d'adopter des pratiques de recrutement qui intègrent une vision équilibrée des risques et des opportunités liés aux différents marchés. La DSI, en collaboration avec les équipes RH, doit ainsi développer des stratégies de gestion des talents et de localisation des compétences adaptées aux réalités de chaque région, tout en renforçant la souveraineté technologique de l'entreprise.

## 3.1 PÉNURIE DES COMPÉTENCES : SEULE RAISON DU RECRUTEMENT IT À L'INTERNATIONAL ?

Les stratégies d'implémentation RH-IT des entreprises dépendent fortement des régions où elles mènent leurs activités. Selon l'organisation de la direction numérique, il est ainsi nécessaire de disposer d'équipes IT locales pour mener les activités dans différentes régions, et être ainsi au plus près des équipes métiers. Cependant, une DSI avec une organisation plutôt centralisée, délivrant des services aux différentes régions de l'entreprise, n'aura pas forcément besoin de se délocaliser pour des raisons de continuité d'activité à l'international.

Au-delà de ces nécessités liées à l'activité de l'entreprise, il existe des spécificités du recrutement et des facteurs de considération différents dans l'IT et dans le reste de l'entreprise. Le numérique en Europe fait face à une pénurie de talents, et ce particulièrement dans des secteurs stratégiques comme la data, l'IA et la cybersécurité. Les formations peinent à s'adapter aux besoins croissants des entreprises, et ne peuvent combler la diminution des possibilités d'offshore et d'externalisation des activités IT.

Ainsi, un facteur clé dans **le choix des pays de recrutement** est leur capacité locale à former suffisamment d'ingénieurs, comme c'est le cas en Inde et en Russie. L'objectif de féminisation des équipes IT joue aussi un rôle pour des pays comme l'Inde et la Pologne où la parité est mieux équilibrée. L'ouverture culturelle est essentielle, mais les différences peuvent aussi poser des défis managériaux.

Il existe des sites pour classer les pays en fonction de certains critères (environnement, transport…) :

- Forces/faiblesses des pays pour y installer une activité : https://www.prosperity.com/rankings
- Une base de référence sur les Job descriptions afin de comparer les profils : https://www.wtwco.com/fr-fr/solutions/remuneration-globale

La **question de la langue** est également à prendre en compte. Les échanges se font principalement en anglais, mais les managers doivent adapter leur communication en fonction des cultures locales.

L'impatriation de talents rencontre souvent des obstacles légaux, notamment pour des profils en provenance du Maroc, d'Inde, ou de Chine.

La question du recours aux prestataires pour mener l'activité à l'international est une autre problématique. Les prestataires peuvent être employés pour des projets spécifiques mais rarement pour des activités stratégiques. De plus, généralement, le recours aux prestataires varie selon les régions, car la montée des salaires dans certaines zones et la complexité des processus peuvent compliquer le recrutement.

La **taille des activités transférées** est cruciale. En dessous d'un seuil critique de 200 collaborateurs, cela devient complexe d'assurer la viabilité d'une implantation. Il faut éviter d'ouvrir des antennes de l'entreprise dans des régions où les besoins en ressources sont trop faibles.

**Stratégies d'implantation RH-IT : REX des entreprises**

**Orange**

- En dehors de la France, les équipes *IT corporate* sont présentes en Inde, Roumanie, Maroc, Tunisie, et Égypte. Des DSI locales sont évidemment présentes dans tous les pays.
- Nos présences géographiques nous permettent d'adresser les aspect souveraineté, réglementaires, sécuritaires tout en optimisant les coûts de structure.
- La compétition est intense dans le secteur des télécoms, l'optimisation des coûts et des implantations est cruciale.

**BNP Paribas**

- Présence dans 65 pays, avec quelques pôles régionaux pour son IT (Paris-Madrid, Singapour - Mumbai, New York - Toronto).
- 10 000 collaborateurs sur la partie IT pour la banque d'investissement, avec 6-7 000 en Inde (Mumbai, Bangalore).
- Stratégie « *follow the sun* » pour garantir la disponibilité continue des outils IT.
- Siège des décisions à Paris/Londres, mais diversification en Espagne, Pologne, et Roumanie de la production IT européenne.

