hazardex

the journal for hazardous area environments

hazardexonthenet.net

September 2014

Unexploded Ordnance:
Managing the offshore UXO threat

Risk management:
The role of intelligence in the energy sector

Ageing plant:
RAM analysis

Hazardex:
Regional events 2014/15

Communications:
The secure lone worker

The role of intelligence in the energy industry

Evaluating risks and threats within business enables companies to identify opportunities and incentives, says Martyn Denton, Managing Director of industry intelligence specialist QRO Global.

The energy industry is continually expanding into new markets and little known regions, offering an ever-increasing range of exciting opportunities and rewards. Inevitably, given the locations and materials that the industry trades in, these opportunities are also accompanied by a significant element of risk, making good commercial intelligence critical, particularly when dealing with the uncertainties of the post 9/11 era.

Intelligence is a concept traditionally associated by many with military operations or covert government activities. However, it also has a vital role to play in identifying and developing global energy markets, as well as driving business operations and answering key questions.

Successful intelligence in the energy industry needs to place the specialist at the heart of its operations to influence how business is done, to manage risk in an efficient and effective way and to ensure that board-level decisions on operations are well-informed.

Intelligence has a purpose

The primary aim of intelligence work is to make sense of large quantities of uncertain, often conflicting, information that is collected and analysed for the purpose of achieving the company's objectives. The intelligence specialist should deliver a detailed insight into the operating environment, whilst presenting issues in perspective with an "over the horizon" view of operations. Part of that process is managing organisational, cultural and personal biases, and gearing the intelligence flow towards driving the decision-making process.

We are all too familiar with the concepts of risk and threat. However, the flip sides of risk and threat are opportunities and incentives. Which competitors are succeeding and why? How can we drive the business forward? Can we match the aspirations of the key decision-makers? Where is the most advantageous operating environment? Can limited risk be managed so as to gain from the many opportunities? These are the sort of questions that will be routinely addressed by the intelligence specialist in an energy company. Effective, intelligence-led business operations will incorporate the management of risk, threat, security and much more besides.

Defining the concept

One of the first barriers to overcome is terminology: 'risk', 'threat' and 'security' are often misunderstood concepts and may be used interchangeably. For example, in many businesses, the primary focus of the security department is to keep unwanted people out and to stop assets going walkabout. There may be a lack of representation at board level for the security department and they may even be viewed as a parallel function of

health and safety. Many boardrooms view the security department as a necessary evil; often the bearer of bad tidings, putting barriers in the way of bright ideas and adding further expense to already costly programmes. Ultimately, security as a function is often perceived as reactive and defensive when it should be dynamic and proactive.

Threat is often a generic term used by the security department to describe anyone or anything trying to breach their defences, whereas risk is the main point of focus for the boardroom: What is the risk exposure? What are the costs involved? How is the risk going to change? In what order do we need to address the risks?

I would like to challenge some of these views and suggest a more joined up approach to information management. I would argue that whilst identifying threats in an operating environment, it is likely that you should also identify commercial incentives. Likewise, opportunities will become apparent during the risk assessment process. Intelligence, a concept frequently ignored in business, should incorporate all of the requirements of risk, security and threat operations. At the same time, it should provide a means of furthering a company's objectives by evaluating viability in the face of changing operating criteria, potential profitability of investment decisions and examining past trends alongside current performance to predict the future.

However, when there are failures in business, headlines are often made for all the wrong reasons. Usually described as security shortcomings, in reality they are frequently the result of a failure to fully understand the operating environment.

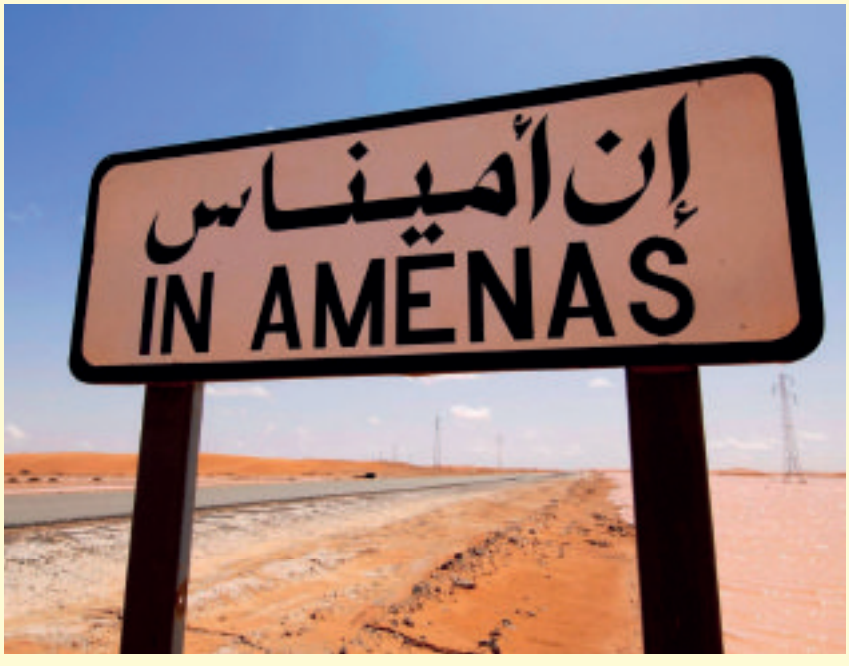
Case study 1 - In Amenas, Algeria

In January 2013, there was an Islamist terrorist attack on the petroleum facility at In Amenas in Algeria near the Libyan border. The 4th largest supplier of gas to the EU, Algerian exports have declined since 2005 due to infrastructure issues. Operated jointly by the Algerian state oil company Sonatrach, BP and the Norwegian company Statoil, over 800 people were taken hostage at the site, 40 of whom died in the Algerian-led military rescue assault. The Statoil report on the incident, released in September 2013, contains some significant observations on security and the role it played in the tragedy.

Statoil was criticised for failing to take a "holistic approach to the organisation and management of security." The report found that "security is not established as a corporate function independent of safety, recognised for its distinct characteristics and requirements. In most cases security is a small part of broader health, safety and environment positions, and one for which few people in those roles have particular experience and expertise."

Statoil's management was criticised for failing to understand the importance of security and making it a priority. The report recommended that Statoil strive to develop a "strong and coherent security culture in the company…. it must be an intrinsic and embedded part of the company's core activities." The report also recommended that the company "improve its ability to detect, delay and stop potential attacks by reinforcing electronic and physical protective measures, enhancing its security risk management capability and developing a coherent programme of security training and exercising, whilst broadening and deepening co-operation with relevant government agencies and organisations."

Whilst the report demonstrates that Statoil has identified areas for improvement as a result of the tragedy, including the separation of the security function away from health and safety, it is unclear whether they have recognised the need for gaining a wider perspective and knowledge of the situation. The report creates an underlying sense of building the fences higher and reinforcing the physical barriers without putting into place a system that could predict the likelihood of such an attack in the future.



Case study 2 - Africa

This example deals with an oil exploration project in an isolated area of Africa where a disastrous event could easily occur in the future if the right action isn't taken at the outset.

The region has a limited infrastructure and high levels of crime and poverty, but potentially lucrative returns for the right commercial intervention. The advice from the company's security specialists is that essentially all is satisfactory as there is a strong military presence in the area and crime has been reduced in recent years. The military is being friendly and co-operative and the security specialists assert their confidence in the military's capability and intent. The board is using these assumptions as the basis for its decision-making.

However, there are real problems with this line of thought. Do they fully understand the factors that could influence the openness of the military? Do the military really understand what is happening in such an isolated area? Can the military be relied on to always be located there in their current strength? Are the military being completely open as to the causes and effects in crime levels? Are the company aware of the methods employed by the military in maintaining control? In short, is the military unbiased in this situation? The answer to all of these key questions is an emphatic negative.

Furthermore, a cursory glance at the wider situation reveals other significant factors. The political system is centralised, unstable and one in which no commercial organisation would want to be involved should there be sudden regime change. It is likely that the commencement of operations by a Western company would dramatically change the societal dynamics of the region, whilst the influence of other foreign companies needs to be considered. For example, some may have less regard for acceptable business and environmental practices.

Ominously, this scenario contains some similarities to In Amenas, i.e. security being driven by personnel on the ground who are dealing with the hard realities of implementing physical security measures on site. Using military terminology, these people are viewing the situation through the sights of a gun, giving them a very limited perspective.

The role of intelligence in market entry

To give a balanced view, I have been recently involved in two market entry and consolidation projects that have benefitted from the input of intelligence. Located in Africa and the Americas, both projects were in developing countries and had relatively similar operating environments.

In both these cases, discussions on potential operations had been clouded by preconceived ideas and a superficial knowledge of the environment. The situation required a real understanding of the operating environment and its associated incentives, threats and risks for the industry sector. A straightforward analysis of the operating environment helped to dispel these myths and provided the certainty needed for

planning and decisions. Risks were quantified and prioritised, and ways sought to mitigate any projected issues. The decision-makers, purse holders, power brokers, regulators, experts and people of influence were identified along with potential competitors, suppliers, partners and customers. It quickly became obvious that several great opportunities existed and a strategy to engage with these key stakeholders was formulated. Whilst it's early days for these projects, they have been established on a sound foundation of intelligence-led operations.

The six Cs

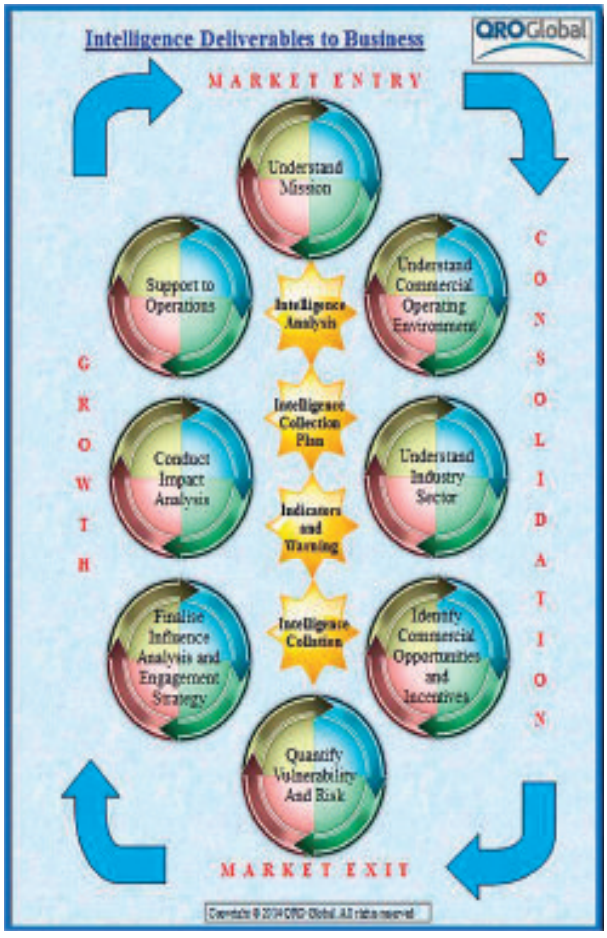
The US Energy Information Administration (EIA) has predicted that the countries of Uganda, which has achieved some stability after years of civil war, and the politically unsettled Madagascar, are poised to become top oil producers in Africa. To succeed in the difficult and unpredictable markets that the oil and gas industries operate within, companies need a proactive intelligence-led approach to business operations. The diagram below represents what a board should expect to have delivered to them by their intelligence expert to support market entry, market exit, growth or consolidation of their business interests. The eight outputs are underpinned by four key intelligence functions in the centre

To clarify, intelligence-led business operations can be broken down into the six Cs: concept, context, challenges, chances, choices and conduct.

Concept: the process starts with the principle that the business objective must be well-defined and understood at the concept phase, providing a common direction.

Context: this is the core of the intelligence work and centres on the principles of intelligence to effect a collection plan and to then transform the resulting information into actionable quantified intelligence. The intelligence picture is broken down for ease of application into Basic (what happened yesterday), Current (what is happening today) and Applied Intelligence (what will happen tomorrow). Often in the business world, the decision-making process is supported only by Basic Intelligence with limited current or predictive analysis. Such 'basic' information can be readily bought from various sources in so-called 'risk assessments' for particular countries or environments. Although of some use, they need to be recognised for what they are: a rudimentary start to the process. Intelligence specialists are able to deliver a much greater understanding, including a detailed appreciation of the incentives and disincentives present in the operating environment.

Challenges: a detailed assessment is made of the identified disincentives in context with the vulnerabilities of an organisation as seen in relation to achieving the objective. The result of this



work is the risk matrix; a prioritised list of risks to the achievement of the objective, the impact on the business and recommendations to mitigate the risks. Woven into this risk matrix are potential courses of action by adversaries and other operational players, as well as the indicators and warning - a red flag system to prompt action in response to a changing operating environment.

Chances: at this stage, a developed understanding of the situation allows for an assessment of business opportunities for the particular industry sector.

Choices: consists of the planning phase, when all of the previous intelligence work is used to define the relationship that exists between people and organisations in the operating environment, the mission and an organisation. These relationships are captured in the Influence Analysis and serve to drive the thought process for determining actions, as part of the Engagement Plan, to shape the operating environment. An analysis of the impact pulls all negative and positive consequences together before the decision is taken to implement the plan.

Conduct: finally, real-time intelligence support to business operations is given during the execution phase.

The net result of this process is that executive decisions are based on a detailed understanding of the operating environment and a set of quantified future opportunities and risks, backed by evaluated solutions, approaches and responses. It is imperative this is forward looking, the key questions being 'So what?' and 'What now?'

When done right, the process leaves the specialist in intelligence in the shadows, and perhaps rightly so. Leaders will always have to take ultimate responsibility for costly and difficult decisions. But, the key question is, can companies in the energy industry use information more effectively, so that decisions on new markets and business opportunities are well informed and timely? World events prove that underestimating or misinterpreting a situation could prove a costly, even deadly business. ■

About the author:

Martyn Denton is MD of QRO Global, which offers a range of intelligence services to business. Martyn has over 30 years' experience in the armed forces, reaching a senior level within the British Army. He has been involved in intelligence operations across the world in both a military and commercial capacity, working in co-operation with the armed forces, law enforcement agencies and government departments of both the UK and foreign nations.