

# Political Risk Management – What Does it Mean in Practice?

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 business readers it moves beyond the nebulous and begins to take a more concrete form. First we conduct a brief exploration of the definition of political risk, in order to provide 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. As we only use three cases, we do not cover much ground, so further reading on issues not covered (for example expropriation and corruption cases, or cases involving the macro-effects of a rapid regime change) is recommended. We then summarise key points from the cases, and finish by briefly addressing the concept of a political risk management strategy.

## 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 real 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) 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 at least to some extent to the context of the organisation bearing the risk. 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. Indeed even with an international company, the corporate HQ’s

definition will vary somewhat from that applicable to operations, at least in level of abstraction. All definitions would include reference to government decisions and behaviour, hence “political” risk, but from there they can usefully be tailored for the organisational context.

The context 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 – in more stable contexts, unexpected regulatory change, for example, might be one of the most significant political risks, whereas in a complex emerging market, the range of potential issues is wider and extends to much more severe issues).

On this basis, we will see how this works as a definition:

Political risk derives from the exposure of people, reputation and performance enablers to potential harmful government behaviour and decisions; potential harmful socio-political conditions such as weak governance, instability or conflict; and potential 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; if an event or condition were not potential, then it would not be a risk, it would be an actual problem*).

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 this probably suffices for now. As we proceed, we can bear this definition in mind as a baseline conceptual boundary.

### **Extrapolating Political Risk Management Indications from Three Cases**

*Note: Each of the three cases utilised might be well known or even 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 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. As well, when we look at what could have been done, this is not intended as criticism. We understand that retrospection is easy compared to facing the unknown. Our intention is to use these cases for learning, not as a critique.*

### 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. An in-depth "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 socio-political risk assessment, which in this case should have included a detailed stakeholder analysis, from standard 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 tenders 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. (As an aside, the case of AES in Georgia is somewhat similar to this one, and is highly instructive and well documented – 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 experienced some legacy issues from the previous ownership, particularly concerning 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. But it was becoming clear that the army's war-fighting imperatives made this separation of roles tenuous. When military operations began to encroach on the company's area of operation, it seemed that the company's facilities themselves might be put to use in the war effort.

Country management notified HQ of the army's character and behaviour, and the increased army presence and activity around the base, and not only sought guidance, but also pressed their argument that any perceived collusion in the war would not end well. Even withdrawal was better than being perceived as somehow collusive in the war effort. 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 raids against local villages. The villagers, and the southern rebels, were of course very upset and blamed the company for abetting 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 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 were 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 sometimes “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***

Operating in a hot zone in a civil war was obviously a tremendous risk and had there been a defined policy on risk appetite, in addition to rigorous prior assessment, it might have been clear that this project was a step too far. The company had an ambitious international growth strategy at the time and even complex emerging markets were on the table, yet its inexperience and HQ's lack of awareness of the realities in such environments 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 might 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, at least given the company's level of experience at the time (it has matured since with respect to emerging market operations).

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 Saharan border controls were practically non-existent, and both people, and weapons from old Libyan army depots, flowed freely in the region.

The attack occurred on 16 January 2013, perpetrated by an armed Jihadist 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 “surgical” 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 40 hostages, most of whom were expats, and all of the insurgent commando of about 40 men.

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 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 population 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.

Glass Eye probably did not do it on his own initiative. AQ likely 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? Partly for more status in the AQ network, which came with its own rewards in terms of intelligence and funding even if his and AQ’s agendas did not exactly align. In addition Bel Moukhtar likely wanted to jolt the system, and remind the Algerian and Western governments of his group’s power, thereby increasing potential bargaining capacity later on.

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 this version of 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***

One of the companies involved openly published its own internal aftermath report. We highlight some of the 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, select only some elements, and we admittedly take literary licence to emphasise key points here. Again, for the full grist, 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 under the wider question, “What are the most tangible risks to our operation inherent in these trends and actors?”. 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. Western (French) intervention was hurting AQIM, and was very likely to result in some kind of backlash in the region. In other words, aggregate analysis could have revealed a significant spike in both the threat’s capability and intent.
  
