Political Risk Management – What Does it Mean?

Insight paper by Harmattan Risk

June 2014

____

Introduction

This paper tries to put some substance to the concept of political risk management, so that for readers it moves beyond the nebulous and begins to take a more concrete form. The paper moves through four stages. One is a brief exploration of the definition of political risk, in order to provide at least some parameters to what we are trying to manage. Next, and mainly, we try to derive some concrete meaning of political risk management by looking at three cases of political risk manifesting, then extrapolating backwards to suggest what management measures might have mitigated these cases, and drawing wider lessons. As we only use three cases, we do not cover much ground, so further reading on issues not covered (for example expropriation cases) is recommended. The case-based learning is the main grist, but thirdly, we briefly take a parallel approach based on simple logical abstraction: If we want to manage this kind of risk, what do we have to do? That is structured as a basic logic tree. Finally, we briefly address the concept of a political risk management strategy.

This exercise will hopefully help readers by positing some suggestions, and it helps us by clarifying the focus of Harmattan's own proposition. Business thinkers know a lot about mainstream business functions, from strategy to human resource management, but political risk management has never been an established function, and as a result it often falls through the gaps in business awareness and education.

An Attempt at a Definition of Political Risk Suitable for Our Purposes

There are a number of definitions of political risk, ranging from those which focus on the effects of government decisions on profit or valuation, to more nuanced definitions that extend towards the fuller concept of socio-political risk. Definitions might be academic to many readers, but in fact they can shape responses to the issue. A very top level definition such as "government decisions that affect profit" is so abstract that it lends little real guidance (and indeed it omits reference to the wider set of political actors), whereas others can be so specific (naming certain risk drivers such as expropriation, war or instability - the industry favourites) that they point to only a narrow range of situations that we might need to prepare for. Very few mainstream definitions include any reference to stakeholders, preferring certain actions or conditions to the nuanced risks that can arise through relationships.

There are some reasonably robust definitions out there, but after some years of familiarity with the literature, we have finally concluded that definitions need to be tailored to general types of situations. For an investment banker, the effect of government decisions on valuation might make sense; for an exporter, government trade, tariff and currency policies would be a useful focus. All definitions would include reference to government decisions and behaviour, hence "political" risk, but from there they can usefully be tailored for purpose.

The type of situation that Harmattan addresses is a foreign organisation having a direct presence, in terms of people, assets, brand, and strategic stake, on the ground in the operating environment, and we focus on "complex emerging markets", countries which are in or recovering from significant socio-political transition and which therefore remain susceptible to weak governance, instability and conflict (a moving target as countries can move in and out of this category, and it can be subjective; nonetheless it helps to narrow down the focus somewhat – we would look at Somalia, for example; we probably have little to add on Poland, unless it devolves into a Ukraine 2014 scenario).

It would be nice if we could just use the definition we had in our book, *A Short Guide to Political Risk* (Ashgate 2010): "Political risk is potential harm to a business operation arising from political behaviour." But in trying to be general enough to capture the full range of sub-concepts, it is too general to be useful. In fact, in the book we then went on to thoroughly deconstruct nearly every word in this short sentence to render some useful parameters, but it was more of a conceptual explanation than a definition. So we will see how this works as a definition:

> Political risk derives from the exposure of people, reputation and performance enablers to potentially harmful government behaviour and decisions; potentially harmful socio-political conditions such as weak governance, instability or conflict; and potentially negative socio-political stakeholder responses towards the organisation. Political risk is especially acute in complex emerging markets, countries experiencing or recovering from significant socio-political transition and still prone to considerable volatility (note that the word "potential" is a key element of the concept of risk – maybe, maybe not, but if nexus of probability and impact if realised indicates at least moderate severity, it needs to be managed).

We could go on, and try to elucidate the parameters of political, or socio-political (a term which explicitly recognises that the boundaries between the political domain and other domains of human endeavour and identity are very porous in many emerging markets). But we will stop there before we get off track. As we proceed, we can bear this definition in mind as a baseline conceptual boundary. We just added to the academic claptrap, but it was an important exercise, because when we say "political risk management", we need some notion of what we are trying to manage.

Extrapolating Political Risk Management Indications from Three Cases

Note: Each of the three cases utilised might be well known and indeed infamous, but in full they are highly nuanced, and we only cover them at a top level. We do not name companies or specific places, (except in once instance where it is recent common knowledge), simply because there would inevitably be arguments with our non-expert interpretation, and we prefer to focus on relevant elements of the situation without getting bogged down in a contest for factual accuracy, a losing battle because even the basic facts are still contested in each case. We think have a reasonable idea of the key salients, and it is these that we seek to convey.

Case 1: US Constructor in Water Distribution Modernisation in South American Country

This large US constructor with considerable international experience won a provincial government tender to modernise the water distribution system in one of the poorest provinces of a less developed South American country. The company was supposed to ensure that households, businesses and villages had access to clean water by simply turning on the (sometimes communal) tap. It would replace the old and dilapidated system in place, thereby providing an alternative to buying from private distributors who used tanker trucks to carry water to user hubs and who sold at variable prices, and an alternative to unclean water from hastily dug local wells. Importantly, the company was also supposed to initiate a system for measuring water usage per registered consumer, and attaching to this to a consistent pricing and billing mechanism.

The modernisation project, including pipeline, purification and pumping construction, went well. Residents were curious, but hopeful, and operations proceeded on track. It was when the company introduced its pricing scheme that issues manifested. The company found itself at the epicentre of a row over "extortionate pricing", and was positioned in the local media and by local politicians as a ruthless capitalist and even an arm of US imperialism bent on belittling and impoverishing locals for its own profit, by manipulating this basic human need. Anti-capitalist groups in the US and abroad took up the cause and further fed the local media frenzy. From negative press, the situation rapidly progressed to protests, then riots and even attacks on company property and attempted attacks on company personnel. Country managers were vilified and threatened. The company cancelled what could have been the lucrative "operate" phase and pulled out, with shaken nerves and considerable reputational fallout. It has remained on the back foot over this incident ever since.

