Political Risk and Consulting Engineers in Emerging Markets

Introductory discussion paper by Harmattan Risk

2018

Contents

Introduction

The objective of this paper is twofold. One is to provide introductory insights on political risk and political risk management in emerging markets for small to medium-sized European and UK consulting engineering companies. This means introducing the concept and its relevance, illustrating some unique political risk challenges for consulting engineering firms, and suggesting how political risk management can be organised in smaller organisations that lack an array of specialist risk-related departments.

Second, this paper is a working hypothesis and is aimed at providing the basis for discussion to refine and contextualise indications herein for greater relevance to the consulting engineering sector. Harmattan Risk has worked with a variety of sectors who need to be on the ground in emerging markets to meet their aims, including the construction sector, but we have yet not worked with consulting engineers, hence this paper can be seen as a framework for further consideration.

The paper draws on our own general knowledge and experience, and while we make reference to certain publicly known cases herein, in references to our own casework we necessarily do not provide specifics on the company involved.

Definitions

Political risk is short form for socio-political risk, the wider set of potential issues that a foreign company can encounter as a result of weak governance, conflict, instability, and tense or sensitive socio-political stakeholder relations. These factors are present to varying degrees anywhere, but more prevalent in less developed countries because of lower levels of official institutionalisation (e.g. it is not uncommon in developing countries, even major transitional economies such as China and Russia, for senior political figures to have substantial business interests, and to favour the interests of their unofficial patronage networks in their official behaviour) and less cohesive national identities (i.e. more and stronger "us versus them" perceptions within the same country). The social aspect of political risk is more prominent in developing countries because weak institutions often coexist alongside social and traditional authority structures, and this can blur the lines between civil society, business and official domains. Additionally, because of the poverty and wealth inequality in many emerging markets, the social effects of foreign direct investment can be much more contentious than in developed countries.

Consulting engineering refers to the professional service of providing feasibility studies, design, and programme management in the development of built infrastructure and technical facilities. In this paper we confine ourselves to civil and infrastructure engineering, which would include for example water, waste, and environment; power and energy; transport and

logistics; public service facilities and urban renewal. Our focus is also mainly on small to medium sized firms, since they are more representative of the broader sector. Much of this paper can likely be extrapolated to other sub-sectors and larger firms.

Consulting Engineers' Emerging Market Opportunity

Emerging markets go by a variety of labels, but for practical purposes are developing countries, such as many in sub-Saharan Africa, and countries in a period of rapid economic transition but with highly uneven development and lagging governance standards, such as China, Russia or Turkey.

"Emerging" might be a hopeful label but it does describe the rapid growth of developing countries in recent decades. Growth is high partly because of low starting points, but also because of the global spread of growth-enabling technologies, allowing some developmental "leap frogging". High growth has created considerable interest in emerging markets as consumer markets, but also significant demand from emerging markets for the necessary infrastructure and facilities to handle increasing economic activity, and for public infrastructure to accommodate increasing demand for modern public services. This makes emerging markets a potentially significant opportunity for consulting engineers, whose services can help scope, guide and facilitate desperately needed infrastructure expansion and related technical development.

The Emerging Market Downside – Political Risk

The main drawback to many emerging markets is that the political landscape and dynamics within it are often the principal cause of problems for foreign companies with a direct presence. Demand and commercial opportunity have far outpaced the evolution of consistent and well functioning political institutions and national cohesion in most emerging markets.

Political risk often conjures up coups, revolutions, terrorism and expropriations, but while these major events do happen from time to time, the less spectacular issues have been responsible for far more headaches. Weak governance, which includes corruption pressure, political and even regime interference in contracts, and ambiguous regulations and bureaucratic processes, can stall operations and cause severe management distraction. The attitudes of local communities with hopes and concerns about the foreign company's project or what it could lead to can result in wariness and hostility which, if unaddressed, can draw in political, organised civil society and media observers and lead to critical scrutiny and reputational liability. A combination of poverty and weak governance, which can include weak and corrupt policing and political-criminal collusion, can make security a day to day concern with very high stakes. Meanwhile, even though extreme political risks, including violent regime change, are infrequent, when they do happen it is usually a surprise because

infrequency lulls even expert observers into expecting more of the same. Companies thus bear the additional burden of keeping an eye on even the outside possibilities given their potential consequences.

The above suggests that while there is opportunity in emerging markets, knowing about and managing the socio-political variable can be as important to success as technical and commercial acumen.

Political Risk Considerations for Consulting Engineers

The usual menu of general political risk factors applies to many companies, including consulting engineers, with a direct presence in a potentially unstable or weakly governed country. These factors include trends and dynamics in the political environment, captured within the categories of weak governance, unrest, instability and conflict. Factors also include official, civil society and predatory socio-political actors who feel they have a stake in the project, and their potential attitudes and responses. Finally, longer-term outlooks for political evolution indicate how the wider socio-political landscape might shift over time and the implications for continued project feasibility. When these factors are matched against particular company exposures or performance enablers (e.g. personnel, reputation, business continuity and contractual consistency), risks, or potential problems and issues, become apparent, and these can then be assessed to derive priorities that warrant explicit risk and stakeholder management initiatives. What matters varies by the company and operational profile, the country, and the project's socio-political significance, but the above broad considerations usually serve as a starting point to catch and assess relevant potential challenges.

Rather than delineate the usual suspects in terms of political risks, this section will look at a few issues that could be of particular relevance to consulting engineering companies, given their focus, operating model and typical exposures. Bear in mind that we defined consulting engineers quite narrowly (see earlier), and that definition will help draw out relevant considerations here.

Working for and with Governments

National or local infrastructure projects are commissioned by governments, and national or local authorities, including state companies, are the usual infrastructure client. Working directly for governments can entail some unique challenges, especially in a context where governing institutions and decision processes are weak and opaque.

In a well established Western democracy, there are policy flip flops and indecision that affect even stated infrastructure investment decisions, but because of set institutional processes and governance transparency, it is relatively easy to see the direction of investment commitment well in advance (one exception is in election periods). Furthermore, Western governments and local authorities generally abide by the law, which itself is quite clear. If they sign a contract with a supplier, for example a consulting engineering company for the design of a new highway, they are bound by the terms, and if they unilaterally cancel a contract, even if they are the government they still face an independent judicial system that is the ultimate arbiter.

In many emerging markets, the above assumptions are only partly valid. Because of weaker institutionalisation, politicians and authorities are affected by a wide array of non-official interests, including patronage networks which may indeed form part of the de facto regime (in other words, traditional ties can be even stronger than official institutional hierarchies). This makes it very difficult to really see the decision influences and real decision process within government, and also introduces a range of opaque interests into what these decisions are. Seemingly abrupt changes in government attitude and commitment for a specific project are not uncommon, in some cases even after a project has been contracted. And unlike in more established polities, where the rule of law is weaker and governments have more control over the courts, concern over legalities and fair legal consideration for affected suppliers cannot be assumed.

The above can affect even basic and initially rational infrastructure decisions, but consulting engineers need to be particularly wary of "prestige projects", often mega projects aimed more at enhancing a regime's image and with "white elephant" potential. These are particularly subject to changes and delays, partly since financing is usually tenuous, but also because they attract intense national political intrigue.

The above indicates that dealing directly with emerging market governments entails higher payment and contract cancellation risks, and more difficulty in seeking redress for these issues. Many consulting engineers prefer to engage in infrastructure projects through transnational and national donor / lender agencies, such as the International Finance Corporation, World Bank or Africa Development Bank. These institutions carry considerable clout with national governments, and can penalise contractual non-performance, hence providing a deterrent. They also provide some financing upfront, and this helps to assure payment even if the government itself cannot or will not pay for whatever reason. Even if an international lender is not initially involved, there could be an opportunity to work with a government to seek lender involvement through grant applications.

Another option is political risk insurance or guarantees from a major donor agency, such as the Multilateral Investment Guarantee Agency of the World Bank. Typically donor or lender

insurance is not as flexible as private insurer coverage and also more expensive, but this option too brings an influential third party into the equation, and the World Bank and similar agencies also have an explicit interest in good governance that adds a layer of scrutiny to the recipient government. The problem with political risk insurance is that it is quite expensive, and it would only be suitable for large and long-running projects. International construction firms routinely use such insurance, but for a smaller consulting engineering company covering a limited design phase, it might not be affordable or indeed worth it.