**Michelin**

- Développement global : Clermont-Ferrand (Europe), Greenville (Amérique), Shanghai (Asie), Inde (Pune).
- Équilibre 50/50 entre collaborateurs internes et prestataires. Chaque région a son propre DSI rattaché au DSI groupe.
- Acquisition de nouvelles équipes locales par réseautage et intégration progressive.

**Stéphane DEMARTIS**, *VP Cloud Infrastructure Solutions and Services*, chez ORANGE,

**Eric FICHOT**, *Head of HR for CIB functions*, chez BNP PARIBAS,

**Julien MARTINO**, *CRM Enterprise Architect,* chez MICHELIN.

## 3.2 LES RISQUES LIÉS AUX RECRUTEMENTS INTERNATIONAUX

Dans le contexte des politiques de recrutement, la **citoyenneté et la nationalité** peuvent poser problème dans le cadre de conflits régionaux entre différentes ethnies, ou pour effectuer des tâches particulièrement sensibles touchant à la politique des états. Par exemple, recruter une collaboratrice d'origine pakistanaise en Inde peut soulever des interrogations sur les visas et l'intégration sociale. Au-

delà de cet aspect administratif, les tensions géopolitiques peuvent compliquer le transfert de projets entre pays, comme un déplacement d'activité de la Chine vers l'Inde, nécessitant une communication adaptée pour apaiser les éventuelles tensions parmi les équipes locales.

Les entreprises doivent aussi gérer des **questions de sûreté** lorsqu'elles envoient des collaborateurs dans des régions sensibles. En Chine, par exemple, envoyer des personnes sans liens familiaux forts peut réduire le risque de pressions locales. Le choix du *sourcing*, tant pour les talents que pour les compétences, peut alors devenir un levier pour minimiser ces risques. Bien que les entreprises puissent anticiper certaines menaces géopolitiques, elles ne peuvent les éviter complètement. Il devient alors essentiel d'être attentif aux choix de *sourcing*, notamment dans le domaine logiciel où la nationalité des talents peut avoir un impact sur les projets. Les processus de recrutement se complexifient donc en raison des vérifications de *background*, indispensables pour éviter les risques potentiels.

Par ailleurs, l'utilisation de logiciels locaux impose de disposer de compétences spécialisées, tandis que les outils de collaboration sont soumis aux **réglementations locales**, comme en Chine, où des solutions comme Microsoft Teams peuvent être difficiles à utiliser. Pour compenser ces contraintes, certaines entreprises choisissent de privilégier la maîtrise interne de leurs logiciels. Les entreprises doivent aussi s'assurer du respect d'autres réglementations locales, comme l'équivalent chinois du RGPD. Pour les données des collaborateurs, par exemple, la centralisation en France peut poser des difficultés en matière de réglementation, car la Chine exige que les données de ses ressortissants soient stockées localement.

L'évolution géopolitique de certains pays demande également une vigilance accrue. Il peut être nécessaire de surveiller la situation des pays dans lesquels l'entreprises est présente pour gérer les équipes sur place en cas de déclenchement d'un conflit. Certains événements géopolitiques, comme le « printemps arabe » en Égypte, ont également montré l'impact des crises locales sur les stratégies basées sur le coût, nécessitant parfois des ajustements rapides. En Israël, par exemple, la stabilité politique demeure un enjeu pour les entreprises qui y sont implantées.

En plus des risques géopolitiques, **des facteurs environnementaux**, tels que les inondations durant la mousson en Inde, peuvent également perturber les activités.

Enfin, la diversification des équipes à l'étranger permet de limiter la **dépendance aux compétences locales** et de renforcer la résilience de l'organisation.

## 3.3 PERSPECTIVES FUTURES DU RECRUTEMENT À L'INTERNATIONAL ET NOUVEAUX ENJEUX

Les entreprises pourraient à l'avenir intégrer les notions émergentes de « *friend-shoring* » ou « *ally-shoring* » pour se concentrer sur des partenariats sécurisés, d'un point de vue géopolitique, pour leurs cœurs d'activité. Cela représenterait un retour vers des prises de décision plus locales, en contraste avec les stratégies de mondialisation des vingt dernières années. Cette régionalisation permet de faire émerger au niveau régional des réseaux de compétences et d'expertises qui renforcent les savoir-faire locaux.