- **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 much we try to align with the interests of legitimate host communities. HSE means preventing and mitigating accidents and natural disasters, and staying ahead of environmental regulations. These are very distinct concerns. To plug security into HSE (or indeed HSSE as it sometimes manifests) downplays the threat equation and positions all issues as potential mistakes or accidents. In this context in particular, 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 people and facilities – this was not a health and safety issue, this was an intentional threat comprised of some very driven people, and it needed to be managed differently.
  
- **Stakeholder understanding gaps:** Threats in terms of “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. Stakeholders are not just those with whom we have routine relationships. Anyone with an interest in us and a capability to affect us is a stakeholder.

Regarding AQIM, or Bel Moukhtar’s group, it probably did not care who was there, in terms of specific companies, but the gas plant was an operation with a high foreign (Western) presence and importance to Algerian state gas revenues, and it was vulnerable to an attack. Both of these factors in conjunction with the points addressed under intelligence failures above, would have factored into a stakeholder assessment that included AQIM, who would

have occupied a unique corner of the stakeholder grid (high capability, high interest) making it stand out as a serious menace.

With respect to the Algerian army: There seemed to be an untested assumption that it was very interested in 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 that it was fully capable of fulfilling this mission. An assessment might have yielded evidence of distraction from events in Libya and Mali, and some complacency with respect to domestic terrorism which the army had more or less quashed long ago. It also could have revealed an inherent, proven bent to eradicating terrorists wherever they could be found, as a priority that exceeded any other consideration including, potentially, the wellbeing of hostages in proximity to terrorist targets. With both of these considerations, we could have negotiated at least larger dedicated security detachments rather than relying on remote regional commands, and at the very best, though harder to negotiate, we might have been able to get private security from legitimate and well vetted providers, who could have been armed with at least automatic weapons and capable of safeguarding the facility's inner core and people holed up therein, and of negotiating a serious hostage rescue effort as opposed to a military assault.

In Amenas was principally an intelligence failure, but more generally an issue of complacency. Reports were available but apparently there was little effort to read between the lines and address the question, "What does this really mean for us?" Security was present as a function, but embedded in HSE and unable to manifest and exert a full security mindset and culture. If there were people who were concerned, they might not have wanted to be the first ones to "cry wolf" when the risks could in fact remain latent forever. With respect to the Army, it seemed to be sufficient to know that they were responsible for security, without really testing what this could mean in practice. No one derived and tested a worst case scenario.

The two major foreign operators involved have made significant revisions in their intelligence process since the tragedy, building their own in-house analytical capacity, and have acted on their own internal reviews with other tangible changes.

## Summary

A quick recapitulation of the key learning from each case might be useful.

### *Water Constructor Case*

- The project might seem fine on paper, but look behind the commercial terms and ask about who could affect the outcome, what their interests are, and how we could proactively respond to them
- Look at the potential results from the perspective of the recipients of the project's outcome, adjust where necessary to ensure reasonable acceptance by legitimate interests, and plan a counteraction against illegitimate or power-based interests – get our national backers' public support early on or else they will not feel obliged to respond to the same pressures
- Proactively reach out to legitimate host community interests to explain what we are doing and why, listen and adjust where necessary
- Get more local partners on board, who are trusted in the local environment, and who can help us to demonstrate that our work is not just by and for us, but part of a wider effort that includes local companies and jobs
- Secure ourselves against immediate fallout and pressure as often rendered by hired thugs and local mafia working in collusion with local elites – if they want to make us afraid enough to leave, then they will have a serious issue on their hands if they try, and we estimate that they cannot afford to be seen as the aggressor, so reasonable deterrence would suffice until we can make our case and calm things down a notch