It is of course possible to work directly with emerging market governments, and there is a wide range of governance standards. Better governed emerging markets / developing countries are not dissimilar to European countries in terms of contractual and legal protections. However, when governance is an issue, contracts need to be carefully designed for clarity of terms, ideally include explicit payment guarantees, perhaps include staged payment to identify any payment issues early on and avoid the risk of non-payment for the whole project, and specify redress or arbitration in a mutually trusted judicial system or forum. When a government does not agree to bare essential contractual protections, perhaps instead insisting that trust needs to go both ways, then it might be time to reconsider the company's involvement.

A lot more could be said about dealing directly with governments, for example to bear in mind that governments and especially politicians often have their own political careers front of mind, that government personnel tend to be less in tune with global business culture, or that if one dislikes a government's authoritarian tendencies, if you came this far then you should keep your sensitivities to yourself if you want to see the project through. The above hopefully suffices as an introductory snapshot to some of the more tangible concerns.

Project Social Profile and Potential Contention

Projects which concern national infrastructure, public services facilities or significant changes to the physical landscape of a particular community tend to have a high national or local public profile, partly because they can to lead to significant changes in people's day to day lives. This generates considerable public interest, and potentially contention.

A consulting engineering firm might have a small operation and footprint on the ground during a design project, but their project is often a harbinger of much more significant change to come. If the project is for a significant new piece of infrastructure, for example an airport, highway or power plant, then it will eventually lead to a multi-year construction project that has the potential for considerable local disruption, even including relocations of people living in or near the development site. Conversely, many people and local businesses will also be interested in the jobs and supplier contracts that such a large-scale project could generate, in

addition to the conveniences that the new infrastructure might provide. In short, the first hints of activity on the ground, even if only a glimpse of surveyors, makes the wider project seem real to affected people, and responses are likely to accrue even prior to the construction phase.

No matter how rational or well planned, not everyone is going to like a project or its future results, but public contention and negative scrutiny tend to be less widespread and less pointed when:

- For public sector projects (as most infrastructure projects are), the investment decision was undertaken through legitimate and transparent official discourse, i.e. not just decided on the apparent whim of the political executive or perhaps an unchecked local authority.
- There is a clear case for the project from a socio-economic or developmental standpoint, and this case has been well communicated in transparent and accessible terms (in public infrastructure projects the government would lead on communications). This case also includes a robust explanation of how the resulting infrastructure can be effectively maintained (hence not becoming a waste after only a few years, for example as many roads in tropical environments do because of water damage).
- There has been a social-environmental impact assessment (SIA) which goes beyond only compliance and actually derives clear recommendations on how to reduce negative impacts in project location and design (consulting engineers might not be responsible for undertaking an SIA, but it is difficult to factor social impacts into project design without access to one).
- There have been other structured stakeholder consultations especially with local communities and representative civil society organisations, as part of an assessment that goes beyond the strictures of a mandated SIA and instead provides detailed intelligence on stakeholder perceptions and concerns in addition to ensuring that affected communities feel as though they have been legitimately consulted and have clear channels to express concerns or grievances (which suggests a grievance mechanism as one output). Again the consulting engineers might not be the ones to organise such an assessment or manage a grievance mechanism, but ideally they would be consulted in the assessment design and of course have access to results.
- If the government is the customer, the more transparent the tendering process for involved suppliers, the less people are suspicious that there could be corruption or nepotism involved or that the project somehow benefits regime-connected business elites or communities at the expense of others.

The converse of the above points are usually indicators that wariness and antipathy will arise. Aside from making an unpleasant work environment for a foreign consulting engineering firm,

public hostility can lead to tangible issues. Protests can delay work, and if they escalate then they can also be a security hazard for personnel in the vicinity. Sabotage and threats can occur. If protests are met by a heavy handed police response, this can associate the project with state repression and make the foreign company seem collusive with a repressive authority. Professional human rights and environmental NGOs might get involved, and their media relations prowess can lead to serious reputational damage which reverberates not just locally, but also in the international market. In a few cases, albeit well after the consultancy and design phase, foreign infrastructure companies have actually been driven out of a country after protests and threats became an acute hazard and local governments wanted nothing more to do with a controversial project and withdrew their support.

It should be noted that negative public reactions might mean little to a more authoritarian government, which might just repress any open criticism of its plans, seeing even social and environmental protest as subversive political dissent. That a government might not be concerned is no help to involved foreign companies. It is likely to only increase legitimate local and public hostility, draw in international ethical observers, and draw associations between a foreign supplier and an authoritarian regime.

A consulting engineering company, even if only involved in preliminary project phases which do not allow for much control over the wider project, still has some options to increase the overall social acceptance of the project and reduce antipathy. Because consulting engineers do handle the design element, there is an opportunity to demonstrate cost effective design options that mitigate negative social impacts. In some cases the consulting engineers will be responsible for the SIA or can press to participate in its design, and this is another opportunity to ensure that issues are identified and taken into account. The company can also make the case for an independent stakeholder assessment and consultation exercise as a corollary to its own engineering work. Additionally, the company's own comportment in how it deals with the host community, including through local corporate social responsibility initiatives, can help to reduce negative perceptions. Finally, robust anti-corruption in the consulting engineers' own operations is imperative, in this context not because of legal liability, but because corruption in any aspect of the project can be a factor in eroding public confidence.

In practice, however, there is much that is beyond the control of consulting engineers when they are handling only the design phase of a wider project. If options that reduce negative social impact are suggested, they might not be accepted if they increase costs. However sound the consulting engineers' own comportment, CSR and integrity performance, if the wider project was ill-conceived or if it is seen as a prestige project for a corrupt regime, then public wariness will likely extend to all phases and players in the project. Concerns about the more disruptive upcoming construction phase could overshadow any sound social performance by the consulting engineers. Simply avoiding involvement in projects that stand on shaky

developmental or ethical ground is sometimes a safer bet than getting involved hoping to have a positive influence on other major players while at the same time trying to stick to one's own budget and schedule. Working with and through international donors helps add a layer of developmental and ethical assurance, but the IFC and World Bank, among others, have had their own issues with controversial projects, so this should not be seen as a guarantee.

Whether or not such issues are relevant depends on the project and in many cases there will not be much cause for contention, but the risk of severe contention should be assessed upfront and monitored as the consulting engineers' engagement evolves. Through the company's own comportment and its influence on other stakeholder it can have some effect on negative social perception, but this should not be overestimated. As a factor of organisational culture and brand, some companies are more sensitive to social perceptions than others. A look at the oil and gas sector, for example, reveals very different tolerance levels for social and ethical criticism, with some quite willing to regard even widespread antipathy as par for the course given the business they are in. But every company has its limits, and especially smaller consulting engineering companies need to be sensitive to how a given engagement could affect their wider reputation in segments and places where they see future growth opportunity.

If the consulting engineers are supporting the more intensive construction phase, then there are additional social perception considerations, and these are noted later in the section on working with construction contractors.

Local Content and Local Subcontractors

Many developing countries have local content regulations mandating that a certain proportion of labour, supplies, and subcontracting in foreign business operations comes from the domestic market. This is not just a way of providing jobs, but also a way of acquiring new skills that boost overall national technical and commercial acumen, hence ultimately accelerating socio-economic development. More strenuous local content is typical in less developed countries such as in sub-Saharan Africa than in transitional economies where local content might only manifest as the official or de facto need for local partner. There is considerable variation in local content rules, and sometimes only operations of a certain size, in terms of staffing or revenues, trigger the rules. The following proceeds on the basis that there will be some local content regulation relevant to consulting engineering, and this will often be the case, especially for larger projects or when setting up a long-term country office.

Enforcement of local content rules can vary. They can be relaxed when a government is competing for foreign investment, and they tend to be more strictly applied when a foreign entrant is pursuing a unique opportunity that few competing countries offer, in other words when the government has more bargaining power. Consulting engineers could also face

different levels of expectations and enforcement, but compliance with stated local content regulations, however flexible enforcement might be, demonstrates the company's willingness to support local development, thereby solidifying legitimate political support and host community acceptance. Whether through enforcement or voluntary compliance, local content can present some unique challenges that a company needs to consider in its own planning and approaches.

Meeting local hiring quotas can be difficult because of a lack of qualified labour. It might seem obvious that one premise of local content is that there a lack of skills and hence a need for learning. But in many developing countries, particularly in Africa, even functional literacy can be rare.

Larger companies whose operations have some economies of scale can afford to actually invest in local workforce education, but for small companies including a typical consulting engineering firm, this is probably unfeasible. Another problem for consulting engineers is that there is very little unskilled work to be done in their operations, hence meeting local hiring quotas with basic labour jobs is seldom an option. Even though a small operation might have low local labour quotas, unskilled people might have to be taken on board and integrated with a complex operation, and this requires considerable management attention.

