Russian Maritime Sabotage: From Subcomponent of Special Operations to Evolving Form of Irregular Warfare

Description

Russian sabotage is a matter of growing concern in Europe, with the risk of maritime sabotage taking particular prominence. And yet, the offence of â??sabotageâ?? was only introduced in the UK in 2023, under the UKâ??s National Security Act. Sabotage is a key component of irregular warfare, whether conducted as part of gray zone operations during peacetime, in pre-crisis shaping operations, or during conventional conflict. This article examines how the Russian approach to sabotage at sea has evolved. Its core contention is that while, until recently, maritime sabotage operations were a subcomponent of special operations, Russian doctrine has evolved and these maritime sabotage operations now constitute a new method of irregular warfare.

Doctrinally, special operations are distinguished by means, not ends. Though special operation forces (SOF) play irregular and unconventional roles, their units are not the only organizations that can do so. Personnel with specialized training and particular skillsets who are provided advanced weapons and equipment have historically epitomized special operations units. This same concept has applied to Russian maritime sabotage until recently but may not do so moving forward. Outside of SOF operations, Russian sabotage campaigns increasingly encompass unconventional warfare via the use of proxies. Moreover, of the growing use of uncrewed systemsâ??both above and below the waterâ??means that the scope and tempo of sabotage operations will exceed the boundaries of special operations. And while the focus on coercion and asymmetry which epitomize irregular warfare remain, the long lead times associated with specialized capabilities and limited scale which historically characterized maritime sabotage may be disappearing. This emerging approach amounts to a full spectrum form of irregular warfare encompassing unconventional operations (the use of non-state actors) and sabotage at scale. Such developments suggest that rather than being a bespoke activity conducted by highly specialized personnel, sabotage may evolve into a much more scalable activity in which a mosaic of organizations and actors participate.

Maritime Sabotage in the Modern Threat Environment

Recent news has highlighted Russian attacks on European, especially Baltic, cable networks. However, it should be noted that relatively few of the breaks are due to suspected irregular warfare acts of deliberately dragging an anchor or fishing gear. In macro-economic terms, cable cuts are

minimally disruptive considering they are a small proportion of the approximately 200 cable breaks a year (most of which occur due to natural causes and human error), and occur within networks that have substantial built-in redundancy. Attackers also face a trade-off between plausible deniability and impact: sabotage on the scale needed to seriously degrade civilian infrastructure necessarily strips away deniability.

However, these incidents have exposed security weaknessesâ??especially the fact that military communication cables may not have the same multiplicity of paths as civilian networks. Moreover, vulnerability varies by region, with semi-enclosed seas like the Baltic enjoying both far less infrastructure redundancy and facing more scope for attack since sabotage is easier in shallow waters. This has prompted a significant NATO response including standing up patrols under Baltic Sentry, and efforts to improve the Recognized Maritime Picture (a real-time operational picture of all maritime activity in a given area created by fusing data from multiple sensors and sources and response times). Notably, the attacks against the Nord Stream 2 pipelineâ??which relied upon explosivesâ??would likely prove easier to attribute today, given the improved surveillance, tracking, and response times achievable in many NATO waters. However, the question of enforcement remains since international law leaves navies little recourse outside their territorial waters in peacetime.

Maritime Sabotage: On the Cusp of a Sea Change

Russian maritime special operations have traditionally been the preserve of both the GRU and Russiaâ??s â??Main Directorate of Deep-Sea Researchâ?? (GUGI). In Western military doctrine, SOF-led maritime sabotage would fall primarily to the GRU Spetsnaz. These units exist within each regional fleet and are highly specialised troops not dissimilar to the United Kingdomâ??s Special Boat Service. They typically operate in relatively shallow waters, with capabilities such as the SOM-1 and TRITON Swimmer Delivery Vehicles, to â??insertâ?? to target. Spetsnaz use of oxygen rebreathers is standard for long range insertion but severely limits depth. Additionally, although the Kilo class submarine is suspected to have a diver lockout capability, Russia has not invested in submarine mounted Dry Deck Shelters. This limits SOF submarine delivery capability to torpedo-tube exits, or requires surface vessel support. Such a limitation implies that although Spetsnaz will likely continue to be used on targets of operational and strategic significance, these will likely be reserved for specialized missions with shallower targets and possible follow-on objectives, where human versatility and adaptability is required.

