KCS Group Europe

Russia: The Mask of The Red State

01/02/2018

Think of the mighty Russian war machine and what do you think of? Massed ranks patrolling through Red Square, Russian submarines conducting operations off the coast of England, Russian jets 'buzzing' Ukrainian territory. It may even be the infamous *'inflatable tanks'* arrayed along the borders as part of the doctrine of *maskirovka* – masking. And yet there is a growing sense that much of Russia's military policy is in itself a *maskirovka*. While a materiel war might be a possibility, the real war – the one fought in cyberspace – is already well underway.

Russia's propensity for cyber-warfare has long been known. We need not return in exhaustive detail to the allegations that Russia interceded in the US Presidential election to ensure victory for Donald Trump – suffice to say that this seems more likely by the day. What is of interest is the degree and scale to which this sort of thing is happening. The Trump allegations are just the tip of the iceberg. KGB misinformation was a favoured tactic during the Soviet era but has, due to technology, been able to take on a whole new dimension. For instance, there are calls to investigate the Leave campaign's financing and social media use throughout the EU referendum. The 2014 election in Ukraine was marred by proven Russian hackers attempting to fix the vote count and delay the result with DDS (with the natural follow-up question being, whether these individuals are state-sponsored). Russia's own national security infrastructure has been informed that Russia is developing cyber-capabilities the impact of which is *'like a nuclear bomb'*. And cyber-espionage against almost every state in Europe, both eastern and western, is a matter of course.

There are three main benefits to this, as far as Russia is concerned. Firstly it is a display of soft power. Just letting it be known to your international fellows that you have a significant aggressive cyber capability is enough to enhance your power, whether or not you actually go on to use it in a meaningful way. Secondly, it is cheaper. The cost of maintaining a full standing army is astronomical. The cost of employing cyber-troops to sit behind a desk and conduct warfare from Moscow (or indeed to hire patriotic criminals for a handful of roubles), less so. And thirdly, the capacity of cyber to be an agent of disruption is far greater than the capabilities of an army. In today's military warfare, in which both sides can track movements via satellite and generally keep well abreast of each other's strategies, it is difficult

to do anything but move openly and declare your intentions. The veil of cyber-warfare allows one to act in almost total secrecy.

So Russian cyber-activity can be broadly divided into three main camps. There is the *'disinformation'* wing – the fake news stories about Hilary Clinton and so on – designed to sway opinions of people in matters where Russia cannot openly influence parties. There is the *'industrial espionage'* wing, where Russian hackers attempt to steal secrets either directly through brute-force black-hat hacking, or by use of online honey-traps (seduction being yet another tract of spying that has gone digital). And lastly there is the *'outright aggression'*, as seen where the state attempted to fiddle the Ukrainian ballot or by taking down Estonia's government infrastructure.

Russia does not need to use all of these, all of the time. It does not even need to use all of them, some of the time. (In part, the conception of possibility is enough to put other states on edge). However it is unavoidable that all three have been deployed recently for the direct benefit of Russia, and that in the current cyber 'arms race' Russia is one of the clear frontrunners. They have the divisions of the army dedicated to propagating warfare from behind their computers. They have hackers-for-hire and web brigades who can conveniently deny any link with the official powers that be. Moreover, there is a lot more that this alliance of patriots and professionals can achieve than, arguably can be gotten through outright warfare.

Outright warfare would be conducted for a few reasons, all of them political: to take territory, to achieve a political goal or to force a reaction from opponents. Two of these do not suit Russia's purpose right now and the third can be far better achieved through the cyber arena. In terms of territory, whatever one's views on the Crimea invasion, to openly move into further land would play Russia's hand too soon and condemn the country to more politically unfavourable opprobrium and sanctions (just what Putin does not need with the World Cup on the horizon. Forcing a reaction: well, all he can conceivably do is get one from NATO, which immediately brings with it a looming *'lukewarm war'* (not a hot war but something more than cold) which, again, is not in either party's interests.

The best (and indeed sanest) course of action for Russia then is to double down on its cyber efforts on the understanding that these are in part untraceable, in all cases deniable, and play to its aims far better than marching more tanks into Eastern Europe. A standing army cannot influence the outcome of crucial political tipping points. A wing of planes cannot steal state secrets or industrial plans. If it is in these dimensions that the wars of today are fought: why, therefore, spend so much time and effort focusing on a ground war that is extremely unlikely to ever happen?

KCS Group Europe

Russia: The Mask of The Red State

Therefore it is proposed that the entirety of Russia's military build-up in hard terms is nothing more than an extensive *maskirovka*: a smokescreen designed to promote the idea of Russian superiority, put friends and enemies on high alert and leave neighbours unsure as to what Russia might do with this force, when in fact it intends to do nothing with this force but cause a scare, while the real work is already well underway back in Moscow. Not only would this be a classic piece of misdirection, it is also the most beneficial course of action for Putin – and could conceivably be so, well into the future. Any military incursion could spark an uncontrollable conflict. With cyber-warfare, wargames can remain games and true Russian power exercised elsewhere. Competing states (and firms) would be well advised to match any build-up of visible defence forces with an equal, if not greater, focus on defending against cyber-attacks. Just because the war is invisible does not mean it cannot kill.