De plus, le recrutement international, dans un contexte de forte réglementation, pose la question de l'évolution des profils recherchés en *offshore*, notamment dans le domaine IT, où les besoins pourraient diminuer en raison de la croissance de l'automatisation de certaines fonctions.

**Perspectives économiques, politiques et culturelles sur l'Inde**

En France, le « risque indien » est souvent sous-estimé, malgré le fait que la France soit le deuxième fournisseur d'armes de l'Inde et que l'État français s'appuie sur la présence de ses entreprises dans le pays pour des raisons économiques. L'Inde possède une capacité de résistance qui l'empêche d'être facilement influencée par un seul bloc géopolitique. Contrairement à la Chine, dont le risque est lié à une possible guerre avec les États-Unis, l'Inde adopte un pragmatisme opportuniste, lui permettant de naviguer dans le contexte géopolitique actuel. Économiquement, elle est devenue un acteur majeur, et la plupart des entreprises du CAC40 y sont présentes de manière directe ou indirecte. Le secteur numérique est le premier secteur économique indien, avec des dirigeants souvent formés dans les universités américaines.

Le nationalisme hindou actuel, incarné par le régime au pouvoir, entraîne des tensions importantes. Bien que l'Inde soit majoritairement hindoue (près de 90 %), des tensions interreligieuses et interethniques subsistent, particulièrement lors des élections. Le nationalisme hindou est parfois qualifié de fasciste en raison de violences, de pogroms, et d'attaques contre des églises. Ces tensions sont renforcées par des clivages géographiques et culturels entre le nord, moins développé, et le sud, où les centres économiques tels que Mumbai et Bangalore prospèrent. Un clivage existe aussi entre l'est et l'ouest, notamment autour de Calcutta. En 2017, une réforme monétaire du gouvernement a considérablement impacté le PIB, reflétant les divisions économiques et les intentions politiques d'affaiblir les partis d'opposition.

La gestion du COVID-19 a également eu des conséquences économiques et sociales importantes, accentuant les divisions. Cependant, il n'y a pas de risque de sécession nord-sud, car les États indiens ont une autonomie politique importante, ce qui fait d'eux des interlocuteurs privilégiés pour les entreprises étrangères. Les prévisions pour les prochaines élections montrent une possible stabilisation de la vague populiste, suggérant que l'Inde ne basculera pas entièrement vers un populisme extrême. Malgré ce contexte géopolitique complexe, le risque politique reste contenu.

Sur le plan économique, l'Inde fait face à de nombreux défis. Bien que sa population soit nombreuse, le pays peine à fournir des emplois qualifiés. Le secteur de l'IT, bien qu'important, ne suffit pas à faire vivre toute l'économie. Le réchauffement climatique a également des conséquences sur la santé de la population et sur la productivité. Les villes indiennes, déjà insoutenables en termes d'approvisionnement en eau et en électricité, souffrent de graves problèmes sanitaires. Les centres *offshore*, souvent bien pourvus en infrastructures, sont relativement épargnés, et la crise COVID a montré l'ampleur de l'*outsourcing*, avec une augmentation du travail à domicile, géré par les entreprises elles-mêmes plutôt que par l'État.

Concernant les forces de l'Inde, le capital humain est important. Bien que le niveau moyen d'éducation soit bas, certaines écoles privées offrent des formations de très haut niveau,

souvent influencées par le système des castes. La culture indienne, riche et intellectuellement articulée, repose sur des textes comme les « cinq livres », un recueil de fables qui traite de la nature humaine et des relations sociales. Cette tradition offre à l'Inde un *soft power* unique, soutenu par la diffusion du yoga et une culture du végétalisme adoptée par environ 40 % de la population.

Sur les questions de politique étrangère, l'Inde adopte une posture opportuniste, cherchant à maintenir de bonnes relations avec ses principaux partenaires commerciaux, notamment la Russie et la Chine, malgré les conflits actuels. Elle ne souhaite pas basculer dans une bipolarité entre les États-Unis et la Chine, ce qui explique une stratégie d'équilibre dans ses relations internationales. Si une guerre éclatait entre la Chine et les États-Unis, l'Inde serait forcée de choisir un camp, ce qu'elle essaie d'éviter en maintenant des relations de bon voisinage, sauf avec la Chine, avec laquelle les tensions sont contenues par une forme de compétition indirecte dans les pays voisins.