As uncrewed and autonomous systems improve and become more affordable, Russian naval planners can expand their means of maritime sabotage and can incorporate a wider array of targets. Russia will likely increase its use of uncrewed systems, adding mass to an already potent capability. When it comes to deep water operations, traditionally dominated by the GUGI, the last couple of decades have

seen rapid change. For instance, the *Lima class* submarines that supported manned (saturation) diving to depths of several hundred meters, were decommissioned in the 1990s and the emphasis moved to robotics, manipulator arms and uncrewed systems. These autonomous and remote systems have much more significant depth capabilities and are cheaper and less complex than manned operations. The depth advantage renders cables vulnerable to sabotage or tapping to depths of at least 2,000 m (6,500 ft), and probably deeper. GUGIâ??s manned capability includes titanium hulled midget submarines such as *Paltus*, X-Ray and the larger *Losharik* as well as motherships. These were stretched versions of Yankee and Delta class SSBNs and more recently *Belgorod* and *Khabrovsk.* GUGIâ??s highly specialized personnel, or hydronautsâ??drawn from the 29th Separate Submarine Divisionâ??are typically sailors who have spent at least 5 years as submariners before undertaking a training regimen modelled on that of Soviet cosmonauts.

However, GUGI has been facing challenges. First, its difficult manpower situation was exacerbated by the decision to make its special purpose submarines, such as the *Belgorod*, able to launch Russiaâ??s nuclear torpedo, the Poseidon. This means that they will come under Russian Navy control when tasked as Poseidon launchers. While GUGI has not lost the Belgorod, its command over it and vessels like it now seems contextual rather than exclusive. Additionally, a fire in 2019 crippled *Losharik*, and killed an undisclosed number of GUGI personnel. Notably, GUGI also has responsibility for laying and monitoring â??Garmoniyaâ?• or HARMONY (Russiaâ??s equivalent to Sound Surveillance System or Integrated Undersea Surveillance System), as well as its seabed survey, assessment, and espionage functions. Since the backbone of HARMONY consists of underwater nuclear power units that power sensor arrays, maintenance is likely to be extremely complex. GUGIâ??s commitments, then, threaten to stretch this comparatively small organization of specialists to its limits.

Necessity is often the mother of invention and the need to adapt to resource limitations spurred a useful shift in focus toward the use of uncrewed platforms and less bespoke launch vessels. Surface ships like the 22010 Oceanographic Research Ship (the class to which the *Yantar* belongs) can also play a greater role as hubs for uncrewed systems. Relatively cheap Unmanned Underwater Vehicles (UUVs) can target a much wider range of targets than bespoke submarines with many UUVs based on systems used in Hydrography and Mine Counter Measure operations. Weaponizing UUVs already in use for civilian or military purposes is relatively simple. While the range of these smaller UUVs is limited, it can be extended by using â??extra largeâ?? UUVs such as the Australian *Ghost Shark* or U.S. *Orca* as motherships. Russia is keen on this and appears to be developing its own long range large UUVs such as the *Sarma-D.* In addition, Russia has invested in a range of smaller UUVs such as the *Harpsichord,* already known to be submarine deployed. Reports of an unspecified Russian sensor device found near undersea infrastructure without any mothership in the vicinity provides further indication that this method is already in use.

GUGIâ??s covert capability to support Russian intelligenceâ??by tapping military cables and targeting networks like the Sound Surveillance Systemâ??remains significant, enabling the conventional battle to be augmented through irregular means. However, limited focus will likely expand to the wider critical undersea infrastructure networks. Interestingly, many Western navies have demonstrated that UUVs can be made into a â??plug and playâ?? capability deployable from containerized systems, which might allow their covert deployment from civilian auxiliaries. This being said, the potential use of civilian vessels has limitations, as their ability to hide in maritime traffic may be less viable during conflict.

