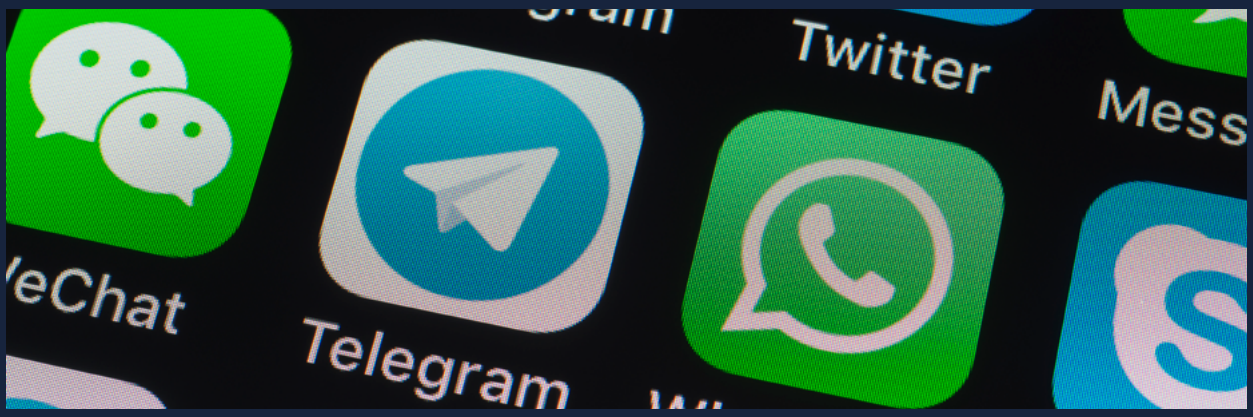
Heligan
STRATEGIC
INSIGHTS

Russia in the grey zone



In 2025 much was said about the long-term strategic threat posed by China, but as we continue to evaluate the ever-shifting threat landscape, there is no doubt in our minds here at Heligan where the most immediate, proximal challenge to UK security comes from – Russia.

While much of our recent work has concentrated on China's influence on UK national security, it is now critical that we turn our attention to a detailed examination of Russia's current threat to the UK and our allies.

Russia's military doctrine explicitly inscribes hybrid warfare, or grey zone activity, into its military doctrine. These are coercive activities that fall below the threshold of conventional armed conflict but are designed to achieve strategic objectives and weaken adversaries. Russia directly refers to these operations in doctrine as "new generation warfare," underscoring its central role. Rather than viewing hybrid activities as merely subthreshold or peripheral, Russia treats them as a fundamental extension of its warfighting capability – integral to achieving strategic objectives.

Russia's long history of conducting these operations has produced a wealth of highly publicised examples, enabling us to examine and better understand the tactics underpinning its hybrid warfare approach.

State-sponsored sabotage

In October 2025 two British men, along with four others, were jailed for conducting an arson attack on a London warehouse providing aid to Ukraine in an attack that caused £1.3 million in damage. Those responsible were apparently recruited through the encrypted messaging app, Telegram, by the Wagner Group, a mercenary group that falls under the Russian Armed Forces.

The following month in Poland, the country's rail network bore witness to a series of sabotage incidents, including an explosion on the line connecting Poland and Ukraine – a vital link that facilitates the transportation of people and goods between the two countries. Poland publicly attributed the attack to two Ukrainians, known to have carried out previous acts of sabotage.

Also in 2025, a coordinated operation saw packages containing explosives delivered to multiple sites across Europe, resulting in fires at mail depots in Germany, Poland, and the UK. Lithuanian authorities, where the parcels originated, have charged fifteen individuals from Russia, Lithuania, Latvia, Estonia, and Ukraine in connection with the attacks. Evidence suggests this operation was orchestrated by Russia's military intelligence agency, the GRU, with recruitment again facilitated by Telegram.

These events depict a strategy of state recruitment of – often unsuspecting – individuals via the app Telegram, to conduct grey zone activities on behalf of the Russian state. On top of this, the motivation in many of these instances appears to be money, rather than ideological impetus.

The shadow fleet

In the Baltic Sea, Russia's 'shadow fleet' – a clandestine network of hundreds of vessels operated by Russia to evade policing following international sanctions – has been attributed to incidents that have damaged critical undersea cables. In November 2024 two fibre optic cables linking Germany to Finland and Sweden to Lithuania were severed, with maritime tracking placing Russian-linked vessels directly above the damage zones at the time.

In addition, a month on from that incident the oil tanker Eagle S, linked to Russia's shadow fleet, was suspected of severing the Estlink 2 power cable between Finland and Estonia, as well as several data cables. Finnish authorities boarded and seized the vessel following the incident.

Russian vessels have been accused of using low-tech methods such as dragging anchors along the seabed to damage cables, an approach that provides plausible deniability. These incidents have had significant consequences as undersea cables play a crucial role in facilitating the internet, financial transactions, and energy transportation between nations, with disruptions risking economic activity and national security.

Airspace violations

Of late there has also been a marked increase in Russian air platforms violating European sovereign airspace – unattributed drones have closed both military and civilian airports in Denmark, and NATO aircraft have scrambled to intercept Russian fighters on a number of occasions. What began as limited incursions across borders has now evolved to much deeper penetrations of Russian aircraft into European airspace, threatening NATO military bases and airports. Russia's objective is to normalise these actions, gradually shifting the boundaries of acceptable behaviour and making repeated violations an established part of the strategic landscape, weakening ours and our allies' collective resolve to retaliate with force.

Election interference

Whilst these acts of sabotage, sub sea infrastructure damage and airspace violations focus on tactical wins, more strategically, Russia has sought to influence national elections in states it considers within its traditional sphere of influence. Moldova's national elections earlier this year, which pitted the pro-European party of incumbent Moldovan President Sandu against the pro-Russian Patriotic Electoral Bloc, is widely believed to have seen Russian interference. An army of bots, as well as paid online activists, are thought to have disseminated false narratives online and on social media to influence voters. When Sandu eventually won the election, with 50% of the vote, Polish Prime Minister Donald Tusk declared that Sandu had "saved democracy," underscoring the high stakes at play for the former Soviet republic.

Key takeaways

Russia's hybrid warfare playbook is now a persistent feature of the strategic environment. Moscow will continue using cyber operations, political interference, disinformation and economic coercion to undermine the institutions and national security of the UK and its allies, gradually eroding our collective resolve. In this context, it is entirely plausible that the next major conflict has already begun – one that we struggle to recognise as "war" because its character is fundamentally different from the conventional conflicts of the past. Western reluctance to recognise hybrid warfare as genuine warfare enables Russia to persist with these operations unchallenged, effectively granting them impunity for actions that undermine our security.

In countering the threat from Russia's grey zone activity, the UK's Strategic Defence Review rightly prioritises key areas for investment and capability development. Heligan sees cyber domain capability, particularly offensive cyber capability, as an area where the UK government will prioritise future spend. Insider threat mitigation solutions, aimed at countering espionage activities, will also be key to shoring up the UK's cyber defence posture. Additionally, solutions that protect critical national infrastructure from malicious actors, including the threat from drones, are likely to get attention, but these priorities represent only a fraction of what the UK must address. Government and industry will need to work closely together to identify vulnerabilities and develop capabilities that can counter both the overt and covert forms of Russian aggression.