En matière de société, l'évolution des rapports hommes-femmes est marquée par une montée des conservatismes. Les espoirs de modernité des années 60 ont cédé à une forme de désillusion, et le concept de modernité est aujourd'hui en retrait. L'image de la femme reste fortement influencée par les spécificités régionales. Le système des castes favorise une certaine mobilité sociale et économique, contribuant à un esprit entrepreneurial. Historiquement, l'Inde a connu une prospérité économique jusqu'au XVIIIe siècle, renforcée par un rapport au temps et aux croyances influencé par la réincarnation et les cycles de vie.

Face aux défis climatiques, la philosophie indienne privilégie la frugalité. La consommation par habitant reste faible, bien qu'une autre Inde, plus pragmatique, s'oriente vers l'accumulation de richesses sans trop se soucier des conséquences environnementales. Le pays adopte une gestion court-termiste de ses ressources, préférant des solutions au cas par cas, un état d'esprit qui favorise une résilience face aux crises mais qui pourrait freiner son développement à long terme.

**Jean-Joseph BOILLOT**, professeur agrégé de sciences économiques et sociales et docteur en économie, spécialiste des grandes économies émergentes, notamment la Chine et l'Inde

# 4 INTÉGRER LA DIMENSION GÉOPOLITIQUE À LA GOUVERNANCE DE LA DSI

Prendre en compte les aspects géopolitiques au sein de la DSI demeure complexe : cela nécessite une compréhension fine des enjeux globaux et une capacité d'anticipation qui ne font pas encore partie des réflexes IT dans la plupart des organisations. Pour véritablement renforcer la résilience et l'agilité de la DSI face aux aléas géopolitiques, une démarche structurée est indispensable, impliquant une collaboration étroite entre les différentes directions de l'entreprise, *business* (lignes métiers) et support (achats, informatique, juridique, finance…), et un partage régulier et proactif d'informations. Cette partie explore les défis, les étapes clés et les bonnes pratiques pour structurer cette gouvernance, en visant à doter la DSI d'outils prospectifs, adaptés à un contexte international de plus en plus instable.

## 4.1 POURQUOI EST-CE COMPLIQUÉ D'INTÉGRER LA DIMENSION GÉOPOLITIQUE À LA DSI ?

L'intégration de la dimension géopolitique à la DSI se heurte à des obstacles majeurs, principalement liés à l'absence de processus formalisés et à une sensibilité inégale parmi les collaborateurs. Actuellement, la prise en compte des risques et enjeux géopolitiques repose surtout sur la perception individuelle et l'expérience des équipes, sans cadre structuré ni réflexion commune. Tandis que des analyses prospectives sont souvent menées pour anticiper les impacts géopolitiques sur le cœur de métier de l'entreprise, cette même approche fait défaut dans le domaine IT. Cette absence de réflexion prospective dédiée à l'IT laisse les DSI exposées aux vulnérabilités géopolitiques sans outils formels pour les évaluer et les intégrer dans leurs stratégies technologiques.

## 4.2 PRENDRE EN COMPTE LA DIMENSION GÉOPOLITIQUE : UNE NÉCESSAIRE COLLABORATION AU SEIN DE L'ENTREPRISE

### 4.2.1 METTRE EN PLACE LA BONNE GOUVERNANCE

Nous l'avons bien vu tout au long de ce rapport, les éléments à prendre en compte pour orienter la stratégie numérique en fonction des fluctuations géopolitiques sont multiples et peuvent affecter les différentes activités d'une direction du numérique (achats, partenariats, RH, juridique…). Prendre en compte cette dimension géopolitique nécessite donc une collaboration et un travail de surveillance continue au sein de l'entreprise.