There are two stories as to what happened. One is as depicted in local media and anti-capitalist / anti-globalisation press: A US company made it such that the only way to get water was through their system, which originally promised wide access to clean water, and then turned around and charged unforgiveable prices for it – people were essentially blackmailed into paying for this basic good, and they rebelled and threw the company out.

The other story is the more complex and accurate one. Pricing went from the old system of a nearly flat rate per registered user (which included businesses, farms owned by wealthy land owners, and high-income households who had seldom worried about water conservation) to a fee per amount of water used. Local landowners using irrigation in particular were hard hit, and the highest echelon of this class also happened to own most of the local papers, and were also indispensable to local politicians who relied on their campaign funding. This class faced far higher water prices, whereas in fact the average household or village did not see a significant price increase, and would have enjoyed a consistent, accessible supply of clean water at predictable prices.

The landowning, business and upper classes coalesced and rebelled, and exercised its control of local media and political networks to vilify the company and portray it as a ruthless profit-seeker. Lower classes, having little access to alternative media and being for the most part under the economic domination of the elites, bought into well crafted critiques, which played heavily upon local anti-imperialist / capitalist sentiment. The provincial government had wanted water reform not just because it was useful for people, but also as fulfilment of policy promises in the last election, but they had not counted on the reaction from the families and businesses that to a large extent funded politicians. The provincial government caved in and joined the chorus of voices calling for the company's ouster.

Facing immediate threats and knowing that it had become the nexus of local violence, the company withdrew, at a loss. The distribution system since suffered as a result of poor maintenance, and pricing again treated poor and rich users as the same type of consumer.

What the Company Did Not Do = Retrospective Political Risk Management Indications

A thorough stakeholder assessment would have revealed the latent animosity to the pricing scheme. A simple "what if" analysis could have at least raised the issue. What if we succeed in the construction phase, then implement the pricing scheme? Who would not benefit, what is their influence and what would be the strength of their reaction? Who are they connected to, and how might these connections be acted upon? What might happen to us as a result?

Doing this analysis up front would have indicated the risks that were encountered. Knowing them, the company could have sought contractual guarantees and public support from the provincial government – "You know what we are planning to do, you agreed with this, now help us get the message out about the benefits and stand behind us".

The company could have created a bigger role for local partners, who would have stood well outside any targeting as “foreign imperialist capitalist” and who would have been able to point to the local jobs created by the project as another reason to welcome it.

The constructor could also have conducted a proactive community consultation and education campaign, making villagers and poor segments of society aware of the long term benefits, and taking note of and acting on concerns before they became problems. The company could have established its own media connections, using more independent and national press to convey the benefits of its project, and after there was criticism, using these sources to counter the arguments of the elite opposition.

It could have beefed up legitimate and professional security around installations and expat management personnel, creating at least some deterrence to hired mobs and thugs who posed a threat, thereby buying time for the media activity to counter the vilification issued by the elite-owned press.

That simple question, “Who would be hurt by this and what might they do?” if asked in earnest, and if answered with in-depth fact-finding and analysis, could have saved a lot of hassle. No doubt the company did perform a risk assessment, but there is a tendency to rush this as a rather tedious section of a wider project plan, and to focus more on the commercial and engineering tasks. De-linking a risk assessment, which in this case should have included a detailed stakeholder analysis, from off-the-shelf project planning templates might be a good way to give it more attention and visibility.

Lessons? It might not please the commercial managers or business development team, who seek signatures on proposals as a measure that they are doing their job, but...Ask some hard questions about the downsides, pose the “what if”, ask who might not like what we are trying to do and how they could respond. If the indication is that there would be a major flap and considerable mayhem, ask whether it is worth it in the first place. Or if there might be a major flap, consider how we could mitigate it proactively and manage residual fallout. Plan to manage perception, and our own security, such that we could both mitigate reactions and then sustain ourselves long enough to be buy the time to make our case.

This case focuses very much on the stakeholder equation of political risk. There were no serious issues in terms of conflict or instability prior to entry, but the host environment had a specific power structure and powerful interests within it which could have been discerned and countered had the right questions been raised at the right time. (Just by the way, the case of AES in Georgia is somewhat similar to this one, and is highly instructive – we recommend a perusal).

Case 2: Western Oil Company in War-Torn African Country

This North American company bought its way, through the purchase of another smaller firm, into several contiguous oil blocks in this African country experiencing a civil war. The purchased firm had originally bought the licence from another state oil company from a developing country with rather low standards in ethical business, and the last firm had continued with the original owner's lax standards in business ethics, and had encountered some fallout from the behaviour of its security providers. That did not deter the new buyer, a mid-sized oil and gas company with some, albeit not extensive, international experience at the time.

The new operator took CSR and social investment seriously, both as a way to gain local acceptance and thereby reduce risk, and as a means of keeping its ethical investors on board. It ran several quite successful social investment projects, from water provision to building local infrastructure and providing micro-finance to local village-based agricultural and artisan businesses.

But there was one obvious issue in this context. The company's operation was based in the south, which was fighting an insurgency against the intractable and often heavy-handed northern-based government, which funded itself mainly through oil exports. Just by being there the company was perceived to some extent as (and indeed was, realistically) an enabler of northern state revenues and hence too of military purchases and capacity, which was often applied with little discrimination against the very peoples among whom the operation was conducted. CSR and community relations did not fully mitigate hostility among local communities, and this in addition to a context of civil war meant that physical security was a necessary corollary of acceptance strategies.

