UK launches soft warfare blueprint

By Elisa Barwick

The inspiration for the new US security and defence doctrines launched in December 2017 and January 2018 has emerged with the release of the United Kingdom's Strategic Security Capability Review. Designating major competing world powers, China and Russia, as the enemies of the Western world was always an Anglo-American imperial initiative, just as it was when US Defence Secretary Dick Cheney announced in 1992 that "Our strategy must now refocus on precluding the emergence of any potential future global competitor." Later as Vice President to George W. Bush, Cheney enforced the British-spun lies about Iraqi WMDs, ushering in a new era of pre-emptive strikes and regime change.

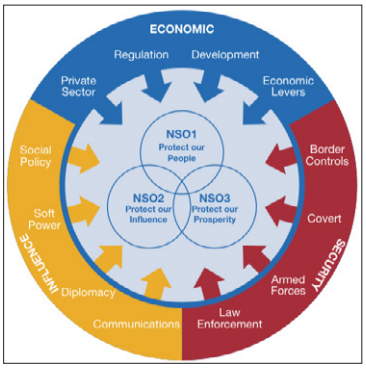
Now the new British paper and its so-called "Fusion doctrine" unveils an era of modern, "soft" warfare against challengers to Anglo-American power. The security review, released as the UK parliament broke for the Easter recess, is a revision of the 2015 National Security Strategy and Strategic Defence and Security Review. *The Telegraph* reported of the scheme on 27 March that "British spies will launch a counter-propaganda war against the Russians" as Prime Minister Theresa May "instructed the intelligence services to use social media to disrupt misinformation".

In the Review's foreword by PM May, "the resurgence of state-based threats and increasing competition between states; the undermining of the international rules-based order; [and] the rise in cyber-attacks from both state and non-state actors" are placed alongside terrorism as the UK's greatest security concerns. Recent terrorist attacks cited include not only those in London and Manchester but the "act of aggression on the streets of Salisbury: attempted murder using an illegal chemical weapon, amounting to an unlawful use of force against the UK".

Britain's new approach to security is based on greater orchestration of all the UK's existing national security capabilities and integration with the private and third sectors, through a new national security doctrine dubbed the Fusion Doctrine. Every government agency and department is expected to view national security as part of its purview. In addition to traditional defences, the new strategy includes modern deterrence, cyber offence and defence, and development of asymmetric response capabilities.

Russia is listed as a threat alongside North Korea, Iran, and an allusion to China's activities in the South China Sea. Russia is blamed without mention of evidence for the poisoning of former MI6 agent Sergei Skripal, which happened against the "backdrop of a well-established pattern of Russian State aggression", including the annexation of Crimea, fomenting conflict in the Donbas region of Ukraine, and Russian support for Syria's Assad regime "including when the regime deliberately ignored its obligation to stop using chemical weapons". Added to this laundry list of lies and mistruths is this corker, given recent exposés of Britain's Cambridge Analytica election meddling: "Russia has also … mounted a sustained campaign of cyber espionage and disruption, including meddling in elections."

The report also elaborates the new era Britain's international relations have entered: "As Global Britain, we are reinvesting in our relationships around the world. We are championing the rules-based system, which has served our interests as a global trading nation and is of vital importance as geopolitics becomes more contested. And we are using our soft power to project our values and advance UK interests." As well as protecting its people and promoting prosperity, the security objectives of the UK include "project[ing] our global influence". "We will establish a Global Britain Board to coordinate Global Britain activity across departments, agencies and our overseas network", says the review. While this sounds exactly like a new imperial expansion determined to upset the current order, the document makes that accusation against other states which are "actively destabilising the world order to their own ends, claiming that the rules and standards we have built, and the values on which they rest, no longer apply".



Theresa May announces a review of Britain's security. Right, a diagram from the new policy document. Photos: YouTube; National Security Capability Review

The increasing emphasis on control over social media under the guise of countering "fake news" allegedly propagated by nations such as Russia is elaborated: "The communications landscape is continually evolving. Communications are increasingly being used by our partners and adversaries alike for strategic real-world advantage. Traditional channels have been largely discarded in favour of digital and social media platforms. This is combined with a decline of trust in traditional sources of information and the era of so-called 'fake news'. In parallel, the rules of the game have changed. The democratisation of information, and the means to exploit it, has allowed hostile actors to exert disproportionate influence in competition with the public interest."

The expansion of the BBC World Service with an extra £291 million investment by 2020 "to increase access to trusted news and information" is another aspect of the "cross-government soft power strategy". In what sounds suspiciously like what the Anglo-Americans accuse China of, the paper discusses using the Foreign and Commonwealth Office, which oversees all UK embassies, and networks such as the Commonwealth of Nations as a further means of extending Britain's power. The document describes all of Britain's international partners and international combines such as NATO and the Five Eyes spying alliance, rubbing in the fact that the British effort will have plenty of backup—or so they hope.

A joint cyber force comprising over 1,000 Government Communications Headquarters (GCHQ) staff, military personnel and contractors, reported recently in UK media, is likely part of this plan. It is to work closely with the US National Security Agency (NSA) and other agencies to develop offensive and defensive cyber capabilities. "Cyber defence is now part of NATO's core task of collective defence", the document notes. This further increases the danger that a cyber attack, which could be easily faked, could be used as a pretext to invoke NATO's Article 5 collective defence clause, whereby an attack on one NATO nation is an attack on them all, and escalate to war. ("London pushes for Article 5 changes at July NATO conference", *AAS* 28 March.)