Les **directions des risques, de la conformité et de la sûreté** ont intrinsèquement une culture de la prévention, nécessaire pour anticiper les conséquences de nature géopolitique. S'inspirer de leurs pratiques de prévention, telles qu'elles peuvent aussi exister en cybersécurité, est une première étape. Il faut ensuite intégrer la dimension géopolitique dans les processus de gestion du risque et l'infuser dans les procédures, revues achats ou architecture des projets IT. La diffusion de cette culture doit ensuite passer par la mise en place de programmes de sensibilisation et de formation dans toutes les

équipes, pouvant inclure de la *gamification* (par exemple, via des mises en situation au travers de « *war games* », permettant de mieux comprendre les enjeux et d'améliorer les partages au sein de l'entreprise) pour renforcer l'engagement et mieux faire intégrer les risques. En plus d'être des sources d'inspiration par leur culture de la prévention, ces trois directions ont également connaissance de nombreuses informations nécessaires à une analyse complète de l'impact des évolutions géopolitiques sur la direction du numérique.

Si la **DSI et les entités relatives à la sécurité numérique** de l'organisation sont de toute évidence au cœur de la réflexion, elles ne sont pas nécessairement au cœur de l'organisation de la démarche. Celle-ci est généralement menée par la direction des risques et les directions métiers, l'IT restant généralement une « fonction support » au service du *business*. Cette direction dispose, en effet, de toutes les informations relatives à l'activité numérique de l'organisation et doit donc proposer ses analyses pour contribuer à la démarche.

Enfin, la **direction juridique** garde un regard attentif sur l'évolution des corpus réglementaires à travers le monde, et sur les nouvelles sanctions internationales, surtout dans les régions où l'organisation est présente (sur le volet numérique ou non).

Il est important que ces différentes entités partagent en continu leurs informations, car une information anodine pour l'une, peut s'avérer impactante pour l'autre. Ce partage d'informations doit permettre ensuite d'alimenter **une veille IT et une réflexion prospective IT, adossées à la réflexion prospective *business***. La cellule de veille et prospective IT ne se trouve pas nécessairement à la DSI qui reste essentiellement contributive, et peut être accolée aux cellules d'autres départements du même type. Il faut cependant que la réflexion sur les futurs numériques soit menée, dans un premier temps, indépendamment des autres réflexions prospectives de l'entreprise, car les implications géopolitiques ne sont pas forcément les mêmes sur le numérique et sur le secteur d'activité de l'entreprise. Cette cellule de « prospective IT », vient ensuite proposer ses analyses et alimenter la direction de la stratégie de l'entreprise et ses travaux font l'objet de présentations au COMEX. Cette cellule, nommée ici « prospective IT », peut prendre différents noms et formes en fonction des organisations : « veille IT », « stratégie IT », ou encore « intelligence économique IT ». Ce dernier type de cellule moins large et plus orientée que la prospective, peut-être plus légitime à aborder ces questions de géopolitique. Quoi qu'il en soit, son objectif sera d'amener des pistes de réflexion sur les adaptations et/ou les mutations à mettre en place au sein de la DSI pour faire face aux évolutions géopolitiques, mais aussi techniques, réglementaires et sociales.

Pour s'assurer qu'un tel dispositif de partage et de collaboration tienne sur le long terme, il est généralement nécessaire qu'un suivi et une animation soient effectués. Ce travail de supervision peut être confié à la **direction des affaires publiques**, ou à une direction de la stratégie, ou encore une structure rattachée à la direction générale.

Enfin, il est nécessaire de coopérer avec la **direction en charge des questions RSE**, car elle est amenée à traiter de certaines questions essentielles comportant des dimensions en matière de géopolitique, de risques et de conformité réglementaire.