The regular navy will also see its role in sabotage grow. The Russian Navy has taken a keen interest in Ukrainian uncrewed surface vessel attacks on coastal infrastructure such as the Kerch Bridge and less reported Russian responses in kind. Admiral Nikolai Yevmenov (commander-in-chief of the Russian Navy 2019-2024) described these as indicative of the â??roboticizationâ?? of maritime warfare and noted the asymmetrical advantages such capabilities could provide. Since at sea infrastructure involves many above water components such as oil and gas rigs and ports, it is not hard to gauge the Admiralâ??s intent. However, the utility of uncrewed surface vessels may well depend on geographical considerations, especially if required to transit longs distances in well monitored or rough waters.

Finally, as incidents of sabotage in the Baltic Sea have shown, civilian vessels (particularly in shallow water) can be used as instruments of sabotage with tools as simple as a dragged anchor. If maritime sabotage increasingly relies on networks of proxies rather than direct action, it will mark a further shift in seabed warfare toward irregular approaches rather than narrowly defined special operations.

GUGIâ??s activities and technological developments offer insight into the evolving nature of undersea sabotage. Once a subcomponent of special operations targeting only key assets, it is increasingly employed as a broader instrument of conventional warfare at sea. Sabotage will remain an important part of Russiaâ??s repertoire. However, instead of being a special operation conducted by specialized units (GUGI and the GRU Spetsnaz), it will become a much more holistic form of irregular warfare encompassing proxies, the regular navy and less bespoke uncrewed surface vessels. The role of maritime SOF will remain, but as one part of a mosaic of operational assets. This in turn means that the scale of Russian irregular warfare at sea will expand.

Conclusion

Improvement in uncrewed and autonomous systems at sea and undersea will likely result in a significant increase in Russiaâ??s sabotage threat capabilities. The evolution of sabotage from a special operation to a broader form of irregular warfare will see a growing risk to a greater variety of targets, with much critical undersea infrastructure coming under threat. Russiaâ??s deep-water expertise will pose a significant challenge in terms of protection and repair options for NATO. GUGI

and the GRU Spetsnaz will likely remain the weapon of choice for highly complex or sensitive missions. However, in addition to these threats, proxiesâ??and indeed the Russian Navyâ??will likely participate in sabotage, often leveraging uncrewed systems. Even GUGIâ??s operations will likely take on a different tempo and scale as the requirement for bespoke vessels and highly trained personnel is reducedâ??if not quite eliminatedâ??by the ability to achieve effects with less complex tools. Maritime special operations will be nested in a larger mosaic of irregular warfare capabilities.

For western militaries, the challenge of scale will require a comparably holistic approach to defense. This can include the repurposing of uncrewed surface vessels presently employed in mine countermeasure roles for anti-uncrewed surface vessel defense, the employment of passive defenses such as submarine nets near infrastructure, and the use of naval exercises to create exclusion zones near critical undersea infrastructure in a crisis. While a discussion of the specific organizational and legal response to sabotage is beyond the scope of this article, this response must be informed by the assumption that sabotage will cease to be a special operation carried out on a limited scale by bespoke units.

Sidharth Kaushal is Senior Research Fellow for Sea-power at the Royal United Services Institute. His work at the institute examines the evolution of maritime capabilities and concepts of operations and he works closely with the Royal Navy and Royal Marines. Sidharth holds a PhD in International Relations from the London School of Economics and Political Science.

Commander Edward Black, Royal Navy, is the First Sea Lordâ??s Visiting Fellow at RUSI. Originally a Mine Clearance Diving Officer, he has served extensively abroad including in Afghanistan and as Defence AttachÃ© in Mali and Deputy Defence Advisor in Kenya. He holds an MA (Cantab.) from Trinity College Cambridge, an MLitt from the University of St Andrews in Terrorism Studies and an MRes from Kingâ??s College, London in Defence Studies.

Date Created

2025/12/18