
NORTH
ATLANTIC
OCEAN

RISKY BUSINESS

Geopolitics and the Global Corporation

In an economy filled with both promise and threat, business executives must draw a new map of the world.

by Sven Behrendt and Parag Khanna

It has become commonplace to argue that the combination of the September 11, 2001, terrorist attacks in the United States and the conflict in Iraq has forced business strategists to make geopolitical uncertainty a component in corporate decision making. The effect of these crises and associated political decisions on energy, transportation, tourism, insurance, and other sectors demonstrates the massive consequences that wars, wherever and however they may take place, can have on business.

Though some view the cessation of hostilities in the Iraq war and the subsequent fall in oil prices as the end of a crisis, in reality they constitute a mere pause in the transformation of the global business environment. The maturity of Western markets demands that firms expand beyond the confines of the developed world into areas that carry risk far greater than that to which they are accustomed. Major conflict scenarios abound in the great crescent from the Middle East through Central Asia to India and Southeast Asia, which encompasses both the greatest potential for economic development and enormous political uncertainty. Multinational corporations (MNCs) are now active in at least 70 countries rated at "medium" to "extreme" risk, and more than $150 billion is invested in 50 countries rated "fairly" to "very" corrupt in the Transparency International Corruption Perceptions Index, according to Control Risks Group, a London-based international business consultancy. Though a sagging global economy in 2001 witnessed the first drop in foreign direct investment (FDI) in more than a decade, FDI in developing countries fell by only 14 percent, versus 59 percent in devel-

Photograph by Holly Lindem

Sven Behrendt
(sven.behrendt@weforum.org) is senior project manager in the Global Agenda team at the World Economic Forum.

Parag Khanna
(pkhanna@brookings.edu) is advisor on global issues to the World Economic Forum and senior research analyst for the Forum's Global Governance Initiative at the Brookings Institution.

The analysis and recommendations presented herein are the authors' alone and do not necessarily reflect those of their employer organizations.

oped economies, according to the United Nations *World Investment Report 2002*.

In terms of their capacity to actively mitigate this risk, corporations are overexposed. From business schools to boardrooms, the corporate world lacks the models and instruments to remain confident in its understanding of geopolitical trends and political and social change, and the corresponding risks these carry for business activity worldwide. Given the difficulty of modeling global market complexity, many chief executives will greet calls for a major shift in corporate thinking with a resigned shrug. But as Jeffrey E. Garten, the former undersecretary of commerce for international trade and the current dean of the Yale School of Management, argues, "CEOs ought to think more broadly about what true business leadership means today.… They ought to realize that they should take more responsibility for shaping the environment in which they and everyone else can prosper. They should be corporate chief executives, but also business statesmen."

Just as economic globalization has forced political leaders to adjust to the rigors of a nonstop marketplace, the pace of political events around the world requires that corporate executives take the initiative to confront the consequences of the links between geopolitics and business performance. Whereas the global surge of multinational corporate activity in the 1990s brought down national borders, the next era of geopolitical change will be less certain, which will make deeper assessments of and adjustments to geopolitical risk essential for continuing business success.

Many political analysts today speak of the post–September 11 world as highly uncertain and fluid, with systemic "shocks" likely and at the same time unpredictable. In this context, geopolitical risk has a clear meaning for business: It is the potential for international political conflict to threaten the financial and operational stability of companies around the world. To develop a framework to mitigate this risk, MNCs must understand the specific nature of the relationship between corporate globalization and geopolitics, map the "sites of risk" for corporations in their activities, and adopt forecasting tools to enhance their enterprise resilience with respect to threats from conflict and terrorism. CEO leadership is crucial to advancing this process.

Global Hazards

The Cold War's conclusion was met by a tremendous expansion of global business, as corporations found themselves newly able to expand into transition economies and emerging markets. The dogma of the 1990s held that free market enterprise and a liberal economic agenda would lead to more stable geopolitical relations. The decline of interstate warfare during this period also provided a geopolitical environment that enabled heavy consolidation across industries, resulting in the emergence of massive conglomerates with worldwide reach. The economy was paramount; corporations were almost unconstrained by political and social considerations.

Yet business's greater international presence and increasing geopolitical complexity have also heightened business's exposure to conflict and violence, leaving MNCs suddenly and nakedly exposed. They have become larger, more obvious targets for attack, but they also are vulnerable because their strategies were based on the assumption of fundamentally stable geopolitical relations.

In this context, the expression "global player" acquires new meaning: Previously a reference solely to an economic actor, the term now describes a company that has, however unwillingly, become a *political* actor as well. Today, corporate global players function in the complex nexus of what the innovative German sociologist Ulrich Beck has called the risk society. To remain a global player today, a firm must be able to survive not only economic downturns, but also geopolitical shocks.

