KCS Group Europe

Intelligence islands in the stream

5th September 2019

There are serious concerns that the UK will suffer from a security deficit post-Brexit, particularly in intelligence-sharing and cross-border strategies. While it may be impossible to divorce an issue of Brexit from the politics that surround it, on the basest level, it never makes sense to cut oneself off from a stream of intelligence. In general: the more sources and opportunities, the better the product.

The biggest losses post-Brexit, under any scenario, look to be data transfers, intelligence sharing and cross-force cooperation. As the EU Home Affairs Sub-Committee concluded, 'unhindered flows of data' would be lost after departure unless a deal is concluded. While the precise details of the intelligence and data does of course remain confidential, it is very likely to include alternative identities of bad actors, identification of networks, leads to criminal conspiracies, and forecasting/threat assessment. Moreover, this must be considered in the context of not just a "result", but the plenitude of sources involved in reaching that result.

Applying this to the corporate world, we can see the dangers of voluntarily constraining the scope and capabilities of an intelligence investigation. Of the many streams of intelligence-gathering, there are three that are the most use for the corporate world: open-source, human-led, and cyber. Realistically, only by combining all three together can the full picture be seen, and full transparency obtained. But there are those wary of committing to a full-blown investigation: perhaps for reasons of cost, perhaps because they desire only a quick, tick-box effort, perhaps because they do not really want to know what an investigation would uncover. Following up on leads requires the broadest possible range of leads in the first place, which can only come from the variety of sources, and the quality of any resulting product will be diminished the more it relies on just one stream (or even, a single source). From a corporate perspective it would make little sense to voluntarily ignore one, or more, streams, as this raises the risk of gaps and uncertainty where actionable knowledge is required.

The importance of the varied streams as the means by which intelligence is gathered must be understood, in order to understand why 'intelligence' itself is a product that goes far beyond sanctions-checks, database results and the like. Expert human sources with a lifetime's experience in their particular sectors or jurisdictions will be able to indicate far more than open sources – yet these in turn are required to create

foundations point out avenues of investigation. Meanwhile the ability to utilise cyber to complement the intelligence gathering and discover further proofs and indications of the truth is the third string to the fusion bow. But each of these offers something different and unique, and should not be ignored. If each source is viewed only as an island, separate from the others, the quality of the work (and any future decisions) will be diminished.

There will of course be occasions where results are needed as fast as is possible, and in such situations "the headlines" may form the bottom line, but with the caveat that these should always be given further consideration if there are grounds for doing so – even to the point of delaying a deal. It is not worth pushing ahead with a deal based on incomplete or incorrect information as this runs a great risk of entanglement in a controversial situation, or reputationally damaging individuals, down the line. And arguably, such a considered decision can only have merit if it is based on the full range of information available and from a multiplicity of sources.

So while we don't know what exactly will happen with national intelligence sharing and streams after Brexit, the signals for the corporate world are clear: the broader your range of sources, the better.