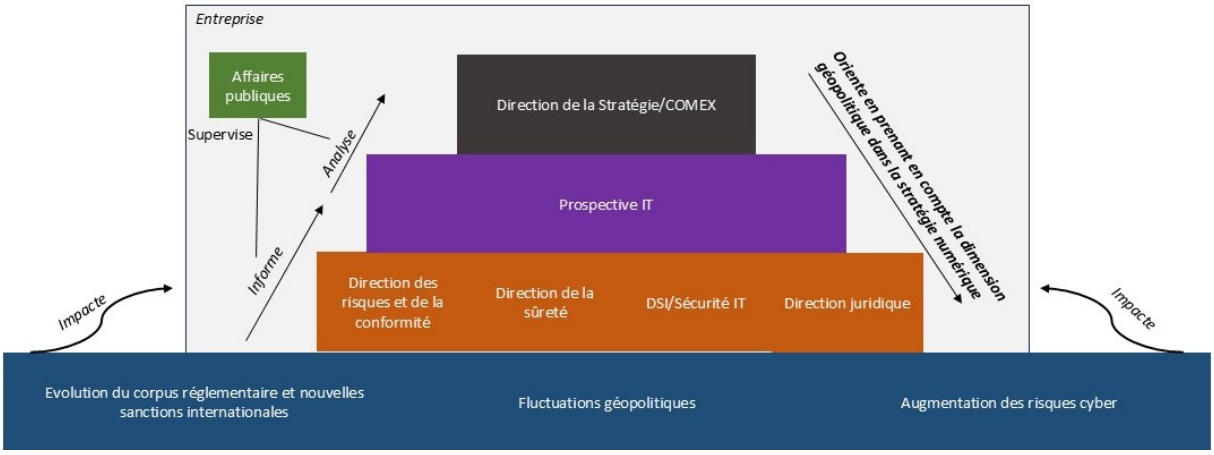


*Schéma de gouvernance pour intégrer la dimension géopolitique aux activités IT*

Au-delà des aspects de gouvernance, toutes les équipes, dans chaque pays où est implantée l'entreprise, doivent participer à cette réflexion prospective pour intégrer les perspectives géopolitiques locales et spécifiques. L'objectif final est ainsi de constituer **un écosystème de gestion des risques géopolitiques et une communauté de veille,** avec une organisation qui intègre les risques géopolitiques dans l'ensemble des processus décisionnels et opérationnels.

### 4.2.2 COLLABORER AVEC LES BONS OUTILS

La cellule de « prospective IT » permet de générer et de mettre à disposition des outils communs :

- **Des scénarios précis des évolutions potentielles de la scène géopolitique en fonction des enjeux IT de l'entreprise** : pour anticiper les impacts des évolutions géopolitiques sur les enjeux IT des entreprises, il est indispensable d'élaborer des scénarios intégrant à la fois les dimensions géopolitiques et climatiques, et une analyse macroéconomique et réglementaire, selon les besoins spécifiques. Afin de garantir leur pertinence, un processus de révision doit être mis en place tous les 6 à 12 mois, pour ajuster ces prévisions en fonction des changements dans l'environnement global. Par ailleurs, la mise en œuvre d'exercices de simulation permet de plonger les équipes dans ces scénarios complexes, les confrontant à des situations critiques pour mieux anticiper les impacts potentiels sur leurs opérations numériques. Le « *war gaming* », un dérivé de ces exercices de simulation, se répand par exemple de plus en plus dans les administrations publiques. Enfin, l'analyse des risques géopolitiques ne doit pas se limiter aux pays non-occidentaux. La crise énergétique en Allemagne, accentuée par la guerre en Ukraine, en est un exemple frappant : la soutenabilité énergétique, notamment pour les datacenters, est devenue un enjeu crucial, démontrant que les pays développés ne sont pas exempts de risques significatifs.
- **Une cartographie et un processus de revue régulière des fournisseurs :** élaborer une cartographie précise des fournisseurs, en identifiant les risques géopolitiques associés à chaque partenaire stratégique, est un premier pas vers une meilleure prise en compte des risques géopolitiques à la DSI. Mettre en miroir cette cartographie avec les scénarios prospectifs permet de visualiser les impacts potentiels des différentes relations fournisseurs.

Cette cartographie doit ensuite être régulièrement revue et approfondie pour éviter de passer à côté de certains risques.

