RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No.014– 19 February 2025

No. 014/2025 dated 19 February 2025

Drones, Cables, the Seabed, and the Future of Undersea Operations

Geoffrey Till

SYNOPSIS

Seabed operations are getting more important and, in this competitive world, more fraught. We need to understand why this is happening and what needs to be done about it.

COMMENTARY

According to the International Telecommunication Union (ITU), the United Nations (UN) authority most relevant to the security of undersea cables, about 80 per cent of cable-cutting incidents are genuine accidents caused by sloppy behaviour by merchant ship crews and fishermen — and the occasional bad storm. The other ambiguous 20 per cent of cases are more interesting, in that they could instead be the consequence of deliberate acts by possible adversaries. The recent cutting of cables off Taiwan and in the Baltic came under this category. For that reason, navies and coastguards around the world have started to think much more seriously about seabed security and the many challenges that it faces in times of peace, crisis, and war.

The French Navy was amongst the first off the mark, producing their open-access *Seabed Warfare Strategy* in 2022. But long before that, the Russians, probably in the 1970s, created their Main Directorate of Deep-Sea Research (known by the acronym of GUGI, from the initials of its Russian name). This particularly opaque institution is headquartered in St Petersburg and was almost certainly responsible for the series of intrusions into Swedish and other Scandinavian territorial waters in the 1980s. These left weird tracks on the seabed, which dominated the Swedish media for weeks and were a real source of concern to the then-neutral Sweden. The stranding of a Soviet Whisky-class submarines 'on the rocks' near the Swedish naval base at Karlskrona only added to the government's fear and suspicions.

Since then, the Russians have greatly augmented their undersea programmes. For some years, they have emphasised the disruptive potential of ambitious undersea drones. Currently, their Northern Fleet is experimenting with a large nuclear-powered drone capable of persistent operations in the deep ocean. In Norwegian circles, this is causing some alarm. The Chinese likewise have at least five large undersea drones under development, one of which at 45 metres is probably the world's biggest — unless it is a strange kind of finless submarine. Many other navies are also investing in such potentially disruptive undersea technologies and building centres of excellence to monitor what everyone else is doing and to establish best practice in this murky world.

The Russian ship *Yantar*, believed to be gathering intelligence in British waters, prompted close monitoring by the Royal Navy. *Image source: Mil.ru, CC BY 4.0, via Wikimedia Commons.*

Why Is This Happening?

So the question is: why is this happening — and what does it all mean? There are a number of reasons for such extensive undersea programmes. The first and most innocent is to be better able to monitor, protect, and if necessary, repair and develop critical underwater infrastructure (CUI). Given its importance for both peace and prosperity, countries that do not engage in protective measures of this kind as best they can, would be derelict in their duty to their own people.

Admittedly, such protective action is neither easy nor cheap. Getting all of a country's stakeholders to cooperate with one another, even over something as apparently simple as cable security, takes a lot of institutional engineering. Getting countries to cooperate can be even more so. NATO has taken a lead here with its *Baltic Sentry,* Task Force X, and *Nordic Guardian* programmes of ship, drone, satellite, and AI-enabled coordinated monitoring, interception, and inspection.

In such protective activities, technology will hopefully prove more supportive than disruptive. Persistent AI-enabled undersea drones should facilitate greater coverage and faster, more informed responses. Legal work is necessary too because there is a great deal of confusion and uncertainty about the rights, duties, and responsibilities of coastal states to stop, inspect, and seize ships and crews, and if necessary, prosecute those reasonably suspected of nefarious activity in the Exclusive Economic Zone (EEZ).

