KCS Group Europe

It's A Hard NOC Life

27th January 2020

The digital era is kind to the armchair detective – with a world of information available at the touch of a button, and technology offering numerous improvements to the accessing, analysing and application of the same, it has never been easier to trace a footprint (or indeed an actual person) and get chapter-and-verse about practically anyone or anything. The downside of this, though, is when a country wants to do some actual spying. So intrusive and omnipresent has technology become, that in-country agents are unable to get around hurdles such as biometrics and facial recognition. This means that some creative thinking is required to ensure that the Great Game can continue…

Undercover, on-the-ground work is reliant primarily on two things: the ability of operatives to work freely (in terms of having a plausible legend), and of avoiding detection (in terms of having documentation to back up that legend). In the Cold War, a carefully forged passport and paperwork would typically be enough, with telephone numbers on business cards, immigration sheets and so on being purposefully manned to add credence from afar, and in extreme cases (such as the famous Argo incident) the fakery would be taken to new heights. But these relied on what were effectively analogue methods. In today's digital world, with the expectation of instant access, it is a lot harder to remain under the radar. A non-official-cover (NOC) operative will need a social media history, an instantly accessible employment and education history stretching back decades, and a set of personal information that will pass not just a check in the country in question, but also the multiple other national and international databases that are now all interconnected.

As if this were not enough, the increased use of biometrics and surveillance can make NOC life practically impossible. Faking documents is one thing, but faking fingerprints and iris scans is quite another. And no longer can an operative lose a tail and feel safe – with cameras, facial ID software and device trackers, knowing where someone is has become just as easy as knowing who they really are.

So faced with these difficulties, spooks are increasingly turning to a new method: staying away from any in-country presence whatsoever and relying on private corporations to act as cut-outs. These companies, which will have a legitimate reason for being in the jurisdiction in question, will be able to operate openly, will not require any specialised or faked documentation, and will have no footprint that can link them back

to any intelligence agency. They are also less digitally reliant than a NOC individual. Tracking a man with suspected fake ID down a street? Bad news. Tracking a businessman who has lived and worked in the country for the past five years? Not so much. Of course, the activities and communications of these corporations will be to some extent dictated by the government and agency, but without the direct 'attendance', plausible deniability can be maintained, and the agency has an extra layer of protection.

This might be seen as the logical endpoint of the privatisation of the intelligence industry. Already in America, for instance, a good degree of governmental intelligence work is carried out by private PMCs and agencies. Why not go the distance and use private companies in the field as well? If spies have nowhere to hide, then remove the need for spies, and remove the ways in which technology can compromise assets. But the corporation-as-spy approach is fraught with difficulties. For a start, it puts the company – most often a genuine and innocent firm – in great danger should it ever emerge that they have been aiding espionage in a host country. Secondly the agency may place its own people in the company, thus running a two-track system of objectives (the genuine corporate interest and the intelligence interest) that risks exposure should wires ever cross, or a silent takeover by the agency itself. And thirdly, if operating under the belief that using a cut-out company offers a greater degree of defence, an agency may push too far with the boxes-within-boxes approach and create such a web of intrigue that keeping a lid on it becomes impossible.

So, activities of private companies should always be viewed through the prism of potential state interference, and the consequences of this for all concerned. While helping one's country is a noble goal, the 'hidden hand' has a reputation for achieving results regardless of the consequences and, in a world where it is increasingly difficult for NOCs to act in the manner required, companies which are small by comparison may find themselves deemed acceptable collateral damage.