- **Un exemplier de cas concrets mêlant implications géopolitiques et numérique :** la sensibilisation de l'ensemble de l'organisation est le premier objectif d'une telle démarche, car l'impact géopolitique sur l'activité numérique est souvent méconnu, ou sous-évalué. Présenter régulièrement aux équipes des exemples concrets d'impacts géopolitiques sur l'entreprise et son IT, permet de renforcer la compréhension des risques. Cet exemplier peut prendre différentes formes, et servir par exemple à la formalisation d'outils de formation et de sensibilisation (comme des MOOCs) à destination de toute l'entreprise.
- **Une documentation interne partagée et mise à jour régulièrement :** diffuser la documentation stratégique en interne permet de partager des informations qui pourraient paraître anodines à certains mais être stratégiques pour d'autres. Cette documentation doit inclure des lignes directrices pour prendre en compte ces risques dans les différentes activités IT de l'entreprise. Les affaires publiques peuvent ensuite se charger de transmettre ces informations au COMEX et au reste du groupe pour une prise de conscience globale.

### 4.2.3 LIMITES ET PÉRENNITÉ DE L'APPROCHE

La mise en place d'un tel dispositif est bien évidemment très gourmande en ressources humaines et financières. La gouvernance et les outils proposés doivent donc s'adapter aux habitudes de l'organisation. Cependant, il nous apparait primordial que la prise en compte de la dimension géopolitique dans la stratégie IT soit appuyée par une gouvernance, aussi légère soit-elle, pour s'assurer que le sujet soit suivi et documenté malgré les obstacles potentiels. De plus, l'intégration des schémas de prospective IT avec ceux du *business* reste un défi, car ces scénarios sont généralement de court à moyen terme (maximum 3 ans).

Pour que ce dispositif fonctionne, il nous apparait primordial d'organiser des réunions physiques mensuelles (en alternance avec des réunions en visioconférence pour intégrer les territoires distants) pour faciliter l'échange et l'actualisation des connaissances. Il ne faut pas s'en tenir à de la documentation partagée.

**Travailler avec la direction juridique : une nécessité pour la DSI**

*Disclaimer : le texte ci-après est un résumé d'une intervention de Martin PAILHES, Responsable Juridique Digital chez BNP Paribas, qui a eu lieu au CIGREF le 26/09/24 sur le thème « Intégrer la dimension géopolitique aux activités de la DSI ». Les propos exprimés n'engagent que leur auteur et non la société pour laquelle il travaille.*

2024 est une année politiquement très chargée. Plus de la moitié du monde a voté cette année, avec 64 pays appelés aux urnes, dont Taïwan, le Royaume-Uni, l'Inde et bien évidemment les États-Unis. Par ailleurs, alors que la guerre fait rage en Ukraine et au Moyen-Orient, nous observons la montée d'un bloc de pays menés par la Chine, la Russie et l'Iran, visant à remettre en cause l'ordre occidental établi après la chute du mur de Berlin.

Il est essentiel de garder à l'esprit ce panorama mondial, car les instruments juridiques adoptés par des États dans ce contexte (par exemple, les lois à portée extraterritoriale, les sanctions émises par un État contre d'autres États ou certains de leurs ressortissants ou entreprises) peuvent avoir un impact significatif sur les activités quotidiennes des DSI.

Les exemples suivants illustrent ce point, notamment dans le domaine du digital où des technologies sensibles voire duales sont souvent impliquées :

**Transferts internationaux de données hors de l'UE : vers l'affirmation d'une souveraineté européenne ?**

Les données sont un enjeu majeur de souveraineté pour les États et un facteur clé du fonctionnement des organisations dans une économie mondialisée. Cependant, leur circulation est de plus en plus encadrée par des lois, en particulier en Europe, pour des questions de souveraineté et de protection des citoyens. L'exemple le plus parlant est le RGPD pour les données personnelles dans l'UE, adopté en réponse à des lois américaines jugées intrusives et non respectueuses des libertés individuelles, prises après les attentats du 11 septembre 2001.

Face à ces défis, des initiatives comme Gaia-X, visant à garantir un cloud européen souverain, illustrent les ambitions d'autonomie numérique de l'Europe, bien que leur application reste difficile à mettre en œuvre.

**Des sanctions de plus en plus nombreuses entraînant une augmentation des risques pour les DSI**

Avec la guerre en Ukraine, nous assistons à une succession de sanctions de la part des États-Unis et de l'UE contre la Russie. L'arme des sanctions économiques n'est pas nouvelle, comme en témoignent les sanctions américaines contre Cuba, l'Iran, la Corée du Nord, etc. La DSI peut être confrontée au respect de ces sanctions de manière inattendue :

- Lors de *ransomwares* : Le paiement d'une rançon devient un dilemme complexe si le cybercriminel est affilié à un pays sous sanctions, comme l'Iran, Cuba ou la Russie.