An understanding of the risk arising from increased geopolitical uncertainty begins with a view of globalization as a process that has made risk an endemic reality — that is, no longer simply the result of conflict in one country or another (though no doubt that remains the case in many parts of the world), but something inherent in the globalized system itself. As *Foreign Policy* editor Moisés Naím has written, "Thanks to the changes spurred by globalization over the last decade … nation-states have benefited from the information revolution, stronger political and economic linkages, and the shrinking importance of geographic distance. Unfortunately, criminal networks have benefited even more."

Globalization involves risk for several concrete reasons:

- **The definition and quality of governance differ vastly.** Governments in the developing world have been slow to adapt to the demands of efficiency required by a greater business presence; thus, such traditional political risks as corruption and expropriation still apply.
- **Nongovernmental actors are empowered.** The increasing spectrum of political and economic activity occurring outside government control or oversight means that vulnerabilities have increased throughout the networks of globalization.
- **Technology advances risk as well as control.** The technologies that facilitate global corporate activity also enable illicit interactions and the sudden appearance of threats; greater security measures taken by governments and corporations can provide "point solutions" to harden systems and structures against specific threats, such as cyberattacks, but because the platforms and infrastructure of business and crime overlap, the window remains open for threats to enter.

Geopolitical risk is not limited to globally networked industries. On the surface, it may seem that urban terrorism and supply chain disruptions affect mostly large MNCs, but rising insurance costs and heightened security measures apply to businesses of all sizes, creating even more incentive to understand conflicts unfolding around the world. These emerging threats interact with changes in international transport and trade. Al Qaeda, for example, has been implicated in recent attacks on economic targets such as oil tankers. Global dependence on key transportation systems such as jet aircraft, container vessels, and tankers is growing steadily, building up an increasing array of complex, economically important, and time-sensitive economic subsystems.

These subsystems are vulnerable not only to conventional "blowback" — the unintended consequences of foreign policy decisions — but also to new, nontraditional forms of warfare. The U.S. Department of Defense's *2001 Quadrennial Defense Review Report* claims that new asymmetric threats such as cyberattacks are likely to increase. Because the so-called revolution in military affairs has widened America's clear lead in all conventional weapons areas, a fact that has deterred most nation-states from traditional military confrontation, the report predicts more attacks that take advantage of the openness of Western societies and economies. Among the most significant risks are those to our capacity to produce, communicate, and use information, which is central to national security in multiple ways, from conducting e-government, to waging information warfare, to combating transnational criminal organizations. A recent FBI survey showed that nine out of 10 business and government agencies had detected

computer-security breaches within the previous 12 months, with hundreds of millions of dollars in losses. Corporations therefore can be adversely affected by the spread of technological know-how.

Furthermore, the impact of just one attack on an economic target — the September 11, 2001, assault in New York — shows that the financial, transportation, and tourism sectors, and possibly the telecommunications sector, are more vulnerable than was previously thought. With the resulting uncertainty continuing to affect the economy, companies are being forced to take on additional costs for security. All in all, according to *Fortune* magazine, the private sector will spend more than $150 billion on homeland security–related expenses such as insurance, workplace security, logistics, and information technology — approximately four times the U.S. federal government's announced homeland security budget.

A Risk/Response Framework

In light of the systemic nature of risk — along supply chains, across geographies, and within transaction networks — a new approach for comprehensively understanding and addressing risk is needed. Such a framework must evaluate exposure at seven sites of risk and develop corresponding strategies. These risk sites are:

1. Presence in Emerging and Unstable Markets. These are traditional political risk sites, encompassing the threat of war, terrorism, organized crime, and expropriation.

2. Distribution of Personnel. Corporate expansion and activity in emerging markets requires staff travel and necessitates having offices in potentially unstable locations.

3. Headquarters. The physical exposure of the corporate "brain" is the material risk inherent in centralized headquarters.

4. Supply Chain and Partnerships. Risk is posed by the potential for breakdown within insecure cross-border operational relationships.

5. Market Volatility. Industries and subsectors such as tourism and energy are vulnerable to geopolitical conflicts.

6. Capital Hazard. Political shocks can cause the sudden loss of investment flow into an industry.

7. Information Vulnerability. Intellectual capital can be compromised by risks associated with false information, miscommunication, poor cybersecurity, and blockage of information flows.

The persistence of such risks should persuade companies that not purchasing terrorism insurance constitutes a moral hazard. Still, many firms in high-risk environments continue to avoid it. Congress has moved to adopt a European-style federal terrorism reinsurance plan, which covers 90 percent of claims over the first $10 billion.

However, insurance is *not* a solution to the existential risks posed by this expanded understanding of risk sites. Although reinsurance schemes are a major mechanism for mitigating the actual costs of risk, the broader nature of risk requires that companies acquire a better sense of the big picture of geopolitical risk in order to secure their operations and markets.

