



Cigref
SUCCEED
WITH DIGITAL

Geopolitics and Digital Strategy

Challenges and levers for action
for digital departments

February 2025



Cigref

Geopolitics and Digital Strategy

Challenges and levers for action for digital departments

February 2025



Intellectual property rights

All Cigref publications are made available free of charge to as many people as possible, but remain protected by the intellectual property laws in force.

EDITORIAL

In the past, geopolitical issues played a minor role in digital strategy development. Decisions were primarily based on business, technical, financial, or legal considerations. However, in recent years, geopolitical factors have gained prominence in hardware development, with constraints sometimes dictating the selection of equipment or components based on new criteria. In the realm of software and digital services, it has become imperative to incorporate geopolitical considerations. Some organisations have already incorporated geopolitical considerations into their strategies, while others are in the process of doing so.

To illustrate this point, consider the decision-making process when selecting a cloud provider. Typically, organisations assess the security and financial aspects of potential options, and occasionally conduct a make-or-buy study. However, questions surrounding the physical location of the datacentre and the risk of connection failure between offices and the datacentre are often overlooked. In the context of software, the question arises as to whether Inner Source and Open Source would be better suited, not for financial reasons, but because a published product is always associated with its country of origin, whereas Open Source or Inner Source escape this notion of national belonging.

Our current 'follow-the-sun' strategies are based on selecting three countries with an approximate time difference of 8 hours, often determined by existing geographical locations. Will we soon have to choose these countries based on geopolitical criteria, or even reduce these follow-the-sun activities in favour of local night work? We are already seeing policies gradually replacing off-shoring with near-shoring and now with reshoring. Furthermore, outsourcing decisions made by partners can result in the internalisation of teams due to geopolitical risks associated with the new location of services. We have therefore decided to address these issues and share our recent experiences, in the hope that the following report will serve as a basis for internal discussions within each member organization.

Marc-Michel STACK, Head of Group IT Technology Intelligence at BNP Paribas and
Taras VELIKOROUSSOV, Director of Financial and Technical Performance ITN, Orange.

SUMMARY

Tensions between major powers - the United States, China, Russia and Europe - and regional conflicts (Russia-Ukraine, Middle East) are affecting technology supply chains and increasing the polarisation of the global digital space. In the face of these geopolitical upheavals, the Information Systems Department (ISD) must develop a detailed understanding of the issues at stake in order to strengthen its digital resilience. These global tensions affect IT strategies in four key areas: strategic autonomy, cybersecurity, talent and supplier management, and governance.

1. IT departments need to develop their strategic autonomy by reducing their dependence on foreign technologies and suppliers and favouring local or European solutions in sensitive sectors (cloud, semiconductors). In this way, diversification of partners and suppliers becomes a key strategy for limiting the risks of supply disruption.
2. CIOs must also think ahead when it comes to cyber security. The increase in cyber threats linked to geopolitical tensions is forcing IT departments to strengthen their defences. This includes security audits, rigorous protocols and monitoring of geopolitical cyber risks. Collaboration with local cyber security partners is also essential.
3. Finally, the shortage of IT skills in Europe is encouraging CIOs to recruit internationally, but the geopolitical and regulatory risks associated with overseas recruitment complicate the process. However, geographical diversification of IT teams also contributes to the resilience of global operations.
4. Proactive IT governance is therefore critical to achieving greater autonomy, security and better management of digital talent on an international scale. By strengthening collaboration between IT, legal, HR and public affairs, companies can better anticipate geopolitical fluctuations. A dedicated IT foresight unit can support this process of reflection and encourage continuous anticipation of risks and opportunities.

In conclusion, a geopolitical approach to IT governance is becoming essential for greater resilience in the face of global crises. The IT Department must assert itself as a strategic pillar of the organisation, capable of navigating a fragmented and polarised digital environment.

ACKNOWLEDGEMENTS

Our thanks go to **Marc-Michel STACK**, Head of Group IT Technology Intelligence, at BNP Paribas and **Taras VELIKOROUSOV**, Director of Financial and Technical Performance ITN, at Orange, who steered this work, as well as to all the people who took part in and contributed to this Cigref working group (in alphabetical order):

François BANOS - RENAULT	Sylvain GERON - CARREFOUR
Xavier BENMOUSSA - SAVENCIA GROUP	Didier LAVOIGNAT - GROUPE SEB
Dorra BOUGHANEM - AXA	Julien MARTINO - MICHELIN
Olivier BURGAUD - SERVIER	Pascal MOREUIL - AIR FRANCE-KLM
Jean-Philippe CAILLAT - GROUPE 3M	Laurent MOUTY - FAYAT
Claudio CIMELLI - MINISTRY OF EDUCATION AND YOUTH	Laurent POUPON - BNP PARIBAS
Danièle COHEN - STELLANTIS	Franck REGNIER - ACCOR
Clément DAILLY - SUEZ	Benjamin ROCHARD - TRANSDEV GROUP
Anne DESLANDES - LA POSTE	Sébastien SCHNEIDER - BPI FRANCE
Jean-Marc DO LIVRAMENTO - ENEDIS	
Etienne DOCK - HAGER GROUP	

We would also like to thank all those who contributed to the work of our working group:

- Jean-Joseph BOILLOT, Associate Professor of Economics and Social Sciences and Doctor of Economics, specialises in the major emerging economies, particularly China and India,
- Fayçal BOUJEMAA, Technology Strategist, ORANGE,
- Stéphane DEMARTIS, VP Cloud Infrastructure Solutions and Services, Orange
- Eric FICHOT, Head of HR for CIB functions, BNP Paribas,
- Martin PAILHES, Head of the Digital & IP Platform of the Legal Department of the BNP PARIBAS Group,
- Nicolas ROUX, Chief Procurement Officer - IT Technology and Services, BNP PARIBAS
- Sandip WADJE, Managing Director - Global Head of Emerging Technology Operational Risks & Intelligence, BNP PARIBAS.

This document was designed and written by Aurélie CHOTARD, Mission Director at Cigref.

TABLE OF CONTENTS

1 INTRODUCTION: WHY SHOULD IT DEPARTMENTS CARE ABOUT GEOPOLITICAL DEVELOPMENTS?.....	7
1.1 Overview of KEY geopolitical trends	7
1.1.1 The United States: between political uncertainty and international influence	7
1.1.2 China: economic stabilisation and strategic tensions	8
1.1.3 THE Russian-Ukrainian conflict: a prolonged stalemate	8
1.1.4 Israel-Palestine and the GULF: a regional escalation	8
1.1.5 France: an unprecedented Domestic crises	8
1.2 Digital technology, a key issue in international relations	8
1.3 The challenges FOR IT in this geopolitical context.....	11
2 ITD PARTNERSHIPS AND PURCHASING: GEOPOLITICAL ASSETS AND VULNERABILITIES	13
2.1 Key partnerships and associated geopolitical issues	13
2.2 Going local: a strategy for digital resilience?	17
2.2.1 The "make or buy" APPROACH	17
2.3 Anticipation through better SUPPLIER knowledge	18
2.3.1 Best practice in geopolitical risk anticipation.....	18
2.3.2 A better understanding of risks.....	18
2.4 Making the right strategic Decisions.....	19
2.4.1 Designing resilient architectures.....	19
2.4.2 Operational resilience in IT DECISIONS	19
2.4.3 Supplier management	19
3 HR-IT POLICIES IN A CHALLENGING INTERNATIONAL CONTEXT.....	21
3.1 Skills shortages: the only reason for international IT recruitment?	21
3.2 The risks of international recruitment.....	23
3.3 Future prospects for international recruitment and new challenges.....	23
4 INTEGRATING THE GEOPOLITICAL DIMENSION INTO IT GOVERNANCE	27
4.1 Why is it Difficult to integrate the geopolitical dimension into IT governance ?	27
4.2 Taking the geopolitical dimension into account: the need for cooperation within the company	27
4.2.1 Establishing good governance.....	27
4.2.2 Working with the right tools	29
4.2.3 Limits and sustainability of the approach	30
5 CONCLUSION: TOWARDS A PROACTIVE IT DEPARTMENT IN THE FACE OF GEOPOLITICAL FLUCTUATIONS	33