In poorer countries, where a lack of qualified labour tends to be more acute, many people are desperate for sound employment prospects and this makes the hiring process itself very sensitive: the foreign company needs to balance a perception of fairness with a need for the right skills. Just hiring well educated workers could mean hiring from the current socio-political elite, who already have considerable advantages by comparison to most social segments. Whatever the skill levels available, local hiring also means compliance with local labour codes, and for a smaller company this can be an onerous new level of bureaucracy.

Local content also often applies to local suppliers, not just workers. Unlike a large construction or extractives operation, a consulting engineering project likely does not need much by way of supplies, but an operation might have been planned on the premise of subcontracting some project elements, and a proportion of these might need be sourced locally to comply with local content rules. Knowing this upfront, the company could try to plan which subcontracting elements are best aligned with skills available in the local market, thereby minimising the amount of coaching the company would have to do in order to get the right performance from local subcontractors. Given a potential lack of skills in local firms, a company should expect more need for coaching and oversight than they would expect in more developed markets.

As with labour hiring, the issue of fairness in supplier selection could arise. In many emerging markets the better local firms are likely to have strong political connections and could be regarded by the wider business community as already having unfair advantages. The foreign company might even face local political pressure to take on these connected players, in so doing helping political figures to gain favours within their patronage networks. This might seem expedient both to satisfy political expectations and to get more sophisticated suppliers on board, but while it is not quite the same as catering to nepotism, it could well be regarded as such by the wider host community. As with local labour, there is a trade off between a commitment to fairness and developmental impact, and expediency.

A final challenge with local content overall is that it increases the need for attention to security and anti-corruption assurance. In higher crime locations, local staff might need to be vetted to ensure that they are not actually agents of local crime groups or susceptible to criminal pressure to seek illicit use of company identity or assets, or to provide information that could facilitate theft or extortion. Both people hired into management positions and local sub-contractors need to be trained and monitored for anti-corruption compliance, since their comportment could directly affect the reputation and liability of the foreign company. In many developing countries, family, clan or tribal loyalties can be very strong, and outside pressure on local associates needs to be considered in both security and anti-corruption approaches.

The principal dilemma for a smaller consulting engineering company is how to manage the trade-off between getting the right local skills and a commitment to fairness. Quite often, being more fair and trying to support disadvantaged segments entails more management time and attention, and potentially even higher costs. An unequivocal commitment to fairness could give a consulting engineering firm a development remit on par with many NGOs, and this seems unreasonable and unrealistic for a commercial company.

Knowing the skills landscape and one's options and obligations upfront is half the battle. As well, the company can seek to understand how development commitment might affect project price perceptions among government and donor agency clients – while price is often the main consideration in developed markets, in developing countries desperate for commercial and technical skills and learning, price might not be such an overriding award factor. It is not feasible to provide a blanket suggestion in absence of a specific company or country, except to say that in cases where local content is applicable, early awareness and planning is essential to avoid complications later on. If local content and related challenges come as a surprise after the company has committed to a budget and schedule, it can become a serious drag on meeting these ill-informed targets.

Working with Construction Contractors

After handling a project design, consulting engineers could follow this phase by working directly with the construction firm handling the build phase, and perhaps this could even move onto programme management when an infrastructure project is financed on a public-private partnership (PPP) model and moves into an infrastructure operating phase. For purposes here we will limit the discussion to the construction phase.

The principal ways in which consulting engineers end up working with constructors is when the client engagement includes subsequent tendering, selection and management of the construction contractor, or if the client asks the consulting engineers to take on this remit as a new project after the design phase is complete. Sometimes this might not be full responsibility for contractor selection and oversight, rather a technical advisory role. Either way and especially when responsible for project management, there are some potential issues in the relationship with construction contractors in the context of governance challenges in emerging markets. Note that in the interests of bringing attention to some of the darker contingencies, what follows is premised on weaker contractor sustainability and integrity standards than European consulting engineers would normally face in working with contractors.

First, as noted earlier, it is important to the social credibility of the wider project that supplier selection be transparent and fair. However, international construction is one of the most notorious sectors when it comes to bribery in contract awards, and while Western European and other developed country firms might be more concerned about corruption liability, constructors from emerging market countries might have far fewer qualms about using bribery. There are a number of large players from China, Turkey, Russia, the Gulf states, and India, to name a few, with a widespread international presence but with tenuous anti-corruption standards, and indeed Chinese state-owned firms, which are particularly active in Africa, are often under pressure to get market access whatever the terms (and in many cases their contracts are tied into wider Chinese foreign relations in the region, often aimed at securing access to extractive and agricultural resources).

Thus, even when the consulting engineers design fair and clear supplier selection criteria and seek to apply a transparent selection process, they could find themselves up against considerable intrigue which undermines their efforts to achieve transparency. Relevant government authority customers in weakly governed states could well be susceptible to bribery pressure, and if a foreign constructor offers bribes, the consulting engineers' selection process might be undermined or entirely discarded in the interests of earning bribery payments or other illicit advantages. This likely sets a negative tone to the consulting engineers' relationship with the constructor and also risks a public perception of collusion in an illegitimate award decision.

Another problem that can arise is that the constructor might not share the consulting engineers' commitment to corollary sustainable development objectives. Bribes might lead to the relevant authority relaxing local content enforcement, for example, and indeed Chinese constructors in particular have a reputation for importing their own labour, in clear contravention of local content regulations but with host government acceptance (in the case of Chinese firms, bribes are not the only factor – the Chinese government often packages discounted infrastructure construction as part of wider cooperation agreements, but from a public perception standpoint it still looks like disregard for grass roots local development needs). The constructors might have scant environmental protections, or CSR to offset hardships caused by the project. They might indeed turn a blind eye to such hardships, including forced relocations and land acquisition carried out by an authoritarian government to clear land to expedite the project. Security for the project, whether provided by private (though usually regime-connected) firms or state security forces, can be heavy-handed and act in contravention of global ethical standards in security and human rights.

While this kind of behaviour has often led to serious problems for large emerging market constructors, there is often little culture or recognition of the value of socio-political risk management, and hence little explicit consideration of the long-term downsides of ignoring social and ethical considerations. Perhaps the best way of understanding the organisational attitudes of less socially conscientious large emerging market companies is to imagine the experience they have had in their own home countries. There, they are probably accustomed to a certain level of weak and authoritarian governance and official heavy-handedness in dealing with civil society, and they probably attained their status as large firms partly through illicit collusion with the regime as part of the extended patronage network. This is where many such firms are coming from, and this is how they expect things to work overseas too.

The obvious risk is that reputation and ethical liabilities are negatively affected by the illicit or unethical behaviour of the constructor, because of the consulting engineers' continued involvement in the construction phase and proximity to the construction firm. Consulting engineers could also become part of the wider target set of violent protests or other threatening local reactions. Given the huge discrepancy in size and numbers of people in the country between the consulting engineers and the constructor, it can be difficult to exercise much control, especially if the constructor has used bribes or other favours to gain regulatory leniency and back door relationships with key government authorities.

This seems like a very messy situation with limited remedial options, and that is indeed the case. Once in this kind of relationship, a consulting engineering firm with a concern for sustainability and reputation has few options but to leave. The best way to manage these issues is by doing so early on. If there are indications that a government customer is prone to bribery pressure and would look forward to the supplier with the best offer in this respect, then the

consulting engineers should initially only agree to the design phase or at the least leave room to opt out of any involvement in the construction phase, while emphasising the sustainability and social impact aspects of their own work in their final hand over.

If there seems to be an opportunity to continue, the consulting engineers' own contract for involvement in the construction phase needs to be carefully designed with explicit reference to good governance, transparency and sustainability, and ideally specific contingencies in which the consulting engineers could opt out of further engagement without penalties. Involvement in the construction phase should be contingent on the inclusion of binding ethical and sustainability safeguards and performance in the construction tender criteria and contract. Such safeguards can include building in compliance with global ethical frameworks (Engineers Against Poverty, Swisspeace and International Alert provide some guidance on relevant frameworks, as do transnational donors and the OECD) including the Voluntary Principles on Human Rights and Security. There also needs to be contractual stipulation for independent compliance training and monitoring. In some cases the consulting engineers might be able to lobby government actors who share their concerns about ethical and developmental impacts, and seek their participation in getting agreement to making such concerns explicit and enforceable.

If a government customer is hesitant to accept such terms or variants thereof, then it depends on the consulting engineering company to decide what this means for them, in the context of their own organisational culture, brand, and risk appetite. Some companies are at least initially comfortable with a more tenuous balancing act and promises as opposed to guarantees. Given the stakes, however, caution and a healthy dose of scepticism about other players' commitment to sustainability are usually warranted.