The government had stipulated that any armed security had to be via government security forces. This was useful in one sense, as it absolved the company of having to do the difficult balancing act of integrating its own private armed security into this delicate terrain, but it was also problematic because the same forces that would provide security were also at odds with the local communities. Country management made several pleas to HQ to try to exercise some diplomatic clout to enable less reliance on state forces, but HQ was rather oblivious to the realities on the ground and thought that state-provided security was sufficiently cost-effective.

The relationship with the army was not easy. The company security management and country directors tried to work with them to impress on them the necessity of political neutrality and of keeping civil war imperatives separate from company protection. Sometimes the army detachment listened, but did not seem to hear. The security detachment still supported government operations against perceived rebel villages in the area, albeit not as a full-blown participant in the war, but more as an adjunct force to be drawn upon when operations overlapped with the company's area of operations.

But things got even worse. The security detachment was ordered to take a more direct role in local suppression, and it in turn pressured the company to make available company land and facilities for military preparations. Country management notified HQ of this pressure and not only sought guidance, but also pressed their argument that any perceived collusion in the war would not end well, and that it might be the time to threaten to withdraw. HQ, still hazy on the local reality, said to stick with programme and keep the army on board, since they were the security providers after all, and the company was dependent on their goodwill for its presence.

The crux came when the army detachment used the company's operating base and its cleared tarmacs to station and replenish helicopter gunships which flew punitive raids against local villages. The villagers, and the southern rebels, were of course very upset and blamed the company for collusion with the repressive and indiscriminate northern government military. Activating their own well honed media contacts, the southern rebel movement got the story of collusion to international NGOs and media, and the story soon spread to the company's home country.

NGOs and the media were scathing in their criticism. The company's HQ, seldom fully aware of the issues on the ground, made some silly mistakes in trying to downplay the issue, but the facts were well documented. The board sought answers, and investors, especially institutional investors who did not want to be associated with ethical malpractices, issued their own ultimatum: Leave or we dump our shares. The share price fell. HQ was nonplussed by the reactions, and duly issued the command to withdraw. A battered country team left, and the rights to the block were sold to yet another developing country state oil company with a thicker skin for ethical criticism (though they later sold too, to yet another ethically obtuse state oil company from a country where business ethics were a remote concern).

As if shareholder rebellion was not enough, several ethical investment groups took up their cause with church groups and NGOs (some of whom were investors too), who filed malpractice and breach of ethics suits against the company. Although this case is over ten years old, several of these suits are still in progress, and a constant reminder of the company's serious lapse in judgment in that operation.

Since then, the company has devised a rigorous and, by some standards, rather constraining risk tolerance policy – they do not operate in conflict zones or where their operations could be perceived as collusive in a conflict. Unfortunately this episode has stuck with the company to the extent to which when one says its name, the reply is often “Oh, right, they are the ones who had the problems because they let the army use their helicopter pads.” This has tainted what has been a reasonably good record for meaningful CSR and social investment, and overall ethical performance.

What the Company Did Not Do = Retrospective Political Risk Management Indications

A hot zone in a civil war? Come on, obviously it is a hot potato. What were you thinking? The company had an ambitious international growth strategy at the time and was trying to make a name for itself by being able to go anywhere and take on hard environments, yet its inexperience and its HQ’s obtuseness were simply not up for the task in those days.

A preliminary risk assessment would have looked into the problems that the previous block operators had had. Rather than just assuming that “we can do it better”, this analysis would have looked in detail at the choices and constraints the previous operator had been faced with, and would have posed the question very openly, “What would prevent us from having the same issues? Is there anything we could do that would reasonably guarantee that we don’t end up in the same pinch?” Apparently this analysis was conducted and resulted in serious CSR efforts, but it did not go as far as scrutinising the necessary relationship with the military and the company’s bargaining power vis a vis. A serious effort to put themselves into the mindset of the army likely would have yielded two observations: One, the army is tasked to protect us because the oil we derive helps pay for the war effort, which is their priority now; two, the army is the army, and their first priority is war fighting against the state’s enemy, even if the perceived enemy happens to be in our area of operations, and the army will ultimately use any means at its disposal to fulfil this mission.

This could have extended to a stakeholder analysis exercise, which would have included the government, the army, local communities, the rebel movement, and then gone beyond the operating zone to look at stakeholders with a direct “stake” in the company, and potential influential observers of its behaviour. This analysis could have yielded at least a scenario of the sequence of events that led to the operation’s demise.

On that basis, risk management planning could have:

- Suggested that the company simply not bother – it was an unworkable situation and the odds were stacked against us, at least if we look beyond just getting oil out of the ground
- Led to, if we decided to try to go anyway, some very hard preliminary bargaining with the government to enforce a stricture that if we have to rely on the army for security, then the army security providers had to remain politically neutral, adhere to stringent ethical norms in security provision (the Voluntary Principles on Security and Human Rights were still nascent at the time of this case, but its core principles were already well publicised in various forms), and accept our human security training and remain open to periodic transparent reviews of ethical behaviour
- Resulted in a much more hard-nosed argument for a larger role for private security, perhaps as provided by a highly legitimate company based in a well developed democracy and answerable to home country regulators and international ethical standards, capable of effective but diplomatic security provision and of liaison and persuasion with respect to government forces which in this scenario would have formed only the outer layer, not the core security detachment
- Led to checks and consultations with host community representatives to discern any perceived hardship or harm incurred by security provision, by way of adjusting and mitigating the harmful effects of security on host communities
- Resulted in an educational and media campaign that made clear the company's ethical standards and acceptance strategy as a corollary to security, not just to buy favour, but also to pin the government to well publicised and widely known concerns and agreements about human security

Aside from entirely abstaining, these measures could have worked to enable the operation to proceed without the damage that was incurred in the historical record. Abstaining probably would have been the best bet.

