NEW-GENERATION WARFARE

Will Ashford-Brown *reveals why hybrid warfare is no longer peripheral but central to Moscow's military doctrine and the threat it poses to Europe*

As much of the strategic debate in recent years has centred on the long-term challenge posed by China, Russia now represents the most immediate and proximal threat to UK and European security. Moscow's systematic use of hybrid warfare – known in Russian doctrine as "new generation warfare" – is already reshaping the security environment, often below the threshold of conventional armed conflict.

Russia's approach to grey zone operations is not opportunistic or ad hoc, but explicitly embedded within its military doctrine. These coercive activities, which include sabotage, cyber operations, disinformation, political interference and economic pressure, are treated by Moscow as a core extension of its warfighting capability rather than a supplement to conventional force.

Russia does not see grey zone activity as something short of war, it is integral to how it pursues strategic objectives, weakens adversaries and reshapes the operating environment without triggering a direct military response. Recent events across the UK and Europe illustrate the scale and intent of this campaign. In October 2025, two British men were jailed for carrying out an arson attack on a London warehouse supplying aid to Ukraine, causing £1.3-million in damage – reportedly recruited by the Wagner Group.

This case highlights a recurring pattern. Russian-linked actors are increasingly recruiting through online platforms to conduct deniable acts of sabotage, often motivated by money rather than ideology. Similar tactics have been observed elsewhere in Europe. In Poland, a series of sabotage incidents targeted the national rail network, including an explosion on a key line connecting Poland and Ukraine.

Beyond sabotage on land, Russia's grey zone campaign is extending into the maritime domain, highlighting the growing role of its so-called 'shadow fleet' – a network of vessels used to evade sanctions – in damaging critical undersea infrastructure in the Baltic Sea.

In late 2024, fibre-optic cables linking Germany to Finland and Sweden to Lithuania were severed, with vessel tracking data placing Russian-linked ships directly over the damage sites. A month later, the oil tanker *Eagle S*, linked to the shadow fleet, was suspected of cutting the Estlink 2 power cable between Finland and Estonia, alongside several data cables.

Low-tech methods can have high-impact consequences. Undersea cables are critical to internet connectivity, financial transactions and energy flows. Disruptions carry serious economic and national security risks, while plausible deniability complicates deterrence.

An explosion in November 2025 targeted a key railway line connecting Poland and Ukraine

Picture credit: KPRM-AP

Russia has also intensified activity in the air domain. There has been a marked increase in Russian aircraft and drones violating European sovereign airspace, forcing the closure of civilian and military airports and prompting repeated NATO interceptions. What began as limited incursions has evolved into deeper penetrations near sensitive military installations.

The objective is to normalise these violations. By gradually shifting the boundaries of acceptable behaviour, Russia seeks to weaken NATO's collective resolve and reduce the likelihood of a forceful response. At a strategic level, Moscow continues to target democratic processes. Moldova's recent national election is a typical example of sustained Russian interference, involving disinformation campaigns, bots and paid online activists. The stakes were underlined when Polish Prime Minister Donald Tusk described the eventual pro-European victory as having: "saved democracy".

The cumulative effect of these activities is a persistent erosion of security, trust and resilience across the UK and its allies. Western reluctance to recognise hybrid warfare as genuine warfare risks enabling Russia to continue these operations largely unchallenged. In response, the UK's Strategic Defence Review is welcome – particularly its emphasis on cyber capability, insider threat mitigation and the protection of critical national infrastructure. However, countering grey zone threats will require far closer collaboration between government and industry, and a broader recognition that conflict has already entered a new phase. It is entirely plausible that the next major conflict has already begun. We simply struggle to recognise it as war because its character is fundamentally different from the conflicts of the past ●

Will Ashford-Brown is the Director of Strategic Insights at Heligan Group.