Again we can see the merits of working with emerging market governments through transnational lenders and donors. While they have an imperfect record, good governance and sustainable development are two of their primary concerns, and they carry a much bigger stick than the average consulting engineering company. As noted in the section on dealing with governments, it can be feasible to directly engage, but governance standards and sustainability commitment would need to be carefully assessed before the consulting engineers commit to long term involvement. There is a very tight link between construction phase concerns and social impact and public contention issues discussed earlier. Both, and especially when combined, represent high potential for what we call entanglement risk – the risk of getting stuck in a deteriorating situation in which the company spends more time fighting fires than doing its core job, and from which it is harder to leave the longer one remains engaged.

Security Concerns

All foreign companies, and indeed domestic ones, face special security concerns in unstable and weakly governed environments, especially where sectarian or ethnic tensions are prone to flaring up or where there is an ongoing insurgency. We hear most about the newsworthy issues, such as terrorist bombings, civil war and major unrest that seems to be a prelude to violent regime change. These are indeed worthy of attention, but most types of security problems for foreign firms do not make the evening news. Security is a complex function and concern, so for purposes here we only outline general types of security risks, and of the various assets to be protected we mainly focus on the most important one, especially for professional services firms such as consulting engineers: personnel. Note that some terminology is useful here: a risk is a potential harmful event or action (e.g. getting punched), while a threat is an actor who could cause harm (e.g. a boxer). We capitalise Security when it refers to the management function, while for general use it is lower case.

There are two basic types of security risk, inadvertent exposure to harmful activity that is not targeted action against the foreign company, and targeted threat behaviour. We will look at inadvertent exposure first. We have worked with clients, for example, who had been affected by ethnic rioting in the vicinity of their offices and residences, and in one case this even involved a mob attack on a staff member caught in the midst of a sudden conflagration. This was not targeted threat behaviour, just the serious outcome of being in the wrong place at the wrong time. On a less dire note, another client operating in North Africa was well aware that the area around the capitol's football stadium was a no-go zone on game nights, because post-match rowdiness often devolved into a form of political protest met by riot police – anyone caught in the area would have been dodging rocks and tear gas for a while. On a more macro-level, when a country is in a period of long-term instability, with regular anti-regime demonstrations and protests and security responses, foreign companies might have to regularly halt operations and have their staff "hibernate" for a while in order to avoid inadvertent exposure to violence. Periods of prolonged instability can also lead to routine security sweeps and crackdowns, and staff, especially local staff who are not obviously foreign citizens, risk being detained if caught up in a sweep.

A grey space between inadvertent exposure and targeted threats is being regarded as an opportunistic target because of being foreign (and therefore perhaps ignorant of the local landscape) and wealthy (as many foreign workers and companies are in the context of a developing country). In an environment of weak or corrupt policing and high crime levels, an expat can be a good target for a shakedown, scam, or mugging / carjacking just for these reasons (shakedowns, or harried searches and hassle accompanied by demands, can be carried out by corrupt police or criminals posing as police, the latter not uncommon in some African

countries). The target criteria of lucrative and easy to entrap are very general, and the typical foreigner fits these quite well in absence of any deterrents.

Targeted, or direct, threat behaviour is about who the company is and what it represents. We have already discussed one sub-type of targeted threat: Threats can be motivated by community anger at what the company's project represents, its potential social effects, or perceived negligence towards the host community (this can include union hostility). This type of issue has been covered, so we will leave this aside and focus on the other two forms of direct threat. One is motivated by ideological hostility to the company's political symbolism (e.g. Western, capitalist, secular, from an ex-colonial power, or seen as in collusion with an illegitimate regime). Terrorist and insurgent groups are the most likely ideological threats, and their behaviour can include attacks and kidnapping.

The other, and more common, direct threat is criminal predatory, wherein the perpetrators have investigated the foreign company and identified it as a potential target for kidnapping or extortion. In both of these sub-types, as noted earlier perpetrators can make use of local staff employed by the company, recruiting / infiltrating, pressuring or bribing them to provide intelligence on company assets and vulnerabilities. In weakly governed countries and where police are corrupt, criminal gangs in particular often cultivate police relationships to help in targeting and to inhibit police investigations of operations against the company. It is worth noting a particular variation of predatory threat: expat or local staff might be arrested or detained as leverage against a company to get them to acquiesce to changes in the bargain with the government, or to demonstrate a populist regime's unyielding stance in dealing with "exploitive" foreign firms. Even if the initial charges were valid, the judicial process can be purposefully fuzzy and manipulated to prolong detention and increase leverage. Often, the initial charges are themselves baseless; where the rule of law is weak, an accusation is enough.

A security threat assessment would be required to catch all relevant security risks in a specific country and operational context and the above are only indicative general types. We can share some nuance from past client discussions, however, to help put some depth to what has been a general discussion so far. Two security risks have been noted as particularly complex: kidnapping and the detention of local staff in security crackdowns. Kidnapping is an insidious process and clear-headed responses can be undermined by constant fear for the victim's wellbeing. Just going to the police might not be an option if they cannot be trusted. Foreign company managers are hopelessly naive against seasoned criminal or terrorist groups and paying a ransom is often no guarantee of safe release. Calling in expert kidnap response consultants is costly but it is usually the best option, and note that kidnap insurance usually includes access to specialist advisors in the event of a kidnapping. There are important nuances around kidnap response that warrant further investigation.

The other particularly disturbing risk noted is a local staff member being detained, or simply "disappeared", in a security crackdown during a period of instability or in a general slide towards authoritarian rule (this was discussed in the context of Algeria during the 1990s, and in a few other countries that are experiencing ongoing issues). Duty of care compliance might not apply to government action against a host country citizen, but managers have agonised over the fates of detained staff, especially in a context where security abuses are routine. Furthermore, to be seen to do nothing hurts trust with other local staff, who regard, usually incorrectly, the foreign company as somehow having some clout and influence to act on the detained person's behalf. Because such instances often fall through the gaps in security or corporate policy, managers have been left on their own to handle such incidents, and some have incurred significant personal risk to seek information on and the release of the detained person(s). The effect on overall morale is similar to a kidnapping case. Without a guiding policy that integrates relevant corporate resources and lobbying efforts / public relations pressure, there is in fact little that a company can do in most cases (although note that the US Magnitsky Act of 2012 was the result of successful company and personal lobbying after a case of local staff detention in Russia, though the staff member died in custody).

To summarise the implications of security issues, security risk can slow down an operation, it can actually hurt staff which is a tragedy in itself, it can incur duty of care liability (not discussed but obvious), it can degrade morale and hence performance, and it can also incur internal and external reputational damage when a company is seen as inept in handling its own security or ill informed about what should have been priority risks. The best example of companies enduring all of these in one manifested risk is probably the In Amenas gas plant attack in Algeria in 2013, when several foreign oil gas companies seemed hopelessly vulnerable in an environment where terrorism was already an acute risk.

Overseas security management is a well established practice on which public information is readily available and we will not go into each element here. Rather we will focus on a few less discussed but still important nuances that have arisen in security management in complex socio-political environments.

Threats as stakeholders: While security theory and practice applies a variant of stakeholder analysis to threat assessment (the "capability X intent to harm" framework), beyond the Security function threats are often not regarded as stakeholders, rather as dangerous aspects of the overall operating environment. Stakeholder analysis is usually assumed to be mapping legitimate actors' positions with an eye to gaining their acceptance for a project. Yet, a criminal, insurgent or terrorist group or manipulative state agency can indeed be a stakeholder, fitting the stakeholder definition of a group with an interest in and potential capability to affect the company. Treating threats as such recognises that they are intelligent, motivated actors with a specific agenda, rather than mere abstractions. It also suggests that communication with

such groups is possible, not via direct discussions towards gaining their acceptance, but with indirect messaging with an eye to deterring their behaviour. There seems to be a concern among international companies, motivated by a perceived need for constantly upbeat messaging, for emphasising potential positive relationships and downplaying hostile or negative ones. This public image concern often actually affects planning, creating blind spots in threat awareness and in the options to deal with threats.