TABLE OF FIGURES

Risk and Opportunity Matrix for Innovation Partnerships.....	14
Governance diagram for integrating the geopolitical dimension into IT activities	29

TABLE OF [INSERTS]

Geopolitical tensions and cybersecurity, with BNP Paribas	10
The Geopolitics of Artificial Intelligence	16
HR-IT implementation strategies: company feedback.....	22
Economic, political and cultural perspectives on India	25
Working with the legal department: a necessity for the IT department.....	31

1 INTRODUCTION: WHY SHOULD IT DEPARTMENTS CARE ABOUT GEOPOLITICAL DEVELOPMENTS?

*NB: This report is the result of a working group whose deliberations took place between January and September 2024. As a result, the vision of the geopolitical scene, as proposed in the report, does not take into account events occurring after October 2024. This first part, however, examines the consequences of the American elections **as we saw them at the time of writing, in November 2024.***

Digital management is now at the crossroads of technological and geopolitical issues, in a world where the balance between nations is increasingly unstable and the pressures and tensions on digital infrastructures are multiplying. Understanding geopolitical dynamics is essential if we are to anticipate the threats and opportunities they present, and thus strengthen the resilience of organisations. This interest in geopolitical developments enables IT to adapt its strategies to better protect information systems, ensure business continuity and align with the objectives of strategic autonomy in the digital domain. It also provides an opportunity for regular, in-depth dialogue between the business units and support functions on the one hand, and the IT department on the other, on the development of services and markets.

1.1 OVERVIEW OF KEY GEOPOLITICAL TRENDS

The year 2024 unfolded in an international climate of geopolitical uncertainty, with changing dynamics between the world's major powers, aggravated conflicts in already tense areas, and political upheaval in France adding a unique dimension to the European scene. Each year, Cigref provides an overview of the international scene in the background note to its Strategic Orientation Report.

The five major geopolitical themes proposed below describe a global context in which alliances, economic stability and regional security are proving to be interdependent and volatile, influencing the balance of international relations and world markets for years to come.

1.1.1 THE UNITED STATES: BETWEEN POLITICAL UNCERTAINTY AND INTERNATIONAL INFLUENCE

In November 2024, the US presidential election will occupy a central place on the international agenda, as it will affect the United States' relations with its allies, particularly in Europe and the Indo-Pacific. The contest between Kamala Harris and Donald Trump has revealed two different visions. Harris represents continuity in the multilateralist approach and international alliances, with a desire to support partnerships in Asia and Europe, while Trump defends a retreat to protectionist policies and a transactional vision of the world. Now that Trump has been re-elected as US leader, an increase in tariffs is likely to further divide the global economy into economic blocs, weakening global trade and exacerbating trade tensions, particularly with China.

1.1.2 CHINA: ECONOMIC STABILISATION AND STRATEGIC TENSIONS

China is experiencing an economic slowdown marked by structural problems in the consumer and real estate sectors. Despite efforts to stimulate growth through public investment, GDP is expected to continue to stagnate until 2025. On the geopolitical front, China is strengthening its influence in the Asia-Pacific region, where tensions with the United States remain high. Washington's Asian allies are closely monitoring the outcome of the US election, as Trump's victory could exacerbate trade tensions with Beijing and lead to renewed technological and economic competition.

1.1.3 THE RUSSIAN-UKRAINIAN CONFLICT: A PROLONGED STALEMATE

The war in Ukraine is stalling, with no decisive breakthrough on either side. Western support remains crucial for Ukraine, and the American election is likely to redefine its contours. The incoming Trump administration is likely to reduce aid and favour an isolationist approach. This prospect worries European allies, for whom American support is essential to contain Russian ambitions in a context of relative lack of clear leadership in Europe.

1.1.4 ISRAEL-PALESTINE AND THE GULF: A REGIONAL ESCALATION

Rising tensions in the Middle East, exacerbated by recent hostilities between Israel, Hamas and Iranian-backed Hezbollah, could destabilise the entire region. US alliances in the Gulf could be tested after the US election, with Trump likely to step up unilateral military support for Israel. This increases the risk of long-term escalation in the region, including in US relations with key players such as Saudi Arabia.

1.1.5 FRANCE: AN UNPRECEDENTED DOMESTIC CRISES

France is experiencing a political crisis marked by internal divisions and governmental instability. The lack of a clear majority and budgetary difficulties are exacerbating tensions, while the government is faced with rising public debt. This situation is causing concern within the EU, where France plays a crucial stabilising role. The country may be forced to reform its budget to ensure the sustainability of its debt, while navigating between the demands of the EU and those of the French people.

1.2 DIGITAL TECHNOLOGY, A KEY ISSUE IN INTERNATIONAL RELATIONS

Today's digital world is becoming increasingly fragmented. This trend is accentuated by technological and economic rivalries between major powers, exacerbated by protectionist policies and technological autarky.

The rivalry between the United States and China, particularly visible in the semiconductor industry, is emblematic of this fragmentation. The United States is trying to reduce its dependence on Asian semiconductors by bringing production back home and restricting China's access to advanced technologies, while China is pursuing its quest for technological autonomy despite these obstacles. For its part, the European Union, aware that it is lagging behind, is investing in its own Chips Act in an attempt to close the technological gap, although it remains dependent on Asian and American players

(in a context in which 60% of the world's semiconductors and more than 90% of the most advanced semiconductors are still produced in Taiwan, and China is showing an increasing ability to blockade this island).

The intensification of this protectionist dynamic is leading to the formation of closed technological blocs, with each region seeking to protect and develop its digital capabilities. This fragmentation is also affecting the generative artificial intelligence (AI) industry, a booming sector whose business model remains fragile. The major players in generative AI, mostly based in the United States, are investing heavily in these technologies, but are struggling to make their operations profitable. The sector also poses challenges for the management of the necessary data and infrastructure, which each bloc is trying to control with sometimes conflicting industrial and regulatory policies in order to limit its dependency.

Finally, the European Union faces a structural dependence on large US technology companies, which are capturing an increasing share of the digital value created in Europe. This situation highlights the tensions surrounding Europe's digital sovereignty, which is being undermined by a concentration of power in the hands of a few foreign players, threatening the long-term competitiveness and strategic autonomy of its companies.

We are witnessing the end of a cycle of striving for universalism and interoperability in the global digital space, which is fragmenting at the pace of economic, technological and governance rivalries, with each bloc trying to preserve its interests and limit its dependence on the others, at the risk of compromising international cooperation and interoperability.