### *Western Oil Company Africa Case*

- Ask the question up-front: Are we ready for this? The last operators had a hard time, so why could we do any better? Is it worth it, or should we build up more slowly to such an environment? Do not go further if it seems beyond our reach or capability at this time (having a well defined risk appetite with respect to the political environment can be a good start in making this consideration)
- Set our standards and principals in stone, and make them a bargaining position – if we need to rely on state security, then they need to adhere to human security irrespective of any war effort, and if after this discussion we do not trust their neutrality, then we either get our own people in to handle inner core security and liaison, or we back off and ignore the deal; there is too much at stake, with this one operation in a very sensitive environment potentially determining our apparent corporate position on human security

- The war, the army, our own position within that context, and the human security risks involved with having state security provision in the midst of a civil war are key factors – assess the interests and scenarios early on, and determine the issues that we might need to contend with
- Ask the host community what they are experiencing as a result of our presence, and ask what more we could do – revise policy and procedure if they are experiencing risk as a result of our presence, and if they are experiencing a reduction in their human security and if we can really do nothing about it, again, leave it to someone else to appear to be in collusion with a war-mongering regime
- When it starts to look like we are a political actor, or are collusive in abuses, then cut our losses and withdraw, an act which shows responsibility at least; we can recover and fight more winnable battles elsewhere
- HQ listens to, and hears, what the country team is saying, and recognises its own limitations in terms of not having been there (for long at least) to really experience and understand the situation and pressures

#### In Amenas Case

- Re-examine the context in which the operation is occurring when major changes are in progress; it is time for blank-slate thinking and a full reconsideration of the potential issues – how does this affect potential threats and their capability to cause harm?
- Just because they are official and tasked with our protection does not mean that security providers are exempt from our assessment – our security providers (and hostiles) should be included in a stakeholder assessment and questions of them should be posed in a way that challenges our assumptions and which yields new insights
- Negotiate for dedicated security who are inculcated (or willing to be inculcated) in ethical tenets, but also immediately at hand and responsive, and if the state security seems incapable of a quick and professional response which puts our people's safety first, then press for independent, legitimate private security (with capability for inner core defence , evacuation planning and execution, and liaison with state security agencies) as a corollary to any proffered state security
- Look at the worst case scenario, and if it is reasonably plausible then plan for it – do not be afraid to temporarily withdraw during periods of high risk; it is expensive but far less costly than the alternative of a security blow-out entailing human tragedy and a subsequent scramble to explain and recuperate

- In high threat contexts (threat is a person or group, risk is a bad thing happening, just to reiterate), give Security some limelight, do not peg them to HSE which is a less dynamic function and less accustomed to dealing with predatory or opportunistic threats

#### Aggregated Learning Points

- Consider stakeholder reactions and develop pro-active communication and engagement plans (engagement in terms of predatory interests seems like an oxymoron, but distance and deterrence are in fact a way of communicating, as is a clear “no” when it comes to corruption pressure, backed up with reference to relevant international regulations to which the company has committed)
- Consult with host communities and adjust the way we handle our own operations and security – there is often room for compromise, and CSR can help manage any residual gaps or provide offsets when a degree of disruption is inevitable (there needs to be a strong linkage between CSR and Security or else there is a bad cop - good cop dichotomy which host communities often find confusing and disingenuous)
- Be proactive in getting legitimate and independent local and national media on board, make a case in our favour when we are certain that we have a legitimate position and that our work will be beneficial to most people affected (if we are not certain or have nothing good to say about ourselves, then it is time reconsider the basic premises underlying our presence; profit is the business aim, but long-term profitability erodes as reputation for responsibility declines – exploring the linkages are worthy of another paper, but to put it briefly, we have seen time and time again that a solid reputation for responsible business is a key factor in negotiations and obtaining deals with government sponsors who cannot afford to contend with reputational liabilities incurred by invited foreign direct investors)
- Pin our sponsors to our principles and limitations and ensure their support on our concerns; if they agree to our work in the first place, they need to follow through
- Ask “what if’s” up front and be prepared to act decisively on negative answers; do not just glance at risk reports, but take the time to aggregate assessments and to use these in hard-nosed “what if” exercises which are visible to the Exco and country management
- Secure ourselves – if someone wants to threaten us for illegitimate gain, it should be hard to do so and our security would make it a serious tangle worthy of front-page news and exposure; but apply security with all due respect for local human security and cultural sensitivity, and do not abide by heavy handed government security when it could threaten the people living in our operating environment or our image as apolitical