First and foremost, companies must adopt a more comprehensive view of the relationships between various types of risk and the company's mission, strategy, and operations, and develop integrated plans for managing their exposure to those risks. Booz Allen Hamilton has termed the state resulting from such activity *enterprise resilience*, which the consulting firm defines as "the ability and capacity to withstand systemic discontinuities and adapt to new risk environments." Though corporations' risk environments differ, each company that wants to achieve enterprise resilience must relate risks to strategies by creating frameworks in advance for evaluating threats. Each risk requires a corresponding strategy that plots short- and long-term responses and solutions. This collection of strategies to guard against future unavoidable risks is the essence of enterprise resilience.

But integrating political variables into strategic planning is easier said than done; we do not have the modeling capabilities to predict the cycles of an interdependent economy, much less a global economy overshadowed by geopolitical risk. Nonetheless, risk analysis can begin with an understanding of systemic dynamics and trends, evaluated at different levels of analysis.

Systemic risks arise from the complexity that emerges as technology enables actors across disparate geographies to influence one another. Whereas traditional risk analysis focuses on geography, risk today evades geographic constraints. The *functional* risks associated with the diffusion of powerful and potentially lethal technologies are the origin of many business risks today. Thus, the transnational nature of both business and risk means that geopolitical analysis must include local, national, regional, and international dimensions. Firms have increasingly utilized scenario-planning techniques and services to augment their strategic planning

Risk analysis instruments supply "early warnings" about trends and measure a country's capacity to withstand political, economic, security, and social shocks.

in order to develop — in advance — responses to unpredictable events and circumstances. But geopolitical risk calls for a modified scenario process. Typically, scenarios are devised, probabilities assessed, and strategies developed for the most likely outcome. In an era of high uncertainty, scenario planning must be capabilities-based, which means that firms must be prepared for *all* possible outcomes and ensure that flexible strategies can be implemented across the spectrum of risks and futures.

Public–Private Partnerships

Scenario planning and forecasting are essential not only to predict and confront risks, but also to collect data and knowledge on geopolitical trends. Both within and across industries, corporations have a shared interest in understanding these trends to ensure a stable market environment. Corporations generally lack their own intelligence-gathering mechanisms — costly private services are available that cover the spectrum from risk assessment to site surveillance — so the private sector should engage with governments in partnerships to improve their collective capacity to track and evaluate threats.

Cooperation with government agencies provides both long-term understanding and short-term analysis. This collaboration is also called for in the *National Strategy for Homeland Security*, which recommends the development of protection plans for 14 "critical infrastructure sectors." Lead agencies within the government have been assigned to work with the private sector to devise collective risk-mitigation strategies.

Separate industries can also work together under government auspices to build long-term risk perspectives, through scenario planning and wargaming. This was done during the development of the U.S. National Intelligence Council's *Global Trends 2015* report, a multiyear research effort that involved considerable consultation with the private sector and academic community. Though such activity requires overcoming certain Freedom of Information Act restrictions, the post–September 11 climate makes collaboration more feasible than it was before.

Operationally, political stability at the regional, national, and local levels contributes decisively to investment decisions. Risk analysis of specific country stability has improved considerably over the years, though it can never be considered an exact science; no one truly knows what the outcome of a China–Taiwan conflict would be, for example, nor are flare-ups between India and Pakistan predictable. However, there are examples of risk analysis instruments that supply "early warnings" about critical trends and provide a way to measure a country's capacity to withstand political, economic, security, and social shocks. The Lehman Brothers Eurasia Group Stability Index (LEGSI), for example, analyzes social and economic data from more than 20 countries. Eurasia Group's founder and president, Ian Bremmer, points out that some of LEGSI's "political findings can be counterintuitive to market analysis, in that they are forward-looking indicators of social trends and industries." (LEGSI analysis picked up on Latin America's social ills before the markets did.)

Risk assessment and resilience planning must become a CEO-led priority. Most companies have now come to terms with the pace at which the business environment changes, but it remains quite another task to understand these transformations and integrate them into more flexible corporate strategies and operations. The inspiration for thorough consideration of such

Knowledge of risk scenarios must be rapidly diffused through management via tailored "political risk templates."

underlying issues will have to come from corporate leadership: CEOs must demonstrate commitment in order for their firms to grasp the geopolitical "big picture." In an era of endemic globalization risks, strategic guidance is necessary to separate "red herring" risks from those that can indeed have an impact on firm strategy. CEOs must avoid conflating scenarios of such low probability that they require only contingency plans to stay in the market (e.g., technical malfunctions) with those that require strategic rethinking, such as market failures and political shocks. If scenarios and the risk horizons contained within them are properly understood, there can be upsides to not reducing exposure.