Security, or Health and Safety (and Environment)? One outcome of the Statoil review after the 2013 In Amenas attack in Algeria was that Security and HSE should be distinct when it comes to threat behaviour, since HSE, even though it has a concern for staff wellbeing, focuses more on accidents and natural disasters than external threats and the political environment. Long before this finding security professionals had been making the case for a distinct organisational identity (instead of being tacked on as the extra "S" in HSSE). However, there is some overlap between the two, particularly in planning responses to potential crises or catastrophes that require evacuation or other large-scale action to support personnel. There are similar logistics in responding to a major political "meltdown" and a natural disaster or disease outbreak, for example. This suggests that there should be some joint planning and capacity between these functions, and indeed alignment and coordination in risk management planning should involve all relevant functions. But in an environment where there are significant predatory threats, Security needs its own space to address them, and should not encumbered by a functional side focus on internal accidents and workplace safety.

Security, Internal Control (anti-corruption) and CSR: Security as a wider objective depends on protection and deterrence against threats, but also on internal organisational integrity and on acceptance in the host community. Organisational integrity, specifically anti-corruption as assured by Internal Control, helps to maintain the company's credibility and hence its acceptability, and importantly, helps to reduce potential extortion risks that can come from corrupt relationships (the recipient of bribes might try to keep up payments by threatening scandal or escalate demands to physical threats). CSR has a sustainability remit, but importantly its role is also to reduce local hostility and increase acceptance of the foreign company as a fair and respectful actor. When these three functions work towards common objectives and coordinate approaches, the result is more robust and holistic overall security.

Unfortunately we have found that these three key functions, whether handled by specialist departments or as part of an operational manager's wider responsibilities, often do not coordinate, with consequent gaps and missed opportunities. A lack of coordination can be especially acute between the Security and CSR functions. Security can see CSR as naively exposing the company to complex local relationships, and CSR can see Security's measures as showing distrust towards the local community. We look at the wider question of political risk

management coordination later in this paper, but suffice to say here that when it comes to security in particular, the stakes are too high for functional silos and coordination between relevant functions is especially important.

Security and human rights: We will not belabour this important point, as it is quite widespread in security management and responsible business literature, but suffice to say that any Security function needs to be sensitive to human rights in the execution of its responsibilities. Companies should never feel pressured to accept a private security company recommended by a government official, and instead should ensure that any provider is professional, not overwhelmingly staffed by an ethnic, regional or sectarian group with a legacy of hostility or tensions with the host community, and open to human rights training and compliance monitoring (either directly adopting the Voluntary Principles on Security and Human Rights or a robust variant thereof). In some cases it will be necessary to use state police or military, but even then a company can insist on human rights frameworks and compliance. If the company does not have its own experienced international security manager on staff, it should consider hiring or contracting one from a respected international provider, because a security manager with experience in complex environments can have considerable influence over local security providers and police, and can ensure that human rights compliance is taken seriously. The classic case of security abuses derailing an operation is Talisman Oil in Sudan, 1998-2003, wherein the army units providing security also used company facilities as staging grounds for attacks on local villages – Talisman's reputation bottomed out, as did its share price. This was an extreme example of abuses affecting company credibility and liability, but the issue is regrettably common to varying degrees, and is invariably damaging to reputation and local acceptance.

Small Consulting Engineering Companies and Security Management

The above indicates that security in challenging socio-political environments is both an essential consideration and capability, and a potentially complex one. Perhaps ironically, security is often cheaper for larger scale operations: one Security office and relevant capabilities covering hundreds of personnel on an operation is likely a smaller proportion of operating budget than the necessary capabilities for a small operation. The team being protected might be smaller, but this does not diminish the need for a certain level of security capacity as indicated by the threat environment. Thus security can seem like an outsized burden for a small organisation, as many consulting engineering companies are. Additionally, consulting engineers are typically lean on support functions and most staff are technical experts and operational managers. Adding security responsibilities to a lean team can seem like a distraction.

The short answer to the dilemma of security need versus cost and distraction is that if a company does not want to have to worry about security capacity commensurate with moderate-high threat levels, then it can constrain its operations to less volatile places. Going to challenging places and not sufficiently investing in security is not an option – even if the staff are willing to take the risk, duty of care regulations can lead to serious liabilities if security gaps lead to harm, and reputation can similarly suffer. But there are some options that can be considered to maximise security cost effectiveness.

One would be to have a professional security manager on hand for guiding expertise (including the management of a security provider if required, and police liaison), but for the rest of the country team to be actively involved in supporting security management. If trained and aware, staff can support security through seeking inputs into ongoing threat monitoring in their day to day interactions and observations, contributing to crisis and contingency preparedness such as updating evacuation plans and maintaining evacuation logistics and documentation, participating in crisis response planning and simulation sessions, and of course they can better comport themselves in line with routine threat avoidance and security protocol. This might sound obvious, but large organisations, for example in oil and construction, often leave nearly all security tasks to the Security function, which marshals and protects the herd using considerable resources while the herd gets on with their own business with scant consideration of security. The additional benefit of more staff engagement and support for security is that staff are much more aware of their own security and better at keeping themselves safe.

Sharing or piggy-backing on another's security capacity is also an option. If working with or through transnational donors, then they often take on at least part of the security requirement, and the consulting engineers can work with the donor Security function to ensure that their own unique needs and exposures are considered in security planning. Similarly, if in the construction phase the contractor is a trustworthy company with an eye to sustainability (and hence human rights and security) it is possible to piggy-back off their security and to play a role in shaping overall project or country security policy.

Finally, there could be other organisations in the area with similar security needs, and pooling resources and threat awareness can help reduce costs overall. Such organisations could include diplomatic stations from one's home country or other European governments, who might be willing to extend or share some security resources, at the very least threat intelligence. They could also include other companies, and even international NGOs operating in the same vicinity.

There are options, then, to maximise security cost effectiveness and hence reduce the burden this capacity represents, if not on management attention then at least on budget. But this is no argument for skimping, and overreliance on others for one's own duty of care requirements can lead to grief when such capabilities are needed most. In the chaos of an evacuation scenario, for example, if something goes wrong with planned transport capacity (like one of two planes breaking down), the organisation paying for the transport assets will reasonably put its own people first. And sharing security capacity with a construction company that does not have a commitment to human rights and security should be avoided. One final point: while it might seem expensive, if operating in a place where kidnapping is even a moderate risk, kidnap insurance is very worthy of consideration. Advisory support often comes with kidnap insurance, and such support is far more expensive if acquired without the insurance policy and takes longer to organise in the event of a crisis. There are some unique considerations in kidnap insurance which are beyond the scope of this paper, but we suggest that this coverage be investigated and that readers learn the options.

Political Risk Management in Smaller Consulting Engineering Companies

This final section turns to the question that naturally follows from a discussion of the potential issues: what to do about political risk? We have already indicated some specific options in the context of the challenges that consulting engineers could encounter in emerging markets. Here, we look not at the various sub-approaches, which in any case are contingent on where and what an operation is, rather at the wider question of how a small but internationally active company could establish a political risk management capability that can then be applied to a range of different country operations.

This is a challenge for smaller outfits. Larger companies have the scale that makes it feasible to afford specialist departments, such as Security, CSR / Sustainability, Internal Control / Compliance, Legal, Government Affairs, and in a few cases even integrated "Political Risk Departments", to take on much political risk management and thereby let operational managers focus more on their core jobs. Specialist departments are not really an option for the average European consulting engineering company, which is probably small and with few corporate services assets. And emulating bigger companies in establishing specialist departments still does not address a major problem that many such companies still have: how to coordinate and integrate these functions around shared objectives, rather than a range of specialist silos patching together disparate political risk management approaches that might be redundant or working at cross purposes.

The approach, in terms of structure, process and internal positioning, would vary depending on organisational size, culture, and typical overseas exposures, so what follows is only a top-level suggestion that will hopefully provide a baseline for extrapolation to one's own company context. These points keep in mind that dedicated corporate assets will be slim to none, but that much relevant capability probably resides within the core operational and management team.

Shared Concept of Political Risk

One important point for any international company, big or small, is to have a clear concept of political risk in their context. Political risk, by whatever label (for example in extractives it is often just known as "above ground risk"), is a unique domain, describing issues within a tightly linked system driven by power politics, ideological contention, socio-political values, and sub-national cultural identities. It is related to but distinct from commercial risk, for example, which is more about market and competitor dynamics within a rules-based business arena. In politics the rules can be obscure or changeable. Because of the networked and systemic characteristics of socio-political environments, it is seldom possible, or at least not a good idea, to treat different issues discretely, in absence of a consideration of effects on other issues (the example of CSR and Security misaligning comes to mind here – the ultimate logic of each could wreck the other's initiatives).

A shared concept of political risk helps different functions and people to align around a common and holistic mental model of the type of system they are each dealing with. Without a clear concept, people will likely undertake political risk management in some form or another, but without a bigger picture that allows them to see when coordination and information sharing is beneficial or indeed essential. Furthermore, because political risk is not a traditional or conventional management function or practice, without a clear and communicated conceptual definition, it is likely to fall through the cracks or off the corporate "radar", making the company more vulnerable to its effects.

Conceptual definition and communication is certainly not costly nor particularly time consuming, yet it is perhaps the single biggest factor in political risk management capability – it is the basis for joined up awareness, the defined subject area for learning, and the basis for holistic approaches that overcome a tendency for ad hoc and reactive responses.

Clear Red Lines / Risk Appetite

An extension of the concept is what risk means to the organisation. Taken in the more conventional sense of a bad thing happening, what is bad for the company? There are the generic "bads" that every organisation has, for example financial loss, personnel harm, reputational denigration, and sub-factors thereof. But there are also negative contingencies that

are specific to the company's organisational culture and values, wider stakeholder expectations, operating model and typical exposures. A large construction company with diverse operations, for example, would not want to get negative press on any lapses in its ethical performance, but given the size and spread of the organisation, a bad reputation in one corner might not be a huge concern for the company and it might be an acceptable risk if the reward is big enough. A small consulting engineering company that relies heavily on credibility and acceptance to punch above its weight in a competitive market might see damage to social and ethical reputation as a critical problem. Then what kinds of situations are likely to lead to this problem? As examined earlier, working with a construction company with scant regard for sustainability concerns might well be one of them. So this is flagged as a red line. Similarly, if a company can ill afford non-payment in even one project, then engaging directly with an emerging market government with a track record for contract manipulation would be another red line.

A short list of the types of situations that could incur damage at or beyond the red line can be formulated, and this then provides at least initial guidance on what to look out for when seeking work or considering specific growth opportunities. It also helps in early "go / no go" decisions that then save the cost of investigating and potentially tendering for a project that, as one might eventually learn, is ultimately too risky to bother with – one can simply avoid entanglement if one knows what to look for, and put the same resources into looking for better prospects.

Most risk appetite and red line definitions in political risk, even for larger firms, tend to be more like rules of thumb than stated criteria of a decision to forego an opportunity, for example we have heard some say, "If there is going to be corruption pressure for every little thing, we won't bother – it is too tedious and stressful, and someone might crack and incur liability". Another said, "After that experience, we avoid places where there is regular ethnic conflict – it makes it hard to avoid being seen as taking sides, and it makes hiring and CSR a political minefield." Rules of thumb actually work, but quite often these rough and ready limits reside in the minds of specific people and are not formulated as company-wide guidance, so when they leave their positions, their experience-based notions might leave with them. A more systematic and inclusive process of defining political risk appetite and then communication as corporate guidance can lead to more consistent and widely applied standards. It is also important that these are periodically reviewed, as the company context and its operating environments can shift over time.

Formulating red lines and risk appetite takes more work than a concept statement, but as it draws on experience and attitudes from within the company and its immediate stakeholders, it is again a reasonably cost effective way to get people on the same page in terms of political

risk, and to introduce some of the key issues that they need to be aware of as they investigate overseas opportunities.

Intelligence and Planning Process

While a specific country operation might have its own unique exposures and issues, the company's corporate centre can develop an intelligence and planning process that offers a ready approach applicable to a variety of contexts, saving managers from reinventing the wheel each time, and which helps keep the process consistent to ensure that sound practice is applied across the board. Consistency in formats and terminology also helps for institutional learning, as consistent outputs can be readily compared to increase awareness of the wider set of issues the company could encounter. Political risk intelligence and planning would need its own paper to cover in detail. We look here at some options to help make the process manageable for smaller organisations who cannot offload the process to specialist support functions. We deal with intelligence first, then translation to planning.

Intelligence

An intelligence process for a smaller organisation needs to focused and concise. There is a tendency in political risk intelligence projects and reports to take a rather "paint by numbers" approach that seeks to detail every possible risk and stakeholder, yielding heavy outputs that can be very hard to translate into focused risk and stakeholder management initiatives. Part of the reason for weighty outputs is that they are commissioned by large companies and will serve several different departments, thus someone can find what they need in the larger mass of material. Another seems to stem from a certain degree of "cover your a - -" whereby the relevant management team is concerned about appearing to be very comprehensive in detailing the risks even if much of the information is too irrelevant or trivial to be useful, and this comes as much from a concern with perceived due diligence compliance as from a real need for tangible planning inputs.

A risk-centric or "point by point" approach also often fails to reflect the interconnected reality of political risk. A risk is a potential bad thing happening, and quite often conventional intelligence outputs yield a huge array of risks that actually stem from a handful of more holistic potential situations. For example, a coup leads to regime change, street violence, sanctions, repression, etcetera, each of which in turn leads to certain effects on the operation. Rather than dealing with the whole situation of a coup, a report will detail all of the potential effects as risks, often redundantly referring back to the coup as a risk driver. A small company trying to plan around the resulting dozens of risks faces a serious headache, and in effect needs to reverse-engineer the outputs to see what potential situations can be coherently managed.

The first suggestion for concise and focused, then, is not to focus on point by point risks, but rather to take a less "risk speak" and more common sense approach and look at potential situations. Looking at the intersection of the operation's exposures and profile, socio-political dynamics, and socio-political stakeholders, and on the basis of our current risk management plans, what situations could arise that we do not want to be in? Which of these are most serious (which are most plausible and would hurt the most)? This easily slides into the planning phase: how can we avoid, or prevent, this situation or mitigate its effects if it does manifest? Thus we derive a far more limited set of situations, or in effect mini-scenarios, each with its own causal plot lines, plausibility, effects, and importantly also indicators to help foresee them, and we are better informed on fewer, more relevant potential issues.

Stakeholder analysis should be part of the intelligence process, and hence the focus is really not just about risk. Negative stakeholder attitudes and potential responses are taken into account in formulating situations we want to avoid (including the lapse of an otherwise beneficial stakeholder relationship), but the positive, supportive stakeholder positions indicate opportunities for mutual engagement, and even wary stakeholder positions indicate where we can work on gaining trust or reducing negative sentiment.

Going to back to the notion of concise and focused, again, we have seen stakeholder assessments that have yielded an encyclopaedia of the socio-political landscape, and to make matters worse, some companies stick to certain analytical frameworks that have five or six redundant or overlapping assessment criteria. The results might satisfy some notion of "doing one's homework" but they are too dense and contain too much trivia to be the basis for engagement planning. Assessment should identify stakeholders starting in direct proximity to the company, then move outward only until the "stake" is too tenuous to matter. Then it should stop. After that, linkages between actors can be considered, and actors or groups which are likely to coordinate and respond in the same way can be aggregated for an even more concise set. The main criteria that matter are attitude towards the operation and capability to influence it. Other considerations are explored in planning engagement or messaging approaches, but are not assessment criteria, and will vary by actor.

In deriving the risk and stakeholder assessments, an intelligence process will probably come up with considerable nuance, and this should be captured, but not in long reports, rather in note-form in appendices for "background / interesting but not relevant" material. Outputs used for planning should be articulated in concise and user-friendly reports and briefings that are tailored to feed into the planning process. This might sound obvious, but if this notion were applied in the political risk intelligence sector it would represent a revolution. Part of the problem is user or client-side, as explained earlier. Another is that political risk analysis is still very academic, and unlike in strategy consulting for example, country experts often do not

know how companies really use the information, and can get carried away with their own interest in the subject matter at the expense of providing interpretable findings.

Many companies outsource political risk intelligence, even for specific overseas projects, to external country risk intelligence providers. It makes sense to use external experts for baseline inputs, because a good political risk intelligence provider will have close links with unique country and regional sources, as well as staff who have been studying a certain country or region for years. But there are good reasons to retain and own the process and its ultimate outputs inside the organisation.

First, good external reports might be long on information, but external analysts cannot really be expected to know exactly how the information will be applied, or the organisational culture of the end user company. It is possible to guide external providers with clear and specific briefs, but some degree of adaptation to organisational process and readership is likely still going be needed before this intelligence can translate into plans.

Second, the company will have its own unique sources that it can draw upon for political risk intelligence. If there is an SIA, for example, while that is likely to be very technical, detailed and templated, and not positioned as political risk intelligence, there is often considerable information in SIAs, especially on the stakeholder side, relevant to political risk intelligence. If the company is doing or involved with a stakeholder assessment project, it should be coordinated with, and ideally integrated with, the political risk intelligence exercise, and a robust stakeholder assessment is pure gold to any intelligence assessment (it is much harder to get stakeholder insight than information on country or even location-level trends and dynamics). Finally, experienced company managers can draw on their own similar or parallel experiences for relevant insight, and also on their wider networks of ex-colleagues, professional associations, and government contacts for valuable insights.

In this vein, by way of illustration, years ago when the author was working with a larger political risk company, a case arose where an international company asked for a political risk report for an ongoing operation in an African country that potentially faced disruption because the president was frail and his most likely successors might have had very different attitudes to foreign direct investment. After a healthy dose of desk research including source interviews, and rendering a draft report, the client came back to us and said, to paraphrase, “What about the indications that the son everyone thinks has the best chance to take over is known to be irrational, violent and potentially a psychopath?” The client manager leading the request had been in-country for two years and had kept up with the local news and rumours.

We had known about the possibility of the son taking power if the president died, and that the son was a bit of a rogue, but we had not known that the son was widely perceived as a tyrant-

in-waiting. Having been on the ground for a while, the client was far better positioned than us for local insight. In the end the balance between our more comprehensive and objective assessment, and the client's experience-based insights, yielded robust planning insight. Had the client not had external insight, they might have gone purely on the rumour mill around this one high profile question mark, while left to its own devices the intelligence provider would have covered much ground at scan-level and would not have explored a critical concern.

This leads to another reason to own and control the process in-house – the company might have unique concerns that general reporting does not satisfy. External providers might not have a full understanding of what most worries the organisation, or what question marks exist among the management team responsible for a country project. If external providers are not given a very clear brief which, in addition to general insight, also calls for a focus on these concerns, then they tend to cover an array of potential issues at scan-level. Reports might contain insight relevant to these concerns, but alongside much else that obscures insight on the most pressing questions.

We have seen this on several occasions, and we again draw on past experience for illustration. In one project, that involved field work and time at the company's country office, the brief was very comprehensive and we covered much ground. But by spending time with country managers and staff, we came to understand certain pressing issues. The final report captured the full requirement, but we did a mini-report on these specific issues, and this little side-line report proved to be the most valuable part of the project and indeed could have been the central focus if we had known these concerns in advance. The full piece was instructive but much of it was rather academic by comparison to that small but very client-centric section.

To further illustrate the problem of lack of focus on pressing concerns, we go back to the example of the 2013 In Amenas gas plant attack in Algeria. Statoil's publicly available post mortem indicated that there was a stream of risk intelligence coming in from several external providers, but the company was overwhelmed by the volume of reporting and did not seek to cross-reference reports to draw out the most relevant issues, and while terrorism was top of everyone's mind, Statoil did not specifically ask about the likelihood of a terrorist attack or how it might occur – it had assumed that if there were such a contingency, then the "experts" would have flagged it. Indeed the possibility was there if one triangulated from all the incoming reports, but no one did, and the external providers only covered the question as one among many others, drawing no special attention to it. External providers should be clearly briefed to cover key concerns in addition to adding new insight, but ultimately it is up to the company to make sense of the outputs in its own unique context. And Statoil's case provides another useful lesson: more and more information does not necessarily make us better informed.

Finally, while a good political risk intelligence provider will likely have some side-line understanding of overseas business operations, relevant laws, ethical standards, and CSR and security best practice, they are country experts, not operational or functional experts, and company personnel with experience operating in challenging environments are often better positioned to interpret this insight with an eye to how identified issues can be sorted into functional tasks and managed in practice. It is of course possible to ask a CSR, legal or security consultancy, for example, to provide intelligence, but in so doing one gets a narrow functional perspective. It is likely better to get the goods from broad-thinking country experts and then handle the operational interpretation in-house.

If the company has the capacity in-house to conduct the intelligence exercise entirely on its own, fine, though even then it needs to be wary that its staff are not just telling gung ho senior managers what they want to hear or falling into other analytical traps. But in most cases, especially in smaller companies, it is more cost effective to draw on some dedicated external expertise since this is premised on years of specialised learning that can be used on an as-needed basis. But to summarise the intelligence portion of this section, ultimately the intelligence process, and resulting planning inputs, should be handled in house. Only the company can know how it really feels about risk and what its main concerns are, and it knows its own internal processes and organisational culture better than any external supplier.

8-Step Intelligence Process (Eight Gates to Wisdom...)

- Company context: Aims, exposures and key performance factors, profile, timelines, locations
- Country and location context: Socio-political character and recent evolution
- Socio-political environment, potential sources of issues: Weak governance, instability, conflict...
- Socio-political stakeholders (including relevant non-political actors): Who matters most, risks they represent, opportunities for beneficial engagement
- Situations we do not want to be in: Intersection of company context with socio-political environment and stakeholders – to be avoided, prevented, mitigated if they happened
- Priority situations: Most plausible, most damaging if left unchecked
- Priority stakeholder engagement opportunities: Aim / purpose, our bargaining position, ingress points / access, messaging and protocol, potential for support in risk mitigation
- What if: Red-teaming / devil's advocacy to test outputs and assumptions

Before moving on we draw attention to the "what if" point above. Statoil and its partners had assumed that the Algerian military was providing its security in In Amenas. In fact it took a

while for the army to get there when the attack happened, and when they did, they did not see it as a rescue operation, rather as a unique opportunity to kill this gaggle of insurgents who were usually not in one place together. The army killed more workers than the terrorists did in the shoot up that ensued, including helicopter gunships shooting at trucks with no concern for who was in them. A basic "what if" would have been, "What if we are attacked? How responsive would our designated security providers be, and how would they respond?" (this is also a stakeholder question). There was plenty of track record to draw upon to suggest that what happened was a serious possibility, but the question was never asked, or never made it upstairs (Statoil has taken a beating, but they were generous enough to publish their findings as lessons for others). The "what if" step is very important and should be brutally honest, and if it shakes up assumptions or changes the hypotheses, then it should loop back to the beginning and adjust the scope of the intelligence exercise.

Planning

The intelligence process has yielded priority situations and stakeholders. First, what initiatives or actions derive from this, and who does what? Second, how do we coordinate and oversee? Third, how do we track and adjust?

To address the first question: Intelligence yields priorities. These might include, for example:

- Government contract manipulation and seeking unfair terms after we commence work
- Pressure to pay bribes for regulatory approvals
- Pressure to use regime-connected local sub-contractors
- Host community hostility because of negative expectations about the wider project
- Negative state media portrayal as part of the regime effort to change the terms
- Criminal or terrorist kidnapping
- Violent unrest in the project or staff residence vicinity
- Coup d'état leading to widespread unrest and repression

How can these be parsed into manageable sets? Perhaps:

- Contract assurance: covers contract manipulation risk
- Integrity assurance: covers bribery and nepotism pressure
- Community and public relations: covers host community perceptions and media risk
- Security: covers kidnapping, violent unrest, and evacuation planning in event of a coup

Then we look at priority stakeholders, for example:

- Contracting ministry (e.g. transport)
- Regulatory authorities
- Host community and traditional authorities
- Local media
- Environmental NGOs
- Police and gendarmerie
- Regional terrorist group X and its local offshoots
- Organised criminal gangs

We integrate stakeholder engagement and management with the above manageable sets (and perhaps adjust those if need be for coherent programme definition), e.g.

- Contract assurance: Ministry of Transport
- Integrity assurance: Regulatory authorities
- Community and public relations: Host community / traditional authorities, local media, environmental NGOs
- Security: Police and gendarmerie, terrorist groups, criminal gangs

Thus we have four integrated programmes from eight potential issues and eight stakeholder groups. This is somewhat simplified and it could be more messy in practice, but if risk and stakeholder management programmes are directly devised from the intelligence outputs, we will be covering the priorities. Programmes that are too broadly defined lose focus, and too narrow a definition risks overlaps and redundancies. Getting the balance right, and assigning similar issues and stakeholders to the best person to handle them, might take some finessing, but in the end should approach what strategy consultants call MECE ("me see") – mutually exclusive, collectively exhaustive.

The right person? In larger companies it can be quite easy to align programmes and functions, because there are a range of corporate services departments, so for the above four programmes, for example, it could be:

- Contract assurance: Legal
- Integrity assurance: Internal Control
- Community and public relations: External Affairs or CSR
- Security: Security or HSSE

However, in smaller companies that do not have specialist support departments, the project or country manager will have to take the lead in recruiting the best people to handle a given programme, based on their experience, interest and country knowledge. An engineer might

need to double as the legal scout, or a surveyor as the community relations lead, and this could also mean leading on relationships with relevant external specialists (e.g. lawyers). These roles need to be taken seriously, because they contribute, in very concrete terms, to the sustainability and success of the operation. It is possible of course to recruit people to help with these initiatives, and it can be especially useful having trusted local people on board because they intimately know the socio-political landscape. How much resource one allocates depends on how pressing or serious the issues are. We look at some options for external support later.

A programme can be structured as:

- Objectives
- Routine prevention / avoidance approaches
- Contingency / crisis mitigation preparedness
- Approach to key liaisons and stakeholder relationships
- Performance indicators

We move onto the second question, how can we ensure coordination and oversight? One way is to have programme leaders involved as team members in others' programmes. For example, contract assurance and integrity assurance might have some crossover and can usefully coordinate. Community relations and security will need to coordinate to ensure that security is effective while not causing offense or being too obtrusive. Thus we can envision a matrix structure:

	Contract assurance	Integrity assurance	Community and media relations	Security
Contract assurance	Responsible	Supporting	Consulted / informed	Consulted / informed
Integrity assurance	Supporting	Responsible	Consulted / informed	Consulted / informed
Community and media relations	Consulted / informed	Consulted / informed	Responsible	Supporting
Security	Consulted / informed	Consulted / informed	Supporting	Responsible

This cross-involvement provides explicit coherence to the overall political risk management initiative, and prevents gaps and overlaps. On this note we once had a case in which we discovered that External Affairs and Security were buying the same intelligence reports from the same provider, paying twice, and they only learned about this because we asked each

function what external information they were using. If they were reading the same reports, they had similar interests and concerns, yet barely coordinated more than saying hello in the corridor. This is a mild example of the potential negative effects of a lack of coordination. Going back to the Talisman Sudan case, the CSR team was frantically trying to achieve a beneficial fit with the host community, while Security was coordinating with an oppressive army presence and HQ saw the problem as an abstraction and just wanted to keep the revenues flowing.

Oversight and coordination is also supported by a leadership and task force structure. The country or project manager is the political risk management leader (even in large companies this should be the case – offloading to a subordinate function risks the wider political risk management initiative losing authority and visibility). He or she leads the political risk management task force, comprised of programme leaders. The task force should regularly meet and exchange progress reports, share new insights, and ensure that everyone is fully aware of all issues that could affect the operation. It can also have an intranet portal or shared drive to store planning documentation and intelligence reports so others can access these in support of their own planning and inter-programme alignment.

Corporate headquarters will need to stay abreast of country and project political risk management, and indeed the intelligence and planning process derives from corporate practices. The regional director or practice director relevant to the project should act as the corporate support hub, and be ready to marshal company resources if necessary to support county contingencies. If HQ is acquiring relevant intelligence reports for other purposes, these should also be shared. We discuss a corporate political risk practice hub later, and this is another key liaison between country task forces and HQ.

Moving onto tracking and adjustment, programme leaders should maintain incident reports detailing manifestations of socio-political issues or related problems in their remit, and these can be aggregated to see where more attention or adjustments are required or where resources could be shifted. If, for example, corruption pressure is actually much lighter than expected, but community relations are more awkward than anticipated, then integrity assurance resources (the programme leader at least) can shift to helping the community relations programme.

Company exposure and profile could shift with different project phases, and this could lead to a new risk profile and new stakeholders. Similarly, the socio-political environment, especially in more volatile places, is likely to evolve during the course of a project. A monitoring programme should be established to keep track of changes in both company exposure and the operating environment, and when major changes happen, it could be worth doing another holistic socio-political intelligence exercise, rather than keep adjusting a programme structure

and focus that could be increasingly outdated. Monitoring could be done by each programme leader in their area of responsibility, but a country risk monitor subscription can augment ground-level insight with a more top-level perspective.

The intelligence and planning process is the nuts and bolts of political risk management, and leads to tangible initiatives on the ground. The process described above is only indicative and again is aimed at smaller organisations who likely do not have specialist corporate departments, though it is also applicable to large companies in some respects.

One question that should be addressed here is whether or not political risk should be handled separately, as suggested above, or integrated within a wider risk management process, such as enterprise or project risk management (ERM / PRM). The answer is nuanced. If initial assessment indicates that socio-political risk overall is low to moderate, it could be incorporated into a wider risk process. But if the terrain is quite volatile and the project has significant exposures, then political risk management should be an explicit and separate activity. ERM is still somewhat compliance-centric, and ERM and even PRM risk registries can be very lengthy and cram together myriad different types of issues. Political risk management is less about point by point risk management, and more about managing the company's fit with its socio-political context. Its mission can be obscured if it is treated alongside more routine issues, and this leads to increased vulnerability when operating in complex environments.

External Support

Political risk management should be owned in-house, but as discussed in the context of external intelligence providers, there is an opportunity to source external support when specialist expertise is required. Country and political risk intelligence providers are one resource, and those positioned more as consultancies rather than research publishers can also handle customised requirements if given the proper guidance. There are an array of consultancies in security, CSR and public affairs that can help on specific issues, and corporate investigations companies can be useful in supporting the integrity assurance / internal control function. Some law firms are specialised in international business and certain sectors and regions, and trusted local law firms will know the local landscape very well. If the company has kidnap insurance, the insurer's retained kidnap response consultancy can be called upon for guidance in kidnap and extortion prevention, and are likely knowledgeable about other aspects of security. External support does cost, but it can be cost-effective if is well briefed and targeted.

A company would also have access to its home country diplomatic station and perhaps other European embassies when overseas, and diplomats often share insights and advice, and of course can provide some support in the event of a crisis.

For ethical compliance design and monitoring, for example in implementation of the Voluntary Principles on Security and Human rights, NGOs often provide corporate guidance and can form part of an independent review committee.

In the section on security, we noted that this is an especially sensitive type of external support. We will not repeat the caveats here, suffice to say that any provider should be carefully vetted, and if it needs to be the police or military, then they should be carefully guided and monitored to avoid reputational liabilities associated with human rights abuses.

Political Risk Management Practice Hub

One might be wondering at this point, "all this is fine, but who does it, where do we find it?" Indeed someone needs to own political risk management, and lead a practice hub or knowledge centre that provides guidance to the rest of the company. The practice leader should be senior enough to have corporate visibility and indeed represent the practice at executive committee level. But they can recruit help from around the company, perhaps with a representative from each operational department and one from corporate services. Together, then can establish and communicate good practice guidelines, set intelligence and planning processes for country and project task forces, maintain an information and intelligence portal, and act as the internal consultancy and as an important corporate liaison for country teams. They can also act as the central purchaser of risk intelligence and related external support (including insurance), thereby ensuring that costs are not duplicated and that all relevant units have access to make the most of expenditures. And importantly they can brief and train other departments and business units in project and country level political risk management.

The person and team responsible would ideally have considerable international and emerging market experience, but they will need to learn more about political risk management in order to frame the concept and develop explicit practices appropriate for the company. This might sound onerous at first, but this is not the same as having as a full time political risk department. The practice leader and team members would spend most of their time on their core operational jobs, but together over the course of a year, if the team were four people for example, and spending only 10 percent of their time on the practice, this still represents about 100 person-days of development.

One important task of the practice hub leader would be to create and update a political risk guidance paper, outlining the concept, red lines and risk appetite, the types of issues to be aware of, the country / project intelligence and planning process, and general approaches to

political risk and stakeholder management to provide baseline ideas for country task force teams. This document should be in the practice portal and relevant staff should be urged to become familiar with it. If it would help to call it a policy, in terms of getting people to read it, so be it.

The above suggestions are indicative and would need to be tailored to the organisational context, but this section hopefully suggests that political risk management is well within the capabilities of smaller organisations, and need not be onerous or a new overhead. Indeed, it is part and parcel of people's regular jobs – they might be engineers or technical or business managers, but when they operate in complex terrain they naturally seek to minimise impediments to a successful operation, and political risk management is, in this sense, a core function, not an exotic add-on.

Conclusion

We have outlined some of the challenges a consulting engineering company could face in emerging markets, what some options are in dealing with those challenges, and how a company might develop or enhance their in-house capability to assess and manage political risk. We reiterate that this was based on a preliminary understanding of the consulting engineering sector, and readers will likely be mentally adjusting the material to better suit sector and company-specific nuances.

Working in emerging markets is challenging, and as political risk consultants our inherent focus is on the downsides. But with prior awareness and sound planning, most places are accessible and workable. Political risk management is not about being sceptical or paranoid, rather it is about enabling opportunities in even challenging environments. With an ability to assess and manage the issues, a company can confidently extend its reach. Conversely, a company can also know when a given opportunity is not worth the hassle so it can focus its energy in more productive directions.