Geopolitical tensions and cybersecurity, with BNP Paribas

The financial sector is a prime target for cyber attackers. In addition to protecting financial data, it is essential to maintain the stability of the financial system and confidence in the banking system. A bank like BNP Paribas must therefore constantly monitor the impact that geopolitical tensions can have on the development of cyber-attacks. Cyber-attacks can have different objectives and therefore different consequences for an organisation's business:

- **Cyber attacks as a tool in geopolitical conflict:** There has been an increase in cyber attacks as a tool of geopolitical influence, particularly the use of cyber strategies during the ongoing conflict between Russia and Ukraine. Private actors and other nations have become involved in these cyber operations. Cyber-attacks are being used as a means of pressure by geopolitical actors. Developments in the geopolitical situation have a direct impact on the evolution of cyber risks (e.g. the numerous attacks against Israel after 7 October).
- **Cyber attacks to disrupt the IT supply chain:** Financial institutions and their supply chains are particularly vulnerable to cyber attacks. Attackers tend to target the least secure parts of the supply chain, but these attacks can also be used in geopolitical conflicts to affect more global industries, such as the semiconductor industry in the case of a regional conflict in Asia.
- **Cyber-attacks as a means of pressure and influence between states:** some countries, notably Russia and North Korea, support cybercriminal activities as a means of circumventing sanctions and waging indirect warfare. These activities include ransomware attacks and disinformation campaigns paid for in cryptocurrencies to circumvent sanctions.
- **Cyber attacks as a tool to destabilise populations:** These cyber-attacks have a wider impact on financial systems and social trust, and are used strategically to sow distrust among populations and disrupt essential services.

To cope with this changing cyber landscape and the context of global tensions, organisations need to better prepare for and anticipate cyber threats of all kinds. This includes improving cyber security defences, understanding the motivations behind cyber attacks and preparing for potential crises, such as a potential conflict in Asia that could have a violent impact on global supply chains.

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

1.3 THE CHALLENGES FOR IT IN THIS GEOPOLITICAL CONTEXT

In a geopolitical context characterised by the fragmentation of the digital space and growing technological rivalry between major powers, the Information Systems Division (ISD) faces major strategic challenges. It must not only adapt to local constraints, but also consider forms of regionalisation in order to seize opportunities and strengthen its resilience. Here are the main challenges facing the ISD in this context:

- **Strategic - Strategic autonomy and control of dependencies:** IT is faced with the challenge of reducing its dependence on foreign suppliers, particularly American and Asian, in strategic areas such as cloud, semiconductors and digital services. Given the fragmentation of the digital space, it needs to diversify its sources of supply to limit the risks of disruption, whether in terms of data, skills or critical technologies. This means prioritising local or European solutions, in line with digital sovereignty policies.
- **Cyber security and infrastructure resilience:** In an increasingly polarised international environment, cyber threats are on the rise. IT departments need to ensure the security of their data and the resilience of their infrastructure through robust cybersecurity protocols, regular audits and strengthened cyber defence partnerships. International expansion can contribute to this resilience by geographically diversifying resources and ensuring business continuity in the event of local crises or cyber attacks.
- **Accelerating innovation and adapting to international regulations:** To remain competitive, IT departments must monitor and adopt emerging innovations in foreign markets while navigating an increasingly complex and fragmented regulatory framework. Indeed, data, privacy and AI regulations vary from one region to another, forcing IT departments to quickly adapt their practices to comply with local laws, such as the RGPD in Europe, while adhering to American or Asian regulations. This technology and regulatory monitoring allows IT not only to remain compliant, but also to take advantage of local technology ecosystems.
- **Optimise operating costs and attract talent:** IT departments can also seek to reduce costs by taking advantage of the economies of scale that an international presence can bring. This allows them to optimise the purchase of critical resources, standardise processes and gain access to skilled talent in key regions. This talent, which is sometimes in short supply locally, is essential to support critical areas such as cybersecurity and AI. Internationalisation therefore facilitates access to a variety of skills, while strengthening the organisation's competitiveness.
- **Facilitate organisational change and 24/7 support:** In an unstable global environment, the IT department must develop a culture of adaptability and agility. A regional international presence helps to foster a culture of adaptability, which is essential to cope with rapid change in the digital sector. It also allows IT to provide continuous support to customers using a 'follow the sun' model, with teams spread across multiple time zones. Such an organisation ensures that critical services are available 24/7 to meet performance and customer satisfaction requirements.
- **Ethical governance and environmental responsibility:** Finally, IT must integrate responsible and ethical practices into its management, particularly with regard to data quality, the use of

AI and environmental impact. The reliance on data and digital infrastructure requires rigorous governance, especially with the emergence of generative AI, to avoid algorithmic bias and minimise negative environmental impact.

2 ITD PARTNERSHIPS AND PURCHASING: GEOPOLITICAL ASSETS AND VULNERABILITIES

In a world where geopolitical tensions are increasingly influencing business decisions, ISD partnerships and procurement are proving to be both strategic levers and sources of vulnerability. International collaborations, whether in innovation, compliance or the provision of critical services, must be approached with caution to anticipate the risks of disruption and ensure business continuity. By integrating geopolitical dimensions into sourcing and partnering strategies, IT can not only strengthen the organisation's resilience to global crises, but also maximise the benefits of a diverse ecosystem of suppliers and partners while minimising critical dependencies.

2.1 KEY PARTNERSHIPS AND ASSOCIATED GEOPOLITICAL ISSUES

International partnerships, both commercial and non-commercial, cover a number of key areas:

- In terms of **innovation**, working with foreign players gives an international company access to disruptive technologies in specific fields, such as cybersecurity with Israel or with leading players in the United States. These partnerships can also support the incubation of emerging players (start-ups) with a view to industrial and academic research, and provide links with industrial partners for the large-scale deployment of the solutions developed. Finally, working with think tanks and universities on these innovation issues helps to create a common understanding and vision of how technologies are evolving.
- **In the monetary area**, these partnerships involve the management of international financial transactions, particularly in dollars, in-depth knowledge of taxation in each region of the world, and consideration of the extraterritorial implications of US laws in the context of these dollar transactions.
- **Compliance** is another critical area that requires knowledge of local jurisdictions to ensure compliance. Identifying partners who understand local legal issues, such as those in Argentina, Venezuela, China or Russia, is essential. These collaborations are also necessary for filing patents and monitoring local patents.
- When it comes to providing **business-critical services** such as cloud, SaaS and telecoms, local suppliers are sometimes unavoidable in certain regions, particularly in China, where the government requires any foreign company to use local service providers if it wants to benefit from these services. The diversity of the regions in which a company operates sometimes makes it impossible or complicated to work with a single partner.
- When it comes to **accessing local markets**, or 'going to market', it is essential to understand the local culture and often to work with local companies. In China, for example, local partnerships are required to access the market. These partnerships also provide support in terms of acculturation, education and training in the countries where the organisation operates, while avoiding an overly Franco-centric vision.

- **Standardisation** is a priority for some organisations, which seek to standardise their procedures on a global scale to facilitate their deployment. This may take the form of participation in multi-partner consortia to establish internationally applicable standards and norms.
- Finally, **the international management of IT human resources** as part of an offshoring or nearshoring strategy may require partnerships with local agencies to facilitate access to skills that are rare or not widely available in Europe. These partnerships can also be formed with French companies located abroad, particularly in the European Union, North Africa or India.

Innovation partnerships need to be considered carefully as they often require the company to streamline its processes to allow for new experiments. In the case of collaboration, the ownership of each party must be clearly defined to avoid subsequent competition.