- Droit de propriété intellectuelle en Russie : *quid* de renouveler, par exemple, ses marques en Russie aujourd'hui ?
- Embauche accidentelle d'employés nord-coréens : les autorités alertent contre un risque croissant posé par des individus postulant à des emplois dans le domaine informatique, qui opèrent en réalité pour le compte de la Corée du Nord. Ces candidats cherchent à infiltrer les systèmes informatiques des entreprises occidentales et à générer illicitement des revenus pour le régime nord-coréen.

**Conclusion** : aussi lointaine qu'elle puisse paraître, la dimension géopolitique peut avoir de sérieuses conséquences pour les DSI. Il est donc crucial pour ces derniers d'identifier et d'anticiper ses impacts.

**Martin PAILHES,** responsable de la Plateforme Digital & IP de la Fonction Juridique du Groupe BNP PARIBAS

# 5 CONCLUSION : VERS UNE DSI PROACTIVE FACE AUX FLUCTUATIONS GÉOPOLITIQUES

Nous semblons assister aujourd'hui à un renversement des règles qui régissaient les échanges internationaux et les activités des entreprises depuis au moins les vingt dernières années, autour d'une mondialisation heureuse. En effet, nous nous dirigeons vers une « dé-mondialisation » (un monde de blocs) qui aura sans doute pour conséquence de raviver les questions géopolitiques avec des exemples techniques symboliques comme la fragmentation d'internet ou « splinternet ».

Parallèlement, face à l'importance croissante du numérique dans l'ensemble de leurs opérations, la DSI, autrefois perçue comme une simple fonction de support, occupe aujourd'hui une position centrale dans la stratégie des entreprises. Cette évolution a transformé la DSI en un acteur stratégique, essentiel pour anticiper les défis et les opportunités, notamment dans un contexte mondial marqué par des mutations géopolitiques majeures. Intégrer ces réflexions géopolitiques au sein de la gouvernance IT, comme exploré tout au long de ce rapport, est une réponse nécessaire à cette transition du numérique, qui exige désormais une capacité d'adaptation rapide et une vision prospective.

Toutefois, cette démarche reste encore émergente, comme en témoigne la participation relativement limitée rencontrée par le groupe de travail à l'origine de ce rapport. Ce faible engagement souligne l'importance d'accroître la sensibilisation autour de ces enjeux géopolitiques au sein de la DSI. Il s'agit d'un défi crucial à relever pour renforcer la résilience numérique de l'entreprise et ancrer durablement une culture de vigilance proactive face aux risques internationaux. En continuant de sensibiliser et de former les équipes IT à ces dynamiques mondiales, la DSI pourra ainsi mieux soutenir les orientations stratégiques de l'organisation et s'affirmer comme un pilier central dans la gestion des risques de demain.

Le Cigref est un réseau de grandes entreprises et administrations publiques françaises qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un acteur fédérateur de la société numérique. Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative.

Pour réussir sa mission, le Cigref s'appuie sur trois métiers, qui font sa singularité.

**Appartenance**
Le Cigref incarne une parole collective des grandes entreprises et administrations françaises autour du numérique. Ses membres partagent leurs expériences de l'utilisation des technologies au sein de groupes de travail afin de faire émerger les meilleures pratiques.

**Intelligence**
Le Cigref participe aux réflexions collectives sur les enjeux économiques et sociétaux des technologies de l'information. Fondé il y a près de 50 ans, étant l'une des plus anciennes associations numériques en France, il tire sa légitimité à la fois de son histoire et de sa maîtrise des sujets techniques, socle de compétences de savoir-faire, fondements du numérique.

**Influence**
Le Cigref fait connaître et respecter les intérêts légitimes de ses entreprises membres. Instance indépendante d'échange et de production entre praticiens et acteurs, Il est une référence reconnue par tout son écosystème.

www.cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr

Cigref
RÉUSSIR
LE NUMÉRIQUE