IDSS COMMENTARIES (6/2006)

IDSS Commentaries are intended to provide timely and, where appropriate, policy relevant background and analysis of contemporary developments. The views of the authors are their own and do not represent the official position of IDSS.

Getting the private sector involved in national security

Adrian W. J. Kuah*

27 January 2006

IN 2004, the National Security Coordination Centre unveiled 'The Fight Against Terror: Singapore's National Security Strategy'. The document laid out a multi-agency, multi-sector, and multi-pronged approach to raising vigilance, increasing resilience and building capabilities to counter transnational terrorist threats. While extremely comprehensive on the government's perspective and policies on the issue, the roles and responsibilities of the other players are outlined in broad terms. The role of the private sector, for example, is seen as a critical component of Singapore's national security strategy, although it is not fleshed out in detail. This raises several important questions, such as how do we get companies to factor in national security concerns into their business thinking, and how can they work with the government to contribute to Singapore's national security?

Old Ways, New Threats

Companies do not, as a rule, spend a lot of time and energy on questions of national security and political risk, preferring instead to dwell on issues such as markets and profits. Simply put, the corporate planner focuses his attention on matching his company's strengths to opportunities in the market place, while shielding its weaknesses from business threats. Or else he evaluates his position *vis-à-vis* his competitors, clients, suppliers, new entrants, and new products, and then makes his move, *à la* Michael Porter's prescription. In making investment decisions, the name of the game is to trade expected return against the level of risk the company is willing to tolerate. In this case, it is assumed that the discount rate and cost of capital used in business calculations already include political risk, which is broad at best, and vague at worst.

Any form of political risk analysis undertaken by companies, even those with global operations, is separate from and adjunct to mainstream business planning, and occurs with less regularity compared to the continuous monitoring of competitors and product cycles. Also, political risk analysis has tended to be an *ad hoc* and passive activity: buy a report, read it and try to fit its findings into the main business plan, or commission a research project every so often. The point is, the ability to assess socio-political and security threats is not something that pervades the organisation; the ability to assess market and business risks, on the other hand, is something that is ingrained in executives of all levels.

Doing Business Post-9/11

With threats to national security becoming more unpredictable, and the effects of terrorism

more traumatic, business strategies that neglect the national security dimension are inadequate, even dangerous. Transnational terrorist attacks carry a risk that cannot be meaningfully priced into overall market risk, unlike the more conventional aspects of political risk such as currency risk, expropriation risk and labour unrest.

There is, post September 11, a rising trend of companies adopting political risk solutions such as business continuity management and critical incident prevention and so forth. The point about such measures is that, one, they are firm-specific, and two, they are reactive in nature. By contrast, no comparable effort is seen on the part of industry in coming together to discuss national security issues that can affect their operations and facilities. Given the interconnectedness of businesses and supply chains across regions and industries, and the common threat faced by all, it clearly makes sense for industry to work out how best to collectively counter these all-too-real threats to their businesses.

One might ask: why should MNCs concern themselves with the national security of any particular country? This is especially relevant to Singapore, where MNCs dominate the corporate landscape. The reality is that, despite their transnational nature, every subsidiary is located in a local and unique physical, socio-political, cultural and economic environment. They are, in short, a citizen of their local operating environment, and therefore have a role to play in shaping the security of that environment. After all, companies are significant players in the local milieu and responsible to some degree or other for the thousands that they employ.

Conclusion

What is clear about this transnational terrorist threat is that it is difficult for individual governments to tackle them singly. This has led to an increase in cooperation between states in areas such as information-sharing and joint operations. However, the level of dialogue and cooperation between the public and private sector has lagged by comparison. There is a pressing need for companies to engage with policy makers, as well as their competitors, in order to derive the necessary synergies to make national security the holistic and comprehensive project that it needs to be for it to succeed.

The top-down policy approach articulated in the national security strategy document must be complemented by a bottom-up approach that emerges from greater dialogue between government and business. The two sectors need to leverage on their respective strengths in order for such a holistic approach to succeed. While the government has the resources and the reach to implement various measures, it may not always know what the security needs of companies are, or what measures would work in any particular industry. Similarly, companies would know best what kinds of policies and measures are needed and effective for their industries and are far better able to assess the impact of such policies on their business operations. For example, companies in the logistics industry would be able to determine the kinds of security measures needed to secure its transshipment hubs and supply chains and networks, although they would not be able to mobilise the resources needed to implement infrastructure on a national scale.

Lest this sound like a naïve plea for companies to incorporate the national security dimension into strategies that are driven in the main by profits and shareholder value, one should point out that a catastrophic terrorist attack could lead to staggering losses in terms of dollars, damage to plant and property and, above all, human lives. If firms, either voluntarily or

under pressure from interest groups, are already including social, ethical and environmental concerns into how they conduct their businesses, what more the issue of national security?

Clearly, the primary responsibility for providing national security falls squarely on the shoulders of the government. However, this does not mean that companies, themselves significant players in the local context and employers of thousands, should not participate actively in determining the form that 'national security' takes.

---

* Adrian W. J. Kuah, CFA, is an Associate Research Fellow at the Institute of Defence and Strategic Studies, Nanyang Technological University, working in the area of defence economics and management.