A key issue was the role and awareness of HQ, specifically Exco and the CEO – they were well informed about the issue through country management reports, yet never fully put their imaginations to use, to try to really understand the pinch that the operation was in, or how this might lead to negative outcomes. They operated in a world where business was defined as in strategy textbooks, wherein the competitive arena as opposed to the socio-political arena was all that mattered, and from the numbers alone the operation was doing just fine, so why introduce these ambiguous and superfluous concerns into the equation? HQ failed itself, the company stakeholders, and the country team, not to mention the villagers who bore the brunt of firepower launched from company bases.

This is a lesson in expanding the imagination and asking the awkward "why, what ifs" upfront and along the way, and of setting one's principles in stone and working within them rather than having an ambiguous boundary that can stretch enough to let things get well out of hand. It is also a lesson in HQ-country team trust and communication, and HQ letting decisions rest where people are best informed to make the relevant judgements.

Case 3: Gas Joint Venture, In Amenas Attack, January 2013

We will not belabour the sequence of events. This case is recent, was all over the media, and public reports remain fresh and accessible. Needless to say, at least two major foreign operators, several oil and gas services firms, and the national Algerian oil and gas company had formed a joint venture for the development and operation of the In Amenas gas processing plant, which converted the output of four gas fields in the immediate region prior to transport northwards for domestic use and export. The plant was in the Algerian Sahara, only about 40 km from the Libyan border, and at the time Libya was still at a height of volatility (which has hardly abated) since the demise of Qaddafi – Libyan border controls were practically non-existent, and weapons flowed freely in the region from old Libyan army depots.

The attack occurred on 16 January 2013, perpetrated by an armed commando using 4X4 jeeps and armed with the whole gamut of infantry weapons. As the attack ensued, with the insurgents fighting the few immediate security forces, over a hundred people managed to escape the compound, though facing bare desert afterwards was probably scant consolation. There were about 800 in the facility at the time, and the insurgents particularly focused on taking expat hostages. About 130, mainly expats but some Algerians too, were under the gun after the insurgents organised themselves. Many of the remaining 800 hid within various spaces in the sprawling facility, eluding immediate capture but still confined without assured water, food or medical supplies, and with no idea how long they would have to hold out.

The insurgent commando publicised a demand for the withdrawal of foreign forces in Mali – France had troops in Mali helping to organise and conduct the fight against the Islamist insurgents who had recently gained a boost from the influx of Libyan weapons and ex-Qaddafi mercenaries now out of a job and looking for an alternative racket (we will not go into the Tuareg rebellion or its relationship to Islamist radicals here – that is a very nuanced story and the Tuareg national movement had nothing to do with the attack). France and the international community could not relent to acquiescence in what had become a key fight against Al Qaeda in the Maghreb (AQIM). It seemed as though the world was going to suffer through a long series of one by one executions.

Only the next day, the Algerian government decided to resolve the issue on its own terms. It launched an attack on the facility using not just the kinds of special forces that we normally associate with hostage rescue (and the subtle approach we might expect of such responses in Europe), but also conventional forces and mass tactical firepower. The fight lasted several hours, and when the Islamists tried to take some hostages out by truck to a safer hiding place (probably to Libya), these were attacked and destroyed, along with the hostages in them. The final death toll was approximately 40-50 hostages, most of whom were expats, and an equivalent number of insurgents, indeed all of the insurgent commando was killed.

The immediate aftermath involved tallying the dead and wounded, providing treatment to survivors, and liaising with and informing families. Then came post-hoc assessment and recrimination, and the two main foreign companies involved, XXX and BP, were on the defensive trying to explain why they did not manage to look after their workers in what was clearly a high risk environment, not just with the legacy of the Algerian civil war of the 1990s and key remnants of the Islamist insurgent base having been driven south from the more populated north, but with spill-over from conflict in both Libya and Mali. Both indications should have been causes of major concern and pro-action.

Who carried out the raid? Algeria and the nexus with its Saharan neighbours is home to myriad groups, from smuggling operators to Al Qaeda-linked insurgents to sub-nationalist rebels hiding out from other countries. The author, who has been to the Algerian Sahara, can attest that there can be an eerie feeling there, as though the endless dunes and rock fields and perpetual droning wind harbour a dark secret, and it is not hard to imagine a ghostly convoy of bad guys hurling in from the dusty horizon on camouflaged 4X4s. But in this case it was an old arch enemy of the Algerian regime, once known as “Michael Glass Eye”, and Marlboro Man later – he had lost an eye in combat in Afghanistan and cigarette smuggling was once a major funding source for his rag tag group of ex-GIA insurgents who had moved south after their strategic defeat in northern urban centres. He had his own ideas, which were more nationalistic than the globalist Al Qaeda aspirations, but it tied in well with Al Qaeda’s regional ambitions and he bought into their line and structure to the extent to which he could obtain better funding and become a key, lucrative liaison between drug smugglers and Al Qaeda distribution hubs.

Did Glass Eye do it on his own initiative? No. AQ asked him and probably paid him to do it, because they were afraid of the direct intervention of Western forces in what had been an unapproachable hinterland, the Sahara. US Special Forces had been trying to coalesce and train anti-terrorist forces in the Sahara and Sahel for a while, but they had taken no active role in fighting. Now, elite French troops were carving a wide swath in the regional infrastructure, and AQ had to at least imply some repercussions. Why did Glass Eye do it? For credibility in AQ, not that he cared that much about what they thought, as for him even AQ was just a means to an end, and AQ's core probably felt likewise towards him. Bel Moukhtar wanted to jolt the system, and remind the Algerian and Western governments of his group's power, thereby increasing potential bargaining capacity later on. He also wanted to ensure his place in AQ's hierarchy, thereby ensuring his status for funding and intelligence access.