CEOs, however, cannot develop an overview of the entire world of risk and its rapidly changing dynamics by themselves. Though CEOs must be trained to differentiate between first- and second-order risks, they must engage senior managers in teams to examine the functional sites of risk and devise mitigation strategies to be incorporated into operations. Knowledge of risk scenarios must be rapidly diffused through management via tailored "political risk templates" that bring together relevant principals for risk-factor analysis in specific risk areas. Particularly in light of the geographically diffuse nature of political risks today, such a strategy will also empower managers around the world to develop crisis leadership skills, which are essential in the event of communications disruptions within a firm.

The Responsible Company

Becoming more resilient in the face of globalization's pressures is not only important for business: It is vital for the national security of the U.S. and its allies. Private-sector organizations operate America's transportation networks, power facilities, telecommunications and data networks, health-care infrastructure, pharmaceutical supply, and most of the security services upon which critical U.S. infrastructures depend. Furthermore, corporate innovations in software, security, and biotechnology will be essential to win the international campaign against terrorism.

But, in many ways, the recognition that the prevailing market-driven paradigm must factor into geopolitical uncertainty also requires that business take on an entirely new understanding of its purpose in a global society.

More proactive than response strategies to physical threats — and more fundamental than regulation, codes of conduct, and corporate citizenship — is the idea that business is a political and social actor with responsibilities beyond wealth creation. The market itself is an authority in global governance. Indeed, the private sector already embodies the "institutional authority" of the standard-setting power of the market, which has considerable impact on political decision making. This in turn means that corporate activity affects both shareholders and stakeholders, particularly in such policy areas as labor, environment, and intellectual property rights in the developing world. Thus, the role of the multinational in self-regulation and standard setting signifies the entrance of the private sector into the broader normative debates of the era.

This is no longer a radical view. Business leaders from Microsoft's Bill Gates to Anglo American's Sir Mark Moody-Stuart have espoused variations on the theme of corporate responsibility as both a moral good and a performance mechanism. The increasingly presumed private-sector responsibility for the stewardship

of global public goods lays the foundation for the new "market ethics." Though such ethics reflect a growing progressive spirit among global leaders, double standards and confused responsibility remain salient features of this ethical tug-of-war between public and private spheres. Business has clearly responded by extending its political management apparatus to negotiate minimal responsibility for public goods management, and at the same time has enhanced social adaptive capabilities through, for example, corporate citizenship programs and improved values communication. But such practices will remain ad hoc until a deeper consensus emerges over a social contract on the sustainable management of the global marketplace.

As Brian Jenkins of the Rand Corporation has observed, "We have spent decades pulling down borders to economic integration, facilitating the seamless transfer of goods across national borders — now the guards and gates are going back up." The strategic change necessary for business is therefore upstream, not to be confused with corporate citizenship policies to make a positive impact on local conditions abroad. Before companies can consider responsible local engagement in overseas operations, they must understand the risks they face in those markets. Corporate citizenship itself will expand only when MNCs make longer-term commitments to developing-country markets.

Nonetheless, it is self-evident that business is a major beneficiary of peace, the most basic public good. Better investment opportunities, reduced operational costs, and expanded markets constitute the virtuous circle that results from the consequences of peace: reallocation of nation-state expenditure (from military toward social/public goods) and the transformation of international lending and aid (from emergency humanitarian assistance toward development assistance).

Thus an important component of geopolitical risk assessment should be an evaluation of the corporate role itself in either increasing or mitigating risks. Does corporate activity promote or hinder illicit trade in weapons and natural resources, does it enable or curb corruption and graft, does it perpetuate illegitimate regimes or foster good governance? And even in the absence of direct political involvement, can business serve as a voice to encourage government engagement in conflict prevention and resolution, or contribute resources toward efforts to rebuild shattered postconflict societies to get them functioning, consuming, and trading again? In the age of systemic risk, corporations are part of both the problem and the solution. +

Reprint No. 03308

Resources

Randy Starr, Jim Newfrock, and Michael Delurey, "Enterprise Resilience: Managing Risk in the Networked Economy," *s+b*, Spring 2003; www.strategy-business.com/press/article/?art=30100980&pg=0

Moisés Naím, "The Five Wars of Globalization," *Foreign Policy*, January/February 2003

David Rothkopf, "Business Versus Terror," *Foreign Policy*, May/June 2002

Jeffrey E. Garten, *The Mind of the CEO* (Perseus Books/Basic Books, 2001)

Global Trends 2015: www.cia.gov/cia/reports/globaltrends2015/index.html

National Strategy for Homeland Security: www.whitehouse.gov/homeland/book

2001 Quadrennial Defense Review Report: www.cdi.org/issues/qdr/

Lehman Brothers Eurasia Group Stability Index: www.legsi.com