Innovation partnerships	
Opportunities	Threats
<ul style="list-style-type: none"> • Expand the company's customer base by entering new markets and developing its business model. • Gain technological expertise. • Innovate faster and at lower cost. • Benefit from a pool of expertise. • Anticipate skills needs. • Anticipate investment needs. • Get closer to suppliers and develop the relationship into a partnership. • Align with market technology standards. 	<ul style="list-style-type: none"> • In the case of partnerships with start-ups, the issue of intellectual property and the company's weight in sales (risks of dependency) must be carefully assessed and monitored. • In some cases, there is a risk of losing business know-how. • The complexity of innovation structures in the European Union. • Difficulties in integrating new solutions into existing IS. • Risk of French start-ups being taken over by foreign players. • Risk of leakage of sensitive data.

Risk and Opportunity Matrix for Innovation Partnerships

When it comes to international sourcing and partnership strategies, companies face geopolitical risks that can be direct (sanctions, conflicts) or indirect (knock-on effects). For example, an event such as a war between Taiwan and China would have global repercussions. It's not just the place of purchase that's important, but the whole range of geopolitical factors that need to be taken into account.

- **The risk of supply chain disruption is critical**, particularly for hardware. Difficulties in delivery lead to supply problems that can affect the availability of equipment. Companies need to influence their suppliers to be among the first to deliver in order to minimise these risks.
- **Regulatory risks** arise from data protection laws (sometimes used by governments to regulate companies' activities) and intellectual property laws, particularly in markets where regulations can vary significantly from country to country.

- **Cyber security risks** take the form of targeted attacks on specific companies and are often difficult to manage. These risks include industrial espionage, which can be difficult to detect. Data leaks can also come from allied countries and can be the result not only of cyber threats, but also of human manipulation by partners or suppliers with access to data.
- In certain regions, such as Venezuela or Turkey, there are **financial risks associated** with exchange rate volatility. In particular, fluctuations can lead to significant losses for companies between the time of invoicing and payment.
- **CSR (Corporate Social Responsibility) risks include reputational risks**, such as managing employees in countries with internal conflicts, such as Myanmar. HR risks relate to protecting employees and subcontractors in high-risk areas such as Russia or Ukraine. Companies also need to monitor subcontractors to avoid internal incidents, such as activists working for a political or militant cause.

When it comes to software, one of the main issues is maintaining the solution. It is often preferable to buy solutions in Europe or the US in order to retain local expertise. Finally, the jurisdiction specified in contracts is also important, because if a European supplier is acquired by a company from another country, the contract could change jurisdiction.

The Geopolitics of Artificial Intelligence

The integration of Artificial Intelligence tools within organisations is becoming increasingly necessary if we are to remain competitive in a global market and develop new ways of working. To achieve this integration, it is first necessary to identify the most relevant use cases, and then to overcome certain technical challenges associated with legacy IS. These different concerns are preventing digital departments from looking at other consequences of the massive deployment of these tools, which are geopolitical, environmental and regulatory in nature:

- **Energy consumption and processing power:** AI consumes a lot of energy and requires a lot of computing power.
- **Europe and strategic autonomy:** Europe has focused more on regulation than on strategic autonomy in AI. The continent is absent from the market for operating systems (OS) and search engines. For example, 75% of searches by European citizens are done on Google. Google practices the economy of intent: by aggregating a company's queries, it is able to reconstruct its strategic plan. Similarly, European players are absent from the cloud market. Finally, in terms of hardware, Asia is the leader, particularly in the semiconductor market.
- **Regulatory challenges:** Regulations are evolving rapidly, but there is a risk that they will not keep pace with technological advances. US regulation is still ahead of European regulation. However, how can regulation not be a force for innovation, such as the RGPD, which subsequently inspired many countries, including the US?
- **Loss of talent and data:** France's strict data protection rules can hinder the development of powerful AI. In addition, French researchers are migrating to US companies because of better investment and salaries.
- **Funding and business models:** Massive investments in AI are being made by American technology giants. The question of the European business model for AI is crucial.
- **Fragmentation and centralisation of AI:** The fragmentation of AI poses challenges for its integration into businesses. Small Language Models (SLMs) and open source solutions are viable alternatives.

Faced with these various challenges, digital departments have several levers to pull:

- **Industrial and geopolitical strategies:** By-design thinking is needed to address geopolitical challenges. Approaches to reduce dependence on specific suppliers should be considered.
- **Key players and alliances: strategic alliances and investments are being made in the sector, such as NVIDIA's acquisition of ARM.**
- **Issues of closure and openness:** debates are underway on whether to close or open the market to encourage the emergence of strong players.

Fayçal BOUJEMAA, Technology Strategist, ORANGE

2.2 GOING LOCAL: A STRATEGY FOR DIGITAL RESILIENCE?

When selecting suppliers, there is a choice between a local sourcing strategy and a global sourcing strategy. For example, a global contract with an American publisher may offer certain management advantages, but also risks in the event of geopolitical tensions. A local approach may be a better way of spreading certain risks in the face of increasing geopolitical fragmentation, which is becoming more pronounced with China's policies and the Russian-Ukrainian conflict. This fragmentation calls into question the viability of certain offshoring decisions, where the geopolitical risks were not always taken into account at the outset.

In thinking about this, we need to be clear about what we mean by 'local': does it mean a site in France or, on the contrary, a site in India? Choosing hyperscalers that do not cover certain geographical areas can be problematic for companies looking to expand internationally. It is therefore essential to assess the risks associated with each supplier.

Developing a local approach usually leads to fragmentation of the IS from a technical point of view. Companies therefore face a dilemma when it comes to sourcing strategy: is it better to develop as global an approach as possible and face the risks of dependence on a single supplier, or is it better to multiply the number of local partners and suppliers, even if this means increasing the complexity of the information system? In general, it is complicated for a company to go one way or the other. However, certain IT strategies are better managed when they are part of a local dimension, at company level. Managing data at a local level allows the company to retain control of its information assets by ensuring that they are compatible with its overall technical architecture. In addition, a more local strategy typically involves the development of vendor-agnostic IT architectures, not least to ensure compliance with various local regulations. In this type of strategy, it is still necessary to develop a common taxonomy and governance to maintain a degree of homogeneity and overall consistency across the organisation.

2.2.1 THE 'MAKE OR BUY' APPROACH

The concept of make or buy is often misunderstood and still limited to purely financial considerations. For some companies, however, the concept is evolving to include strategic aspects. For example, an open source approach can address the make or buy issue in some cases, particularly to bring the value chain closer to critical activities. However, open source is not always appropriate. For example, for standard applications such as ERP, in-house development is unlikely to add value. Building an ERP in-house to respond to geopolitical risks could be a solution, but would it be viable in the long term?

Some countries, such as China, are developing their own solutions to protect themselves from foreign dependency (for example, by building their own alternative to Salesforce). However, this approach raises the question of available resources: do all countries or companies have the resources to develop their own CRM or critical applications?

It is not always necessary to 'build' to have total control. The on-premises option can be a first step in reducing geopolitical risks, although some providers reject this solution. OVH Cloud, for example, aims

to develop a set of solutions that are entirely open source. This shows that a hybrid strategy between 'make', 'buy' and 'open source' can offer advantages in certain contexts.

2.3 ANTICIPATION THROUGH BETTER SUPPLIER KNOWLEDGE

There are two different approaches in the purchasing organisation: Vendor Management and the Operational Purchasing function. A major challenge is to determine where geopolitical risk fits into this structure. A simple risk matrix is not enough. We need to go further and adopt a global approach to good organisational practice that includes elements of proactive risk management.