And there is a theory, hard to confirm but not beyond the realm of imagination, that Bel Moukhtar Glass Eye had been a DRS (Algerian national intelligence) agent for a while, and that the DRS either turned a blind eye to what he was about to do, or even encouraged it, as a false flag operation in order to better situate Algeria as the hub in the regional struggle against terrorism, and thereby as the recipient of more foreign military funding. This is not totally outrageous, because there is some rather compelling evidence that during the civil war, the DRS did use false flag operations, often quite heinous, to try to stir popular and civil government resentment against the Islamist groups. In the in Amenas storyline, the DRS commissioned Glass Eye but underestimated his volatility and independent streak, and maybe even his real commitment to his other (AQ) paymasters, and he went rogue, thereby necessitating the Algerian army attack, a thoroughly unexpected contingency, unplanned and hence messy. How much credence we lend to this scenario, we cannot say. Not much probably. The facility was close to the Libyan border, where guns and groups were coming from anyway, and the French incursion in Mali was hot on the table and hence sure to bring some retribution. But it is worth looking for future corroboration of these speculations. During the civil war, Algerian security apparati re-defined the concept of "dirty war" and zero sum struggle, and their measures can challenge the imagination.

Whatever the case may be, when the Algerian government attacked, there might have been a hostage rescue element involved, but overall it was a mission of annihilation of their long-time opponents (or embarrassing rogues according to the latter theory), killing 40 or so guys with Kalashnikovs and RPGs who represented the cream of the ex-GIA and GSPC now harbouring in the Sahara. There was no question in military minds that this would drag into protracted and embarrassing negotiations and ferrying out food and water for those detained *and their captors* for days or weeks. That was unacceptable. The response was immediate, heavy-handed, non-surgical, messy and complete. And perhaps oddly (though understandably if one reads between the lines) there was hardly any Western government criticism of this approach.

What the Company Did Not Do = Retrospective Political Risk Management Indications

XXX, already having a good reputation for transparency, published its own internal aftermath report. Neither BP nor oil / gas services providers have done likewise. We high-light some of the XXX report's key findings about what they think they could have done better. The whole piece is well worth reading and we never had the time for a detailed deconstruction of the document. We paraphrase and interpret, we select only some elements, and we admittedly take literary licence to emphasise key points here. Again, for the full grist and more diplomatic language, the full report is available online.

- **Intelligence failures**: There was purchased information from risk advisories about the country and location and risks therein, but no final integrated analysis bringing these strands together. Had that occurred, there likely would have been indications of an attack, perhaps not clearly enough to define the target, but at least of very augmented armed capability of Saharan threats and their interest in taking advantage of the boon from Libyan conflict spill over (including available weaponry and maybe too personnel) which boosted their capacity and their will to act on it before Western forces had a chance to thwart them. Glass Eye also had a convenient immediate motivation or cause (whether or not true to his heart or just plain convenient or suggested by AQ), which was Mali, and Western (French) intervention which was hurting AQIM. There was sure to be a backlash in some form or another. In other words, aggregate analysis could have revealed strong but time-bound capability and intent. The bad guys had a window, and the joint venture did not see it (and this in spite of received advisor reports – perhaps that makes a good example of not being able to see the forest for the trees, as advisory intelligence reports can often be so nuanced and "fine print" that is hard to draw conclusions from them – try to glean a few key messages across several such reports and one risks a serious migraine).

- **Security as HSE**: Security means managing and deterring threats, i.e. predators, or those who really see us antithetical to their values and interests no matter how nice we are to host communities. HSE means preventing and mitigating accidents and natural disasters, and staying ahead of environmental regulations. They are night and day, one dealing with the dark side, the other with happenstance. To plug security into HSE (or indeed HSSE as it sometimes manifests) downplays the threat equation and positions all issues as a potential mistake or accident. In fact, just because we are paranoid does not mean that they are not out to get us. Security needed its own space, its own process and language, and its own responsibilities in order to better foresee and manage such things as direct attacks on our people and facilities – this was not a health and safety issue, this was an intentional threat by some very driven people, and it needed to be managed differently.

- **Stakeholder understanding gaps**: Bad guys and the security providers we use are indeed stakeholders, and we need to understand their motivations and capabilities in order to discern risks. They cannot be treated as peripheral to the wider stakeholder equation.

  To fling an imagined paraphrase, "AQIM has better things to than to look at us, military protection is fine, they are professional and will act properly if need be." Wrong, wrong. That might be imagined and hypothetical but it is probably not far off what actually happened. AQIM (and its affiliates) and the army were very direct stakeholders, so why not treat them as such and discern their motives and capabilities in detail?

  AQIM, or Bel Moukhtar's rag tag group, probably did not care who was there, be they XXX, British or whatever – it was an operation with a high foreign presence and importance to Algerian state gas revenues, and it was vulnerable to an attack, period. And what better things to do? Run drugs and contraband, the odd kidnapping, sure, but now and then the group needs to remind officialdom of its political clout and renew its status in the AQ hierarchy. Given regional conditions (Libya the means by way of guns; Mali the rationale or cover story), this attack was waiting to happen. We cannot discount a terrorist group as a stakeholder – they have a stake in us, through what we represent, and what an attack on us could do for them. Had local AQ affiliates been mapped alongside other stakeholders, they would have occupied a unique corner of the grid and stood out as a serious menace.

  The Algerian army: Committed to creating a safe environment for foreign operators in order to keep the expertise flowing and thereby make the most of the country's reserves, and expert in anti-terrorism after years of civil war. We can leave it to them. Or can we? An assessment might have yielded evidence of complacency, distraction from events in Libya and Mali, and also an inherent, proven bent to addressing terrorist threat using uncompromising force and a philosophy of eradication – kill them all and sort it out later, hardly appropriate in a hostage crisis involving our people. Why did we place all of our trust in a war-fighting apparatus that had acute national security distractions and a bent towards eradication? We could have negotiated at least dedicated security detachments rather than relying on regional commands, and at the very best, though hard to negotiate, we might have been able to get private security from legitimate and well vetted providers, who would be armed with at least automatic weapons and capable of safeguarding the facility's inner core and people holed up therein.

