UK steps up provocations against Russia

By Steve James and Chris Marsden
27 December 2017

Christmas Day saw the frigate HMS St Albans shadow the Russian warship Admiral Gorshkov as it passed through the North Sea.

The BBC report dutifully cited the Royal Navy stating that the presence of the new guided-missile frigate, which is still undergoing sea trials, as being "activity in areas of national interest" and an example of a recent "upsurge in Russian units transiting UK waters."

This was contradicted by the Royal Navy's admission that the Admiral Gorshkov was in fact only "close to UK territorial waters" and the BBC's own admission that Russian ships have used these *international waters* "regularly… in recent times to sail to and from the Mediterranean for deployment off Syria."

This did not stop Defence Secretary Gavin Williamson striking a heroic pose, declaiming, "I will not hesitate in defending our waters or tolerate any form of aggression… Britain will never be intimidated when it comes to protecting our country, our people, and our national interests."

The incident is only the latest example of the UK stepping up its propaganda campaign against Russia.

On the military front, this month saw leading figures in the British military, NATO, and their associated think tanks claiming, without evidence, that Russian naval forces are developing a capacity to sever undersea fibre optic cables.

Chief of the Defence Staff, Air Chief Marshall Sir Stuart Peach, posed "a new risk to our way of life."

"Can you imagine," asked Peach, speaking to the Royal United Services Institute, "a scenario where those cables are cut or disrupted, which would immediately and potentially catastrophically affect both our economy and other ways of living?"

Conservative MP Rishi Sunak in a report, "Undersea Cables, Indispensable, Insecure," from the Policy Exchange think tank banged the same drum.

A foreword by former NATO Supreme Commander in Europe, Admiral James Stavridis, warned that the Atlantic Ocean was in transition "from being a theatre characterised by near complete NATO supremacy following the collapse of the Soviet Union to a space that Russia is actively contesting through a resurgent and revanchist naval doctrine."

Sunak's report underscores the modern world's dependence on undersea fibre cables. Each cable consists of between 4 and 200 fibres protected by steel wire, insulation, armouring and plastic sheathing. Each fibre can carry up to 400GB of data per second. Ninety-seven percent of current global communications travel over 545,018 miles of cabling organised in 213 separate systems.

The main daily physical threat to the cabling network is the continual stress from the conditions in which they operate. Undersea landslides caused by the 2006 Hengchun earthquake, for example, knocked out six of seven undersea cables carrying phone and internet services between North America and much of South East Asia. Repairs took 11 ships nearly two months to complete, during which time the region's communications with North America travelled along the one remaining link. However, such is the nature of internet routing that should one route to a destination address be unavailable, others will be automatically sought and exploited. In 2012, for example, flooding in Manhattan data centres caused by Hurricane Sandy knocked out major network hubs, but the impact on global traffic was minimal.

Less dramatic outages happen all the time. Of all reported cable breaks between 1959 and 2006 as many as 44.4 percent have been attributed to fishing, while 21.3 percent are classed as unknown.

Even such cable breaks can have military consequences. In 2008, shipping in the Mediterranean accidentally cut three cables connecting Italy with Egypt, reducing 80 percent of bandwidth between Europe and the Middle East. The US military, which uses the commercial cable network for 95 percent of its strategic communications, was unable to operate many of the drones deployed against Iraq and Pakistan, so that flights were reduced from "hundreds of combat sorties per day" to "tens."

Sunak nevertheless centred his attention on direct military risks, warning that cables can be cut under the sea, but cited no example of Russia doing so and only one undersea operation, involving the cutting of telegraph and telephone cables during the First World War—by the Royal Navy.

He naturally ignored the primary threat to the internet--the wholesale data harvesting operations mounted by US and British intelligence services as revealed by former US intelligence contractor Edward Snowden. As of 2014, British spy agencies could access data feeds from more than 18 submarine cables making landfall in Britain.

However, Sunak did refer to the US- and Israeli-devised Stuxnet worm which wrecked Iranian nuclear centrifuges, but only to suggest that similar software (by implication Russian) aimed at sabotaging control systems could undermine the network management of entire cable systems or regions. He neglected to draw the obvious inference: that the US is undoubtedly equipping itself with such capacities.

To reinforce his message, Sunak cited the limited revival of the Russian Navy, particularly its submarine fleet over the last decade and a half. The Putin government has, besides modernising its ballistic-missile-armed nuclear deterrent vessels, built a small number of relatively powerful attack submarines. It also has a spy vessel, the *Yantar*, which allegedly has been working to identify cable locations.

Even so, every single investigation of relative strengths places the US, with or without NATO assistance, as possessing numbers and capabilities well in advance of its cash-strapped Russian rival.

This did not prevent the holding of a tabletop exercise, "Forgotten Waters," hosted by the Center for a New American Security think tank, which considered a war scenario in which American warships and troops were seeking to cross the Atlantic in large numbers to reinforce NATO forces in Europe in a major confrontation with Russia. The naval war gamers confronted, "Atlantic waters infested with Russian submarines, surface vessels, or aircraft that transited south" through the GIUK gap--the waters between Greenland, Iceland and the UK. They were also told that "an undersea cable between Iceland and Canada had been cut, creating a significant telecommunications disruption."

The discovery of this new "Russian threat" should be seen alongside the hysterical and unsubstantiated accusations of Russian meddling in elections and plebiscites.

On December 22, Foreign Secretary Boris Johnson visited Moscow for talks with his Russian counterpart, Sergei Lavrov. The meeting saw a public clash over accusations made by Johnson and May of Russian political interference--including in the 2016 Brexit referendum.

May, in a November 17 foreign policy speech to the Lord Mayor's banquet, accused the Putin regime of "deploying its state-run media organisations to plant fake stories and photoshopped images in an attempt to sow discord in the west and undermine our institutions."

Prior to departing for Moscow, Johnson described Russia as "closed, nasty, militaristic and anti-democratic," and said it could not be "business as usual" in relations between the two countries.

Citing the alleged threat to undersea cables, Johnson added that the UK is "prepared and able" to launch retaliatory cyber-attacks, if hackers continued to target Western power stations and communication networks, subvert elections and spread fake news.

At a joint press conference with Johnson, Lavrov described relations between the UK and Russia as "at a low point," before adding, "We hear some aggressive statements from London. Despite all that, we have never taken any aggressive measures to reciprocate."

Lavrov publicly rejected accusations that Russia had interfered in Britain's general election and Brexit referendum, to which Johnson replied, "Not successfully."