2.3.1 BEST PRACTICE IN GEOPOLITICAL RISK ANTICIPATION

Among the best practices to be adopted is the introduction of specific contractual clauses in supplier contracts, adapted to geopolitical risks and in line with current regulations. It is important not to limit oneself to a theoretical approach, but to integrate concrete mechanisms into the organisation. This will help the company to be better prepared to deal with unforeseen situations. Sharing best practices on regulations and contracts is also essential to managing these risks.

In terms of strategy, it is important to define elements of consensus within the organisation, but also to highlight any differences that may exist. This provides a balanced and nuanced view of the risks, while encouraging constructive discussions about the direction to take.

At a time when everything is geopolitical, it is essential that companies are provided with precise assessment criteria. For example, signing contracts in a local jurisdiction may be a good way to mitigate certain risks. It is therefore essential to keep abreast of and adapt to regulatory developments in order to better manage the impact of geopolitical tensions.

Another important issue is cloud strategies. Some providers attract customers by limiting reversibility options, thereby capturing a significant proportion of the value. This raises issues of strategic autonomy and geopolitical risk. The choice of cloud services is often dictated by regulation: some sectors are heavily regulated, while others consider that their data is not subject to geopolitical risks and can therefore minimise this dimension in their technological choices.

2.3.2 A BETTER UNDERSTANDING OF RISKS

It is crucial to select the critical applications for which it is necessary to diversify geopolitical risk. Teams need to be trained on these issues and understand the difference between what is 'core business' and what is not. This needs to be part of a global resilience strategy.

There are three levels of supplier risk to consider. The first level of risk is strategic and relates to the global decisions that may be made by the Executive Committee about the location of IT applications and services. Each decision, whether insourcing, nearshoring or offshoring, involves specific supplier management risks. The second level concerns the situation of the supplier, its compliance with various regulations, its location and its financial situation. Each organisation needs to be fully aware of this information when making its selection and throughout the subsequent relationship with the supplier.

In pragmatic terms, this means carrying out due diligence on each supplier when they are brought on board and monitoring these criteria on an ongoing basis. Finally, the third level focuses on services and, more specifically, on the risks that may arise in connection with the service provided by the supplier and its introduction into the company's information system (data extraction, espionage, etc.).

It is therefore essential for companies to adopt a 'Know Your Supplier' (KYS) approach. This will enable them to share a common understanding of the issues and incorporate geopolitical analysis into their supplier selection processes.

The banking sector can serve as an example, as it is highly regulated. The implementation of IT governance structured on several levels (level 1: purpose & strategy; level 2: IT structuring; level 3: deployment of units) ensures the continuity of practices and the compliance of operations in a complex geopolitical environment.

2.4 MAKING THE RIGHT STRATEGIC DECISIONS

The geopolitical dimension needs to be integrated into everything the digital department does. It's not just a question of looking at contracts, but of reviewing all processes to ensure the resilience of systems and technological choices.

2.4.1 DESIGNING RESILIENT ARCHITECTURES

It is essential to design solution architectures that take account of specific geographical features and local risks. Each geographical region must have its own solution adapted to the legal and geopolitical context.

Recommended tool: An architectural reading grid, similar to ethical and CSR practices, could be used to share best practices with teams. This would include monitoring local regulations and raising awareness of the impact of geopolitics on IT decisions.

2.4.2 OPERATIONAL RESILIENCE IN IT DECISIONS

Resilience must be considered at the design stage: choice of solutions, robust architectures, diversification of infrastructures. Resilience then becomes a key criterion in IT decisions.

Recommended tool: A comprehensive framework that includes geopolitical risk management, supplier monitoring and IT architecture adaptation should be developed to ensure continuous review of practices. This also includes embedding a corporate culture that values resilience as a key element of strategy.

2.4.3 SUPPLIER MANAGEMENT

Supplier monitoring should not be limited to commercial aspects. It is important to understand not only their financial position, but also their location, associated geopolitical risks and compliance with local regulations. A resilience strategy involves mapping suppliers critical to business services and continuously monitoring geopolitical risks. Although costly, this approach allows potential threats to

be identified before they affect the business. Sourcing diversification is an essential element of resilience, which is often constrained by cost, particularly when procurement departments prioritise cost control over risk management.

Recommended tool: A map of critical suppliers, updated regularly.

It is important to anticipate the risks associated with dependence on a supplier. Failure does not only mean bankruptcy, but can also be the result of a buy-out or a change in the terms of use. Supplier management must incorporate this risk management. Regular reviews of risks and associated practices need to be put in place so that the geopolitical dimension can be integrated into sourcing and supplier management strategies on an ongoing basis. This framework should be incorporated into IT governance processes.

It is important to diversify geographical locations to avoid concentrating risks in a single country. For example, when setting up servers, it is advisable not to centralise all infrastructure in a single geopolitically sensitive region, but to consider safer alternatives.

Recommended tools:

- *A list of specific questions to ask when engaging with a supplier to assess its resilience and ability to respond to unforeseen events.*
- *A regular review of the geopolitical resilience of critical suppliers.*

Supplier management should not be the domain of procurement alone. We need to redefine the roles of supplier management teams to include this dimension of resilience and geopolitical embedding. A new role could be created with specific responsibilities for ensuring resilient processes are in place, in collaboration with the business units.

Recommended tool: Create a new job description for a 'vendor manager' with responsibility for managing resilience processes.

3 HR-IT POLICIES IN A CHALLENGING INTERNATIONAL CONTEXT

In an unstable international context, HR-IT policies face a number of challenges related to recruitment and talent management in different countries. While the digital skills shortage is encouraging companies to recruit across borders, factors such as the complexity of local regulations, geopolitical risks and cultural specificities have a major impact on these decisions. The stakes are high: it's not just a question of ensuring the continuity and resilience of IT operations, but also of adopting recruitment practices that incorporate a balanced view of the risks and opportunities associated with different markets. The IT department must therefore work with HR teams to develop talent management and skills localisation strategies tailored to the realities of each region, while at the same time strengthening the company's technological sovereignty.

3.1 SKILLS SHORTAGES: THE ONLY REASON FOR INTERNATIONAL IT RECRUITMENT?

Companies' HR-IT implementation strategies are highly dependent on the regions in which they operate. Depending on how the digital department is organised, it may be necessary to have local IT teams working in different regions to be as close as possible to the business teams. However, an IT department with a more centralised organisation, providing services to the different regions of the company, will not necessarily need to relocate for reasons of international business continuity.

Beyond these business needs, there are specific recruitment factors and considerations that differ between IT and the rest of the business. The digital sector in Europe is facing a talent shortage, especially in strategic areas such as data, AI and cybersecurity. Training programmes are struggling to keep up with the growing needs of businesses and cannot compensate for the dwindling opportunities for offshoring and outsourcing of IT activities.

A key factor in the choice of recruitment countries is their local capacity to train sufficient numbers of engineers, as is the case in India and Russia. The objective of increasing the number of women in IT teams also plays a role in countries such as India and Poland, where there is a better gender balance. Cultural openness is essential, but differences can also pose management challenges.

Some websites classify countries according to certain criteria (environment, transport, etc.):

- Strengths/weaknesses of countries for setting up a business:
<https://www.prosperity.com/rankings>.
- A reference database of job descriptions to compare profiles:
<https://www.wtwco.com/fr-fr/solutions/remuneration-globale>.

Language is also an issue. Exchanges are mainly conducted in English, but managers need to adapt their communication to local cultures. There are often legal barriers to bringing in talent, particularly for profiles from Morocco, India or China.

Another issue is the use of service providers to carry out international activities. Service providers may be used for specific projects, but rarely for strategic activities. In addition, the use of contractors generally varies from region to region, as rising salaries in some areas and the complexity of processes can make recruitment difficult.

The size of the activities outsourced is critical. Below a critical threshold of 200 employees, it becomes complex to ensure the viability of a site. We must avoid opening branches in regions where the need for resources is too low.

HR-IT implementation strategies: company feedback

Orange

- Outside France, corporate IT teams are present in India, Romania, Morocco, Tunisia and Egypt. Local IT departments are of course present in all countries.
- Our geographical presence allows us to address sovereignty, regulatory and security issues while optimising structural costs.
- Competition is fierce in the telecoms sector, and optimising costs and locations is crucial.

BNP Paribas

- Present in 65 countries, with a number of regional IT hubs (Paris-Madrid, Singapore-Mumbai, New York-Toronto).
- 10,000 investment banking IT staff, of which 6-7,000 in India (Mumbai, Bangalore).
- 'Follow the sun' strategy to ensure the continuous availability of IT tools.
- Decision-making headquarters in Paris/London, but diversification of European IT production in Spain, Poland and Romania.

Micheli

- Global development: Clermont-Ferrand (Europe), Greenville (America), Shanghai (Asia), India (Pune).
- 50/50 balance between internal staff and service providers. Each region has its own CIO who reports to the Group CIO.
- Acquisition of new local teams through networking and gradual integration.

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

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

Julien MARTINO, CRM Enterprise Architect, MICHELIN.

3.2 THE RISKS OF INTERNATIONAL RECRUITMENT

In the context of recruitment policy, citizenship and nationality can be problematic in the context of regional conflicts between different ethnic groups, or when carrying out particularly sensitive tasks involving state policy. For example, recruiting an employee of Pakistani origin in India can raise questions about visas and social integration. Beyond this administrative aspect, geopolitical tensions can complicate the transfer of projects between countries, such as moving operations from China to India, which requires appropriate communication to ease any tensions between local teams.

Companies also need to address security issues when sending employees to sensitive regions. In China, for example, sending people without strong family ties can reduce the risk of local pressure. The choice of sourcing, both talent and skills, can then become a lever to minimise these risks. While companies can anticipate certain geopolitical threats, they cannot avoid them altogether. It is therefore essential to pay close attention to sourcing choices, particularly in the software sector where the nationality of talent can have an impact on projects. Recruitment processes are becoming more complex due to the need for background checks to avoid potential risks.

In addition, the use of local software requires specialist skills, while collaboration tools are subject to local regulations, as in China, where solutions such as Microsoft Teams can be difficult to use. To compensate for these limitations, some companies choose to focus on internal control of their software. Companies must also ensure that they comply with other local regulations, such as the Chinese equivalent of the RGPD. In the case of employee data, for example, centralisation in France can create regulatory difficulties, as China requires data on its nationals to be stored locally.

Geopolitical developments in certain countries also require increased vigilance. It may be necessary to monitor the situation in the countries where the company operates in order to manage local teams in the event of conflict. Certain geopolitical events, such as the Arab Spring in Egypt, have also shown the impact of local crises on cost-based strategies, sometimes requiring rapid adjustments. In Israel, for example, political stability remains an issue for companies based there.

In addition to geopolitical risks, environmental factors such as monsoon flooding in India can also disrupt business.

Finally, diversifying our overseas teams reduces our reliance on local skills and strengthens the resilience of the organisation.

3.3 FUTURE PROSPECTS FOR INTERNATIONAL RECRUITMENT AND NEW CHALLENGES

In the future, companies could adopt the emerging notions of ‘friend-shoring’ or ‘ally-shoring’ to focus on geopolitically secure partnerships for their core business. This would represent a return to more local decision-making, in contrast to the globalisation strategies of the past twenty years. This regionalisation allows networks of skills and expertise to emerge at a regional level, reinforcing local know-how.

What's more, international recruitment against a backdrop of strong regulation raises the question of how the profiles sought offshore will evolve, particularly in the IT sector, where the need could diminish as a result of the increasing automation of certain functions.

Economic, political and cultural perspectives on India

In France, the 'Indian risk' is often underestimated, despite the fact that France is India's second largest arms supplier and that the French state depends on the presence of its companies in the country for economic reasons. India has a resilience that prevents it from being easily influenced by any single geopolitical bloc. Unlike China, whose risk is linked to a possible war with the United States, India adopts an opportunistic pragmatism that allows it to navigate the current geopolitical context. Economically, India has become a major player and most CAC40 companies have a direct or indirect presence there. The digital sector is India's leading economic sector, with its leaders often educated in American universities.

The current Hindu nationalism embodied by the ruling regime is a major source of tension. Although India is predominantly Hindu (almost 90%), inter-religious and inter-ethnic tensions persist, especially during elections. Hindu nationalism is sometimes described as fascist because of violence, pogroms and attacks on churches. These tensions are exacerbated by geographical and cultural divisions between the less developed north and the south, where economic centres such as Mumbai and Bangalore thrive. There is also a divide between east and west, particularly around Kolkata. In 2017, a government currency reform had a significant impact on GDP, reflecting economic divisions and political intentions to weaken opposition parties.

The administration of COVID-19 has also had significant economic and social consequences, exacerbating divisions. However, there is no risk of north-south secession, as the Indian states have considerable political autonomy, making them privileged interlocutors for foreign companies. Forecasts for the next elections suggest that the populist wave may stabilise, suggesting that India will not tip completely towards extreme populism. Despite this complex geopolitical context, political risk remains limited.

Economically, India faces many challenges. Despite its large population, the country struggles to provide skilled jobs. The IT sector, while important, is not enough to support the economy as a whole. Global warming is also affecting people's health and productivity. Indian cities, which already have unsustainable water and electricity supplies, are suffering serious health problems. Offshore centres, often well equipped with infrastructure, are relatively unscathed, and the COVID crisis has revealed the extent of outsourcing, with an increase in home-based work managed by companies themselves rather than the state.

In terms of India's strengths, human capital is important. Although the average level of education is low, some public schools provide very high levels of education, often influenced by the caste system. Indian culture is rich and intellectually articulate, based on texts such as the 'Five Books', a collection of fables dealing with human nature and social relations. This tradition gives India a unique soft power, supported by the spread of yoga and a culture of veganism adopted by around 40% of the population.

In foreign policy, India is opportunistic, seeking to maintain good relations with its main trading partners, especially Russia and China, despite current conflicts. It does not want to fall into a bipolarity between the United States and China, which explains its strategy of balance in its international relations. If war broke out between China and the United States, India would be forced to choose sides, which it tries to avoid by maintaining good neighbourly relations, except with China, with which tensions are contained by a form of indirect competition in neighbouring countries.

At the social level, the evolution of relations between men and women has been marked by an increase in conservatism. The hopes of modernity in the 1960s have given way to a form of disillusionment, and the concept of modernity is now in retreat. The image of women is still strongly influenced by regional characteristics. The caste system favours some social and economic mobility, contributing to an entrepreneurial spirit. Historically, India enjoyed economic prosperity until the 18th century, reinforced by a relationship with time and beliefs influenced by reincarnation and life cycles.

Faced with the challenges of climate change, Indian philosophy favours frugality. Per capita consumption remains low, although another, more pragmatic India is moving towards accumulating wealth without worrying too much about the environmental consequences. The country takes a short-term approach to managing its resources, preferring to find solutions on a case-by-case basis - a mindset that promotes resilience in the face of crises, but could hinder its long-term development.

Jean-Joseph BOILLOT, associate professor of economics and social sciences and doctor of economics, specialising in the major emerging economies, particularly China and India

4 INTEGRATING THE GEOPOLITICAL DIMENSION INTO IT GOVERNANCE

Addressing geopolitical issues within IT remains complex: it requires a detailed understanding of global challenges and an ability to anticipate that is not yet part of the IT reflex in most organisations. To truly strengthen IT's resilience and agility in the face of geopolitical risks, a structured approach is essential, involving close collaboration between the different parts of the organisation, both business (lines of business) and support (procurement, IT, legal, finance, etc.), and regular, proactive information sharing. This section examines the challenges, key stages and best practices for structuring this governance, with the aim of providing the IT department with forward-looking tools adapted to an increasingly unstable international context.

4.1 WHY IS IT DIFFICULT TO INTEGRATE THE GEOPOLITICAL DIMENSION INTO IT GOVERNANCE ?

There are significant barriers to integrating the geopolitical dimension into the IT department, mainly related to the lack of formalised processes and uneven awareness among staff. At present, geopolitical risks and issues are considered mainly on the basis of individual perceptions and team experience, with no structured framework or shared thinking. While predictive analysis is often undertaken to anticipate the impact of geopolitics on the company's core business, the same approach is lacking in IT. This lack of forward thinking dedicated to IT leaves IT departments exposed to geopolitical vulnerabilities without formal tools to assess and integrate them into their technology strategies.

4.2 TAKING THE GEOPOLITICAL DIMENSION INTO ACCOUNT: THE NEED FOR COOPERATION WITHIN THE COMPANY

4.2.1 ESTABLISHING GOOD GOVERNANCE

As we have seen throughout this report, there are many factors to consider when determining the direction of digital strategy in the face of geopolitical fluctuations, and they can affect the various activities of a digital department (purchasing, partnerships, HR, legal, etc.). Taking this geopolitical dimension into account therefore requires collaboration and continuous monitoring within the company.

Risk, compliance and security departments have a culture of prevention, which is necessary to anticipate geopolitical consequences. Drawing inspiration from their prevention practices, which may also exist in cybersecurity, is a first step. We then need to integrate the geopolitical dimension into our risk management processes, into our procedures, our procurement reviews and our IT project architecture. Spreading this culture must then involve setting up awareness-raising and training programmes for all teams, which can include gamification (e.g. the use of 'war games' to put people in situations where they can better understand what is at stake and improve sharing within the company) to strengthen commitment and better integrate risks. As well as being a source of inspiration

through their culture of prevention, these three departments also have access to a wealth of information needed for a full analysis of the impact of geopolitical developments on the digital department.

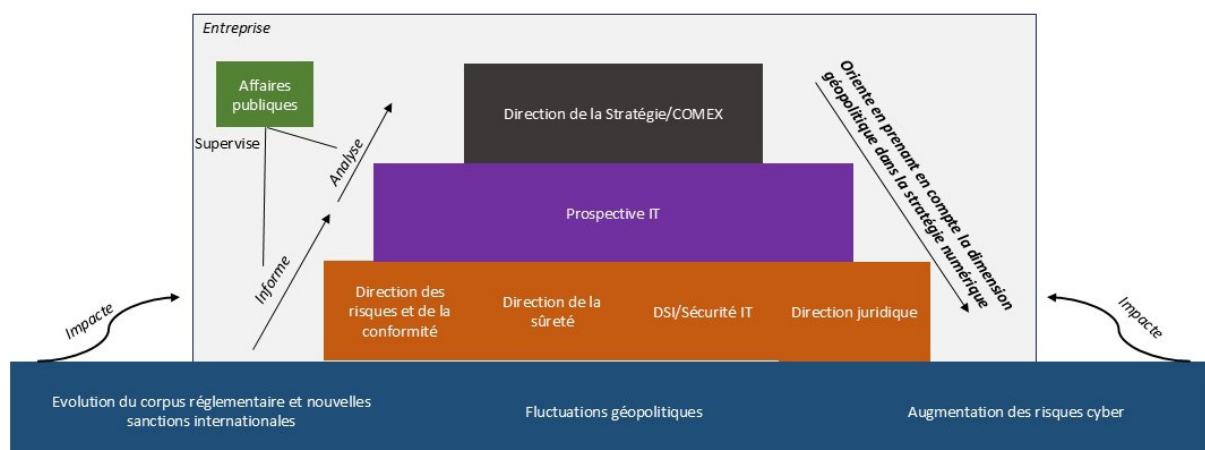
While IT and the organisation's digital security units are obviously at the centre of the debate, they are not necessarily at the centre of organising the approach. This is generally led by the risk department and the business departments, with IT generally remaining a 'support function' to the business. This department has access to all the information related to the organisation's digital activities and must therefore offer its analyses to contribute to the process.

Finally, **the legal department** keeps a close eye on regulatory developments around the world and on new international sanctions, especially in regions where the organisation is present (whether or not in the digital arena).

It is important for these different entities to share information on an ongoing basis, as a piece of information that is insignificant to one entity may have a major impact on another. This information sharing must then be used to feed IT monitoring and forward IT thinking, supported by forward business thinking. The IT monitoring and foresight unit does not necessarily need to be located in the IT department, which remains essentially a contributor, and can be attached to units in other departments of the same type. However, thinking about the digital future must initially be done independently of the rest of the company's forward thinking, because the geopolitical implications for digital technology and the company's business sector are not necessarily the same. This 'IT foresight' unit then provides its analysis and input to the company's strategy department, and its work is presented to the Executive Committee. This unit, referred to here as the IT foresight unit, can have different names and forms depending on the organisation: 'IT watch', 'IT strategy' or even 'IT economic intelligence'. The latter type of unit, which is less broad and more focused than foresight, is perhaps more legitimate in addressing these geopolitical issues. In any case, its aim will be to provide food for thought on the adaptations and/or changes that need to be made within the IT department to cope with geopolitical developments as well as technical, regulatory and social changes.

To ensure that such a sharing and collaboration mechanism is sustainable in the long term, it is generally necessary to monitor and coordinate it. This oversight may be entrusted to the **public affairs department**, to a strategy department or even to a structure attached to the general management.

Finally, it will be necessary to work with the department responsible for CSR issues, as it will have to deal with certain key issues relating to geopolitics, risk and regulatory compliance.



Governance diagram for integrating the geopolitical dimension into IT activities

Beyond the governance aspects, all teams in each country in which the company operates must be involved in this forward-looking reflection to integrate local and specific geopolitical perspectives. The ultimate goal is to create a geopolitical risk management ecosystem and monitoring community, with an organisation that integrates geopolitical risk into all decision-making and operational processes.

4.2.2 WORKING WITH THE RIGHT TOOLS

The IT foresight unit generates and makes available common tools:

- In order to anticipate the impact of geopolitical developments on a company's IT challenges,** it is essential to develop scenarios that include both the geopolitical and climatic dimensions, as well as macroeconomic and regulatory analysis, depending on specific needs. To ensure their relevance, a review process must be put in place every 6 to 12 months to adapt these forecasts to changes in the global environment. In addition, simulation exercises are designed to immerse teams in these complex scenarios and expose them to critical situations to better anticipate the potential impact on their digital operations. War gaming, an offshoot of these simulation exercises, is becoming increasingly common in public administrations, for example. Finally, geopolitical risk analysis should not be limited to non-Western countries. The energy crisis in Germany, exacerbated by the war in Ukraine, is a striking example: energy sustainability, particularly for data centres, has become a critical issue, demonstrating that developed countries are not exempt from significant risks.
- Supplier mapping and a regular supplier review process:** Establishing an accurate supplier map that identifies the geopolitical risks associated with each strategic partner is a first step in helping the IT department better manage geopolitical risk. By comparing this map with future scenarios, the potential impact of different supplier relationships can be visualised. The map then needs to be regularly reviewed and updated to ensure that risks are not overlooked.
- An example of concrete cases combining geopolitical and digital implications: **Raising awareness throughout the organisation is the first objective of such an approach,** as the geopolitical impact on digital activities is often unknown or underestimated. Regularly presenting teams with concrete examples of the geopolitical impact on the business and its IT

helps to reinforce their understanding of the risks. This can take various forms, including formalising training and awareness tools (such as MOOCs) for the whole organisation.

- **Distributing strategic documentation internally means sharing information** that may seem trivial to some but is strategic to others. This documentation must include guidelines for addressing these risks in the company's various IT activities. Public Affairs can then take responsibility for disseminating this information to the Executive Committee and the rest of the group to raise awareness across the board.

4.2.3 LIMITS AND SUSTAINABILITY OF THE APPROACH

Setting up such a system is obviously very demanding in terms of human and financial resources. The proposed governance and tools must therefore be adapted to the organisation's habits. However, we believe it is essential that the inclusion of the geopolitical dimension in the IT strategy is supported by governance, however light, to ensure that the issue is monitored and documented despite the potential obstacles. What's more, the integration of IT foresight with business foresight remains a challenge, as these scenarios are generally short to medium term (3 years maximum).

For this system to work, we believe it is essential to organise monthly physical meetings (alternating with videoconferencing meetings to include remote areas) to facilitate the sharing and updating of knowledge. We need to do more than just share documentation.

Working with the legal department: a necessity for the IT department

Disclaimer: The following text is a summary of a speech given by Martin PAILHES, Head of Digital Legal Affairs at BNP Paribas, at the Cigref conference on 26/09/24 on the subject of "Integrating the geopolitical dimension into the activities of the IT department". The views expressed are those of the author and not of the company he works for.

2024 is a politically very busy year. More than half the world has voted this year, with 64 countries called to the polls, including Taiwan, the UK, India and of course the USA. At the same time, as war rages in Ukraine and the Middle East, we are witnessing the rise of a bloc of countries led by China, Russia and Iran, aiming to challenge the Western order established after the fall of the Berlin Wall.

It is essential to keep this global overview in mind, as the legal instruments adopted by states in this context (e.g. laws with extraterritorial reach, sanctions issued by one state against other states or some of their nationals or companies) can have a significant impact on the day-to-day activities of CIOs.

The following examples illustrate this point, particularly in the digital sector where sensitive or even dual technologies are often involved:

International data transfers outside the EU: towards the affirmation of European sovereignty?

Data is a major issue of sovereignty for governments and a key factor in the functioning of organisations in a globalised economy. However, its circulation is increasingly regulated by law, particularly in Europe, for reasons of sovereignty and citizen protection. The most telling example is the RGPD for personal data in the EU, adopted in response to US laws deemed intrusive and not respectful of individual freedoms, passed after the attacks of 11 September 2001.

Faced with these challenges, initiatives such as Gaia-X, aimed at guaranteeing a sovereign European cloud, illustrate Europe's ambitions for digital autonomy, although their application remains difficult to implement.

Increasing numbers of sanctions mean greater risks for IT Departments

With the war in Ukraine, we are witnessing a succession of sanctions by the US and the EU against Russia. The weapon of economic sanctions is not new, as the US sanctions against Cuba, Iran, North Korea, etc. demonstrate. The ISD may have to comply with these sanctions in unexpected ways:

- Ransomware: Paying a ransom becomes a complex dilemma when the cybercriminal is linked to a sanctioned country such as Iran, Cuba or Russia.
- Intellectual property law in Russia: *What about* renewing trademarks in Russia today?

- Inadvertent recruitment of North Korean workers: Authorities are warning of a growing risk of people applying for IT jobs who are actually working on behalf of North Korea. These candidates seek to infiltrate the computer systems of Western companies and generate illicit revenue for the North Korean regime.

Conclusion: However remote it may seem, the geopolitical dimension can have serious consequences for IT departments. It is therefore vital that they identify and anticipate its impact.

Martin PAILHES, Head of the Digital & IP Platform of the Legal Department of the BNP
PARIBAS Group

5 CONCLUSION: TOWARDS A PROACTIVE IT DEPARTMENT IN THE FACE OF GEOPOLITICAL FLUCTUATIONS

Today we seem to be witnessing a reversal of the rules that have governed international trade and economic activity for at least the last twenty years, around a happy globalisation. In fact, we are moving towards 'de-globalisation' (a world of blocs), which will undoubtedly lead to a revival of geopolitical issues, with symbolic technical examples such as the fragmentation of the Internet or 'splinternet'.

At the same time, the growing importance of digital technology in all business activities has meant that the IT department, once seen as a simple support function, now occupies a central position in corporate strategy. This evolution has transformed the IT department into a strategic player, essential for anticipating challenges and opportunities, especially in a global context characterised by major geopolitical changes. Integrating these geopolitical considerations into IT governance, as explored in this report, is a necessary response to this digital transformation, which now requires a capacity for rapid adaptation and a forward-looking vision.

However, this approach is still in its infancy, as evidenced by the relatively low level of participation encountered by the working group behind this report. This low level of engagement highlights the importance of raising awareness of these geopolitical issues within IT. This is a critical challenge that must be met if we are to strengthen the digital resilience of the business and establish a lasting culture of proactive vigilance in the face of international risks. By continuing to educate and train IT teams in these global dynamics, IT will be better able to support the strategic direction of the business and assert itself as a central pillar in tomorrow's risk management.



Cigref is a network of major French companies and public administrations whose mission is to develop its members' ability to integrate and master digital technologies. Through the quality of its thinking and the representativeness of its members, Cigref is a unifying force in the digital society. Cigref was founded in 1970 under the French law of 1901, and does not engage in any profit-making activities.

To achieve its mission, Cigref relies on three core businesses that make it unique.

Membership

Cigref embodies the collective voice of France's leading companies and government agencies on digital issues. Its members share their experience of technology use within working groups, to help identify best practices.

Intelligence

Cigref participates in collective reflection on the economic and societal challenges of information technologies. Founded nearly 50 years ago, Cigref is one of the oldest digital associations in France, and draws its legitimacy from both its history and its mastery of technical subjects, the foundation of skills and know-how that underpin the digital world.

Influence

Cigref promotes and respects the legitimate interests of its member companies. As an independent forum for exchange and production between practitioners and players, it is a benchmark recognized by its entire ecosystem.

www.cigref.fr

21 av. de Messine, 75008 Paris

+33 1 56 59 70 00

cigref@cigref.fr

The image features a solid blue background with a repeating pattern of chess pieces, including pawns, knights, and rooks, rendered in a lighter blue, semi-transparent style. In the center, a white circle contains the Cigref logo. The logo consists of the word "Cigref" in a large, bold, white sans-serif font, with the tagline "SUCCEED WITH DIGITAL" in a smaller, all-caps, white sans-serif font positioned directly below it.

Cigref
SUCCEED
WITH DIGITAL