

## Smiley's happy people

---

26th August 2021

**The ongoing revelations about the arrest of a security guard at the British Embassy in Berlin, suspected of supplying sensitive documents to Russia, brings into sharp relief not only the 'Great Game' of espionage, which never really went away, but the moves by which the game is played. So much focus these days is given over, understandably, to cyber-matters and the degree to which your data may be hacked, ransomed, or monitored through a machine. It is crucial to remember that amidst this world of better spying through technology, the human element remains very much a factor and cannot be ignored – for good and ill.**



Much is unknown about the affair, but the perpetrator was able to pass documents to a Russian handler in return for cash. He was not even a diplomat, 'second secretary' (which means spy) or political liaison, but still managed to get hard-copy documents and smuggle them out. Clearly, there are significant questions to be answered by the Embassy over what level of due diligence was done in the hiring process, particularly as it seems he was in thrall to Russian separatist ideology, and how sensitive information could be acquired and removed from a building where security is supposed to be watertight. But over and above these concerns, we are concerned with the methodology. Was the use of an inside man mandated by the fact that this information, whatever it was, could not be obtained through any technological means? Or was it simply easier, in both access and invisibility, to use the old-school approach?

Stealing secrets through technological means is something of a zero-sum game: you either find a way in, or you do not, and the take will depend on what documents or communications has been digitised. But computers are not subject to the four standard 'MICE' indicators of why people spy: they do not need Money, they have no Ideology, they cannot be subjected to (blackmail-style) Compromise, and machines have no Ego. It is the very human nature of these indicators that has made individuals so susceptible to spying over the decades and why the in-person well continues to be so fruitful: human impulses will never change. Moreover, humans can go places that technology cannot, retrieve information from desks and safes and vaults that is not in digital form, and have the independent thought and action that often enables them to pass under-the-radar.

It would be remiss to claim that incidents of this type, herald a 'new dawn' in spying, of a return to old-school principles. The danger has always been known (not for nothing do multiple intelligence services eschew computers for certain sensitive material, preferring instead to use typewriters) and the occasional public story of, say, a rock with a microphone being found outside an embassy in Moscow or a network of sleepers being discovered in a smalltown suburb, is likely only the tip of the iceberg as far as these things are concerned. Perhaps the problem is that 'cyber' dominates the security conversation to such an extent – particularly in terms of state actors attempting to steal state secrets, or corporates at risk from all kinds of bad actors – that the impact and the damage of a single human source has been under-estimated.

## Smiley's happy people

---

The counterpoint to this is that human sources should be understood as having immense value in terms of reach, access and quality in ways that technological means cannot – although of course this is in no way an endorsement of spying; rather an advocacy for corporates that, in terms of due diligence and intelligence-gathering on the risks, weaknesses and threats that they face, there is no substitute for the local knowledge and individuals able to ask the right questions and for the human factor to be employed in getting to the heart of the matter rather than relying on databases and records.

### KCS Group Europe - Strategic Intelligence & Corporate Security

A leading provider of security and intelligence services, we operate discreetly in some of the world's most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients to identify and deal with any risks, weaknesses and threats which could impact on their business financially or reputationally.

Our key areas of expertise include:

- Corporate Intelligence Services
- New market or sector entry research
- Know your customer screening

In addition, through our specialist team at KCS IS, we also offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits, providing unparalleled, analysis, contingency planning, and implementation for our clients.

**To find out more or to arrange a meeting to discuss your business needs, please...**  
email the team at [info@kcsgroup.com](mailto:info@kcsgroup.com) or call (00 44) 2072451191

---