The Scandinavians have been actively exploring the legal options. Perhaps inspired by the success of a group of fishermen in driving a Russian naval live-fire exercise out of the Irish EEZ in January 2022, there is interest in leveraging legislation for environmental protection for this purpose. At the same time, it is important to maintain the right to free navigation. The Scandinavians have also been resolute in boardings and seizures, especially of 'dark' ships of uncertain ownership and dubious operational standards. In the last two months, Finland, Norway, and Sweden have all seized suspect ships with Russian connections. So far, though, none of these cases have yet resulted in prosecution. Proving deliberate intent is difficult and takes a long time.

The second possible reason for such intrusive activity is a form of reconnaissance, getting professionally familiar with the conditions in high seas areas of strategic interest. UNCLOS allows this in the EEZ, so long as it does not represent a clear threat to the coastal state. Thus, when the Russian spy ship *Yantar* turns up in British waters with its undersea drones, its activities are closely monitored and escorted but not stopped. Hence the need for aerial and undersea drones to strengthen maritime domain awareness. When the *Yantar* hovers over key British CUI installations such as cables and its activity begins to look more like 'battlefield preparation', the counter-reaction gets more determined. Submarines surface in its vicinity in order to add emphasis to the protective message.

This relates to the third possible reason for such undersea intrusions, namely as either, or both, a deterrent warning shot across the bows or as part of a softening-up process before the planned initiation of combat operations. Plainly, military operations against an opponent who has lost digital connectivity and is therefore mired in domestic and operational confusion would be far easier. GUGI-operated 'fishing boats' are suspected periodically of cutting cables connecting the island of Svalbard with the Norwegian mainland for such deterrent purposes. This could be a rehearsal for conflict, or a warning: 'Look how vulnerable you are; behave accordingly.' How the target chooses to interpret and respond to such challenges is clearly critical. It offers the very real prospect of dangerous misperception. Hence, the need for the close and effective monitoring, and investment in the equipment and techniques that make it possible.

Finally, such undersea activities can be seen as a form of economic coercion through a strategy of cost imposition. It costs the defender a lot more to harden and repair CUI than it does an attacker to damage or destroy it. This strategy, moreover, avoids the greater costs and risks of war so vividly evident in the Ukraine and Gaza conflicts. It also confers the operational initiative and escalation dominance on the attacker. Since the attacker is permanently able to choose the time and place of an assault, his options are huge; this puts the defender into a highly expensive but merely reactive mode.

Responsible Reactions

Anxious to avoid the permanent and substantial disadvantage of a purely reactive counter-strategy, the rational defender has two options, both of which involve heavy investment in undersea operations. The first is to deter such attacks through denial, showing the adversary that such attacks will not work. Thus, the defender hardens CUI and builds resilience, for example, by the construction of back-up pipelines and

cables. This is expensive, however. The alternative is to deter by punishment and to inflict counter-costs on the offender. The defender, for example, might seize suspect vessels, thereby temporarily or permanently depriving the offender of their use — something the Scandinavians have started doing. A more muscular version of the deterrent-by-punishment approach is to 'do it back only worse,' by launching various retaliatory undersea attacks. This would in effect be a form of economic warfare, a cost-effective and coercive action that falls some way short of overtly blowing things up and killing people. This option would furthermore require significant preparatory investment and carries with it a greater risk of inadvertent escalation than a strategy of denial.

Indeed, all these undersea activities carry risk to some degree. Many of them chip away at the principles of trust and transparency on which the maritime world order depends. It is true that they are only novel in the extent to which they are happening 'in peacetime' and in the enlistment of developing technologies such as AI and autonomous vehicles. But the latter is especially important. The key question here is which side benefits most from such potentially disruptive technology? On that, the jury is out.

Regardless, we must expect many more such incidents in a grimly competitive world, especially when the material resources of the deep ocean come to attract much more attention, as they surely will. We must hope that a new operational consensus will emerge through either formal or tacit agreement, as to what is permissible and what is not, in the conduct of these murky undersea operations. So far, though, there seems little sign of this happening. Accordingly, countries should probably work to establish such codes of behaviour but also take responsible and substantial precautions in case they fail to appear.

Geoffrