KCS Group Europe

Intelligence failure and the lessons for the corporate sector

15/10/2018

The intelligence community has had its share of failures over the years, from the surprise attack on Pearl Harbour in 1941 to the lack of sharing that contributed to 9/11. But while governmental agencies are always looking to learn from these failures, there are equal lessons for the corporate sector about the pitfalls that accompany intelligence – and how these can be avoided.

There are a number of red-flag issues that are a major part of intelligence work, and even the best analysts can fall prey to these from time to time. Regrettably, even one mindset can be fatal to a successful project and can have serious consequences both short and long term. Let's take a look at some of the most egregious.

Signals v noise. There is a distinction between the two – the noise is the mass of 99 percent of the obtainable and the signals the one percent that actually matters – the distinction between information and intelligence. It is all too easy to get swamped by the signals and to lose sight of the key information. This in turn can prompt poor decision making. What is important, is making the distinction between the signals and the noise and understanding that the mass of noise needs to be examined properly or else the signals may not be apparent.

Intelligence sharing. Widely considered to have been responsible for not catching the 9/11 perpetrators, it has never been so important to discuss and share at all levels both intra-company and between companies. Being caught off guard, or not realising that there is a problem, can only be negated by being open about the need for intelligence and doing it properly.

Satisficing. This is when the analyst has reached a particular conclusion and is now looking for evidence to back up that conclusion. Whether it is the right one to draw, and whether this evidence is indicative of the whole situation, is immaterial – it is a damaging mindset to be so self-limiting. This occurs in the corporate sector when the deal is essentially going to happen no matter what (or may indeed have already been done) and the 'icing on the cake' is to have preconceptions handily confirmed.

Assumption. The most dangerous thing an analyst can do is to assume. Decisions must be based on evidence and logical thought to reach a conclusion, rather than thinking you can know what is going to happen and acting accordingly. However when considering a deal or merger or similar, it is not uncommon for firms to think that there is no reason to require deep due diligence – they know the company in question, or they couldn't find any problems themselves, and so on.

Stovepiping. This is the technique of deliberately limiting your sources and techniques of gathering intelligence, with the result that whatever results has a good chance of being incomplete or plain wrong. Relying on a single source base alone means that it is rarely possible to have confidence in your results. You might have gotten a great deal of information from the approach, but other avenues could enhance, contradict or cause you to think again about what you know. And yet repeatedly stovepiping occurs as a means of ticking a box – to prove that intelligence collection has occurred without considering the ramifications that to only do half the job is just as bad as not doing it at all.

All this is set against the current climate of intelligence work and the state of security – one of fake news, increasing evolution of bad actors, deliberate subsuming of the facts and so on. This is a vital time for intelligence and the corporate sector can learn from why government intelligence fails, and ensure that they protect themselves against the consequences.