Lessons? It is hard to take anyone to task after such a tragedy, and like other situations that Harmattan has become aware of, it is hard to blame the dead and to imagine that we could have done much better. That basic truth being said, this was a case in which there was an element of "let's do our job and read these darned risk reports" without trying to really aggregate and translate these into clear probabilities and risk management programming. Reports happened, various people read them, no one did much about them, just as most of us would bargain on things working out okay in the end, and just as most of us would not want to be the first ones to cry wolf when the problem might remain latent forever.

But it happened, and in retrospect it was a failure in intelligence, particularly stakeholder conceptualisation and analysis and a grasp of the implications of recent regional trends; a gap in the process of intelligence to action; and failure through complacency or an aversion to openly state the downsides (the other firms involved notwithstanding, XXX business culture is quite consensus and group oriented, and this could have been a factor had some people had their own individual doubts). Could a dedicated political risk consultant have helped? We would like to think so, but in fact the joint venture was already utilising experienced advisors. The post-hoc frustration is that the information was there but remained fragmented and the threat therefore remained unclear and ambiguous, hence even if there was a strong intelligence to action process it might not have been utilised because no one was really crunching the intelligence inputs to identify critical issues that would have triggered further action.

We can all learn from this mistake, not just XXX who was brave enough to publish some instructive findings for the rest of us. We suggest no negligence nor do we say we could have done better. If we could have, then experienced advisors would have spoken up at the time. It was a hard lesson for everyone. To their credit, XXX has made significant revisions in their intelligence process since the tragedy, building their own in-house analytical capacity, and have acted on their own report's findings with other tangible changes. There are indications that other oil and gas companies have followed their lead.

Aggregating Case Lessons for Political Risk Management Indications

The reader can likely extrapolate key points from the above cases, but as is our bent we will try to render a comprehensive summary here, hopefully not too long winded. So, what are they key salients that derive from these three cases? (and note that these were limited in scope – it would be useful to look at cases involving labour friction, expropriation and FDI policy change, among other issues, but we have enough here for some useful insights for on-the-ground operations). We also go a little beyond to flesh out some issues and responses not mentioned in the cases.

Intelligence

- Create and enable an independent, in-house intelligence capacity that is capable of aggregating all-source inputs, including those from expert risk advisories, and capable of challenging preconceptions or complacency among our business executives – give the team the room to do their job, and do not punish them for "nay-saying" or crying wolf, rather, listen hard and question them to obtain and test their full rationale.
- Ask the "what if" well upfront (and test it again later) and conduct scenario exercises around different outcomes – if we begin to succeed, who is going to be annoyed, what agreements might be abrogated, what might happen? If we take on this project, how would it be different from other related cases or indeed the last guys who tried? Could it be different? Model the outcomes to identify the critical "swing" variables, which we can either control (then keep going) or which are up to chance (consider not bothering or hope for much luck).
- Do not just look at trends and conditions, but look hard at specific stakeholders, and assessments should be comprehensive (e.g. Harmattan was once counselled by a client to ignore terrorist groups because they were not a stakeholder, "just a threat" – we did an intention-capability assessment anyway – it was a silly stipulation for such a key type of actor – if they want to cut our heads off then they probably matter). If "they" might have an interest in our operation and some capability to affect it, for better or worse, then "they" are worthy of our interest and research.
- Grasp the interconnection between global, regional and national political trends and potential trends in the immediate operating environment, and stakeholder (including bad guys) interests and behaviour.
- Integrate risk assessment with respect to conditions on the ground with scenario analysis and stakeholder assessment for a necessarily comprehensive picture, control this process in-house for aggregate indications, do not just hope it trickles down from external risk intelligence reports, which can often read like abstract textbooks. If we own the last mile,

then we control analytical quality, we can direct the right questions, and we fully understand how the final picture was derived.

Strategic Bargaining

- Beware that while a government ministry or state-owned partner might seem welcoming, they are after all agents of their country and will have a development agenda which might not fully take on board our commercial and intellectual property rights – any abrogation on their part could well be a rational move as they aspire to become international players in their own right. Keep some key IP back until we reach the finale.
- Similarly, new nationalistic and populist governments sometimes get a kick out of nationalising sectors where much FDI is present. Assess this risk up-front in the intelligence process, and if it is indicated, then strengthen contractual terms and get some serious heavyweights on board in project financing, and save the best for last in terms of IP hand over.
- We start by just promising to our job well, but based on our risk assessment, we can foresee the state-related or bureaucratic impediments that might affect us – we stipulate these concerns (such as unilateral FDI policy changes from the government) and put them on paper, seek written guarantees, and suggest standard processes and forums to smoothly negotiate mutual concerns as they arise.
- We stick to our guns no matter what in terms of anti-corruption and the ethics of project security – they have to play ball; we are bringing best practice to the table, and if they want a lesser player with looser ethical principles than us, go right ahead. No compromise, or else we set ourselves up for future manipulation and ethical observers see us as sheer profit mercenaries, an image that does sit well with us.
- It is hard to establish a baseline of integrity for any of the above if we do not have a clean and fair win in the first place. The second we take a job that was handed to us in absence of fair competition, we are exposed to pressure and manipulation. We will not compete on unfair terms, and will keep our transactions fully above board, not just to satisfy ethical observers, but also to pin our state partners to the original, well publicised, agreement.

Security

- Do not rely only on government forces for security – our security will never be their main job, and while we might have some control over them, in many complex emerging markets they are still prone to human rights abuses, and we do not want to be associated with that.

- Bargain hard at the beginning: “If you want us here, then please listen” – we need security, but your forces have to comply with best practice ethical standards, and we will require our own armed security management for both inner core protection and as liaison with your forces. The best shot at bargaining is in the early stages, when we have passed all the technical and commercial scrutiny and it would be a bother to find someone else to deliver – and bear in mind that ethical, responsible and alert security could well make the difference in a complex emerging market, so this is not an issue to be brushed under the rug.
- Ensure that we have a mandate to train government security forces in the Voluntary Principles on Security and Human Rights or some clear permutation of them, and a mandate to assess compliance and to call for changes should current forces not meet standards.
- Have a contingency for evacuation (and plans for other types of risk so regard this as indicative) – it can seldom work as a mass migration which is way too indiscrete. People would need to discretely trickle out on contrived but realistic premises, from various exit points and over time in order to not trigger a regime crackdown on our movement. Plan well ahead, and plan for the worst if intelligence indicates that the environment or pressures on us might become unbearable. Help national staff if they might be at risk or face repercussions – it can be hard to extract them, but we can do all we can to help them.

Consultation and Communication

- Based on intelligence, we can see who might have an issue with our presence or operation – if we have a good argument that our operation is in society’s long-term interest, then we make the case, via media and through local consultations (and if, after honest assessment, we think that our work is detrimental to the host society, then we either change the terms or do not go there).
- Estimate the media fallout from negative vested interests (derived from stakeholder assessment under “Intelligence”) and prepare a counter campaign, using strong evidence and clear logic, not polemics or attacks – remain diplomatic and cognisant of our status as guests and beware that all stakeholders, including friends who have high expectations of our etiquette, are watching.
- In shaping both operations and security, talk to local host communities: Listen to their concerns, explain our motives and how we will be working, and then take tangible measures to demonstrate that we have heard and are sensitive to their issues. This might mean varying traffic routes to prevent congestion, working only in daylight hours so as not to `disrupt sleep, having non-obtrusive security guards who are very sensitive to local culture

and human security, etc. If we do not do respond to key concerns, then we will be accumulating resentment that could well manifest as serious risk later on, and we will be losing a key constituency.

- Social investment / CSR is most sustainable when it actually augments our business capacity, because being based on a real need, it results in adaptation to the global economy and the capability to work with other international and domestic firms in the future. But sometimes our presence will have a significant social impact and we will not be in a position to hire many local people or use many local suppliers (and “make-work” hiring is not ideal – it increases expectations and is unsustainable).

  In this instance, we will identify community investment needs, and financially support credible and legitimate community representatives and NGOs or experienced foreign donors with a good track record in the country (as identified in an operational-level stakeholder assessment) towards addressing pressing concerns (this might mean, just for a brief example, water wells, generators to keep local clinics running during power outages, micro-finance for farmers and export-oriented artisans, women’s education to better enable social resources, buying a lathe or internet-capable computers or other equipment to be shared among villagers, or IT for local schools – these are just examples and tangible needs vary). Job and language training are often particularly welcomed – these present opportunities for people to move beyond their immediate circumstances, and to be better poised for meaningful future employment.

- If we begin to become a problem or a threat to the people around us, it is seriously time to renegotiate terms with our host country sponsor or customer, or simply leave, and if we do leave, we will have a phased hand over of our CSR activities to ensure that projects which we have started have a good chance of being brought to fruition. We will also make it clear that we will be keeping an eye on our past host community commitments, and we will publicise our objections to any infringements on human rights as a result of association with us.

Risk Transfer and Local Content

- Where appropriate or useful, we will commission local companies to help provide supplies or as partners in our operation – the host government might well have local content stipulations in place, but with imagination and an eye for the pragmatic, in addition to a willingness to train and share our know-how, we can probably cost-effectively exceed these baseline targets.

- We will only select partners who are ethically clean (as tested by a due diligence investigations process) and responsive to our standards, and an unwritten criterion will be their willingness to help us to garner information about the local business environment and contribute to negotiations with the government should approvals or the official license to operate prove to be awkward for a foreign player.
- We know that sometimes we might be perceived as the foreign bad guy, and the more we take local partners on board, the less weight to any opposition's argument that this operation is just foreign manipulation or a front for global capitalist sociopaths. If we win, then so do our local partners, and their workers.
- Relationships with unions can be hard to manage - they might not trust us as a foreign firm, at least not right away. But if need be we will manage the relationship and work with unions for mutual benefit. Their interests and capabilities will be logged in the stakeholder element of the risk intelligence assessment, so that we have a baseline understanding of them before we even start negotiations.

  And we are well aware from the intelligence process that, in some cases, unions are just tools of the regime and that union issues can be a way of putting pressure on us to comply with regime stipulations. We make a distinction between independent union concerns and regime-manipulated issues. We balance legitimate unions seeking safe, secure jobs for members with our own rationales towards labour flexibility, and we aim to build labour agreements into our contractual agreement. Granted, that might not prevent strikes. If strikes occur, we approach the situation with an ear for listening and some cards held in reserve to meet legitimate demands. If it is more of a fight than a negotiation, we might want to take our leave, not knowing if the unions have been politically motivated to take an intractable stance against us and not wishing to incur further violence or harm. But in less extreme cases we will be patient and see it through.

Conflict Sensitivity

- Our intelligence process, oft alluded to and all important, will indicate potential conflicts in our operating environment.
- Hire from one rival, socially invest more in one contestant and neglect the other – bad news.
- Allow the formation of rival cliques within our workforce, representing conflict beyond our company, also a flat No.
- Balance interests and try to instil the notion that our company brings people together in a common endeavour.

- And we support peace-building undertaken by legitimate, neutral and professional NGOs and transnational donor agencies from established democracies.
- If our project would only pour funds into the government war coffer, not only would we seek to revise this to ensure a strong social investment or national savings element, but we might not engage at all. We cannot afford to be regarded as factor in a war.