- Create and utilise a dynamic intelligence to action process, that garners and analyses relevant inputs towards questions around the sustainability of our operation and which creates a full picture of risks and risk scenarios, which we can use to shape our initial entry, to adjust how we do things once involved, and in planning contingencies for a coordinated rapid response to manifesting risk
- HQ-country team liaison and understanding has to be tight and trusting; HQ can press the business imperative, and the country team has to listen, but when the country team says enough is enough, HQ cannot force people on the ground to do what they deem unsavoury or high-risk – they are the ones on the ground after all, and they know the situation much better than Exco or HQ (this is also a duty of care issue, not just one of alignment between corporate and country)

### Political Risk Management Strategy

The above cases can coalesce with general emerging good practice to form guidelines and policy. That is potentially quite detailed. What we suggest here by way of wrap-up is simply a brief explanation of the concept of political risk management strategy, the top-level philosophy and approach that a company shapes and tailors over time as it proceeds in complex environments.

Political risk management strategy:

The unique and contextualised way in which an organisation identifies and defines its non-commercial, non-technical socio-political risks, and then addresses them through programmes that fit together for synergy, and which align with strategic positioning and core competencies.

Political risk strategy generally aligns with corporate or business unit strategy, and can range from simply guarding the core business, to integration (and acceptance) within core supplier and market geographies and communities. There are many potential variations, including an evolutionary or emergent approach allowing for adaptation along the way.

Strategy implies a long-term plan, and not getting side-tracked by short-term tactical considerations as we pursue long-range goals. Any plan needs to be sufficiently flexible to take into account immediate risks and issues, but a handful of negative incidents should not derail the wider strategy. For example, a company that has successfully relied principally on an acceptance strategy cannot afford to lose its way or succumb to gut reactions if it experiences a handful of security issues. These need to be dealt with, but in the wider context of the acceptance strategy. However, when the operating terrain undergoes

fundamental shifts (for example as in the In Amenas case where the Sahara had become much more dangerous in a short period) then a strategic repositioning is warranted. In the main, any strategy is a long-term plan, which takes into account our ambitions and limitations, our business environment, our detractors and threats and supporters, and which aims for a specific goal, in this case legitimacy and sustainability of our operations.

The elements of a political risk strategy often include:

- Who we are, what we are trying to achieve, and our socio-economic and symbolic impact on communities where we work
- Risk appetite as a clear recognition of the limits in terms of the kinds of situations (e.g. civil wars, or dealing with very corrupt governments) where we are not prepared to operate
- What we expose in the project (relevant elements of people, reputation, continuity, control)
- The threats that could organise against us and how to deter them and keep our distance
- The risks inherent in the operating terrain and contingencies to minimise exposure or effect
- Potential friends and supporters, and how to access them and appeal to them through tailored messaging
- Our own self-comportment and our own honesty and responsiveness to communities affected by our operations
- Maintaining a balance between hard (security) and soft (acceptance) protective measures, keeping us safe while not exacerbating tensions, infringing on rights, or making ourselves appear unapproachable and disinterested in our effect on the people around us
- Our willingness to explore the downsides, including both risks to us, and risks to the communities within which we operate, using a defined intelligence process which is not constrained to support commercial imperatives, and which is de-linked from standard planning templates for greater visibility and independence
- A clear red line about who we are and our ethical responsibilities and limitations, beyond which we will not cross, and even before the red line we would need confirmed support or at least acknowledgement of our concerns by government customers or partners if we were to proceed

This is a concept, but it needs to be explored internally through discussions between commercial, operational and specialist risk management teams, not to mention the senior leadership level. There is no single answer as to what constitutes the best strategy; the above are baseline points and would need to be contextualised within the organisation's culture, experience, and ambitions.

*Copy right Harmattan Risk*