KCS Group Europe

Public Enemies No. 1, 2, 3…

9th September 2021

Is the threat picture irrevocably changing? That's the question posed by Director of MI5, Ken McCallum, in his second yearly annual threat update recently. Tellingly, 'disruptive threats' from states – defined by McCallum as 'less visible' when compared to the typical terrorist atrocities – are now put on a par with the latter – and in the current climate, are arguably of greater likelihood and long-term import. The remarks indicate that while MI5 is unquestionably still focused on asymmetrical terrorism, the UK's security posture over the next decade is likely to be defined by how it responds to more subtle and varied threats… that on occasion may not even seem to be threats at all.

If we accept the formulation that (at least to the perpetrators) terrorist attacks are political and ideological in nature, then actions by nation states to disrupt, damage and destroy the infrastructure and security of other states are essentially a modern-day Cold War. We would think, for instance, of last year's sustained Russian campaign of hacking against US government departments via SolarWinds, or China's gaining access to some federal agencies.

What is key in McCallum's latest speech, however, is the confirmation that such attacks are deliberately and specifically targeting private companies and individuals, as part of a blanket approach to sow disinformation in 'the West' and look for a foothold anywhere it can be found. Clearly, access to the heart of government – the 'nuclear codes', or as close to – remain the holy grail for foreign states, but these are also the best-protected targets (at least theoretically). Attention by nation-states therefore turns to cyber-attacks against other entities with access to critical infrastructure or that sit within the supply chain and even firms that are not necessarily critical but for which an attack would be highly embarrassing and damaging in its own right, prompting uncomfortable questions and a lack of public trust in Western systems. Of course, if state-sponsored hacking groups can ransom some money out of these firms, then so much the better.

But a range of subtler methods, too, are being utilised within the mantra of disruptive and less-visible threats. Information is the most powerful currency of all, and disinformation can be equally powerful. The idea of states sowing misinformation first gained currency in the 2016 Presidential election, with Russia widely believed to have been responsible for spreading misinformation and discontent among Americans online that ultimately contributed to a victory for Donald Trump (who, of course, insisted that there was 'no collusion').

Now though, state-sponsored bad actors have a whole toybox of misinformation topics to deal with: most obviously at present the coronavirus crisis and the whole host of anti-vaxx/conspiracy theories that find such fertile ground online from those sporting the latest in tinfoil headgear, but also any issue of politics, social affairs or the economy that can disrupt a business. Anything from mounting a 'hate campaign' against a particular sector or country to disrupt activities there to the benefit of the bad actor state, to seeding deliberately incorrect and misleading information online (the ubiquitous fake news) that leads to the adoption or abandonment of a particular strategy, disinformation is an incredibly powerful weapon that if applied with care, can have a company dancing to the tune of a foreign power and not even know it.

And it is not only in the acceptance of information that public and corporate life is being disrupted – it is the giving of it as well. Nation-state bad actors are returning to the first principles of corporate espionage: targeting ordinary staff of all kinds of companies to elicit information from them. Sometimes the targets will be a means to an end, sometimes their information itself is the goldmine – and the rise of social media makes it so much easier to form a bond of trust without really knowing who is on the other side of the screen.

KCS Group Europe

Public Enemies No. 1, 2, 3…

Over the past five years it is believed that at least 10,000 UK professionals have been phished by foreign nationals on networking site LinkedIn, to be manipulated into providing information (or allowing external access to their organisation) on a one-time, or more extensive basis.

The upshot of this is clear: the 'front' of the conflict between nation-states for political and economic pre-eminence is now squarely with the corporate world and the general public. Not only do firms need to do the utmost to protect themselves at the cyber-level from intrusion, but they need to enshrine firm policies about the evidence basis for what they read/are told, and strict rules on what interaction is permissible with individuals who may have an ulterior purpose in mind. The lack of engagement with misinformation is, after all, the bad actors' Trump card…