Summary of Case-Based Learning and Extrapolation

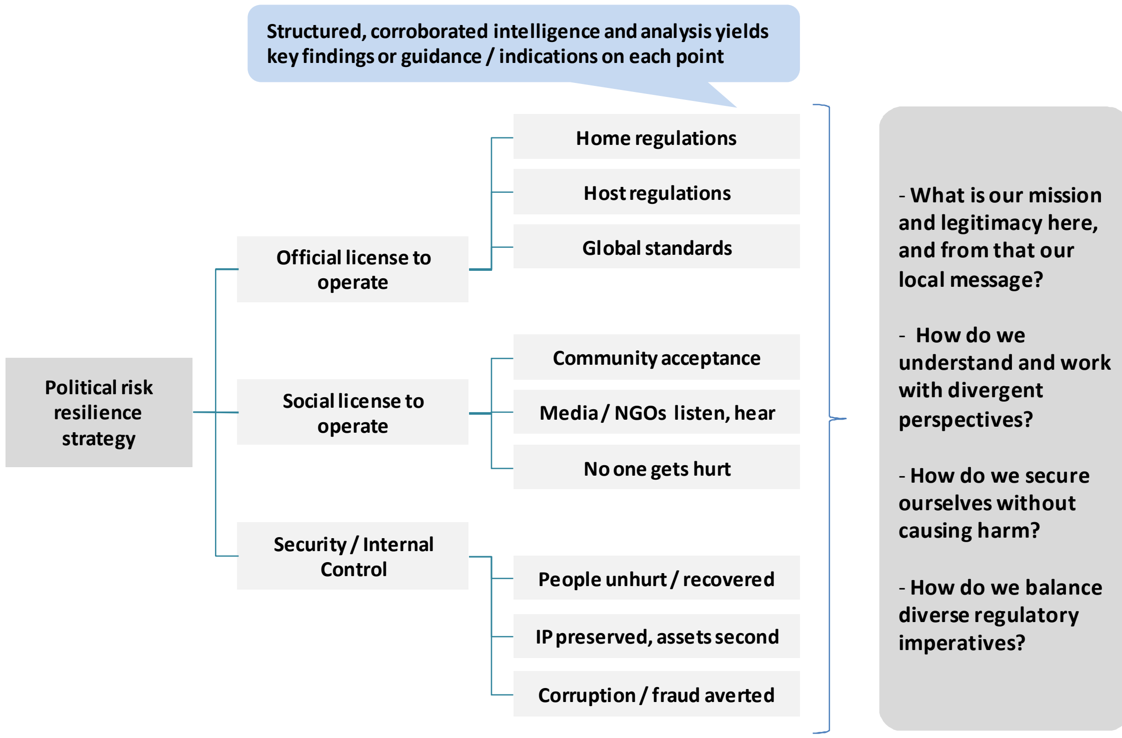
That takes us a bit beyond the cases. We do ramble on, don't we? But just to summarise, here are the areas we have looked at, and even then this is not quite complete (duty of care is a major issue and we have done entire projects around it, for example, though part of that is covered under Security – dare us to spill the beans on this issue and you can expect another 30 page paper):

- Intelligence process
- Strategic bargaining
- Security
- Communications and consultation
- Risk transfer and local content – main focus was local content
- Conflict sensitivity

Each is important, but the most critical element is the intelligence process, and how it leads to tangible initiatives. It is the font of everything we do in political risk management, and that process decides which measures are necessary. Intelligence cannot just be an abstraction. It must be a fundamental but independent part of the decision process, and knowing how to structure intelligence outputs and link them to decisions is one significant key success factor in political risk management.

A Logical Look at Political Risk Management

We had big ambitions for this paper and will come back to it later but right now the author is tired and his mind is drifting, so we will keep this very concise indeed, as it is less interesting anyway, but still potentially instructive in some ways. This diagram depicts much of what we can derive through common sense, and indeed no depiction would ever be complete – unique situations will always arise.



This is not the whole story. Corporate diplomacy is an element that needs exploration, and this does not delve into the internal structures or competencies that handle these issues. This paper is best read in conjunction with the one entitled ***Is There a Political Risk Management Function?***

And, by the way, all business functions have a political risk management role when heading to complex environments, so do not let this convey a message that some of us are exempt from worrying about it – we deal with socio-political risk everyday through individual choices and judgements that add up to a culturally and politically sensitive approach. Assigning political risk management only to remote specialist functions and ignoring on-the-ground Operations' role is a sure-fire way to alienate key people from helping to address this critical imperative.

A Strategy

Dell's strategy was once to get a huge range of options in its supply chain, make them compete for a supplier relationship, then let customers customise their own computers which suppliers would then assemble and deliver to customer specs – with Dell's agents doing inspection and quality control, but then directly to the buyer, with all orders and delivery through the mail or online messaging. Dell provided quality goods with the bricks and mortars taken out of much of the equation, and hence attained a very competitive price point. HP, Compaq or IBM were left in the dust for a while. Things changed since, but we get the idea – a strategy is a unique way of doing things that helps us to maintain standing and pace in our competitive (and socio-political) environment.

The same thing with political risk. Dell version: we outsource political risk analysis and security but hold suppliers to stringent standards, and we do not worry too much about our cultural fit, since after all if we succeed then there will be positive spin-offs for the host. HP version: we delve into the host environment, get to know groups and people, learn their needs, and tailor our operations to minimise animousity, while still looking after ourselves.

A strategy is unique to the company culture and philosophy. Just painting by numbers might yield some insight, but it does result in a strategy. A strategy is a balance of science and art, and in complex environments there is both a need and opportunity to develop a consistent, integrated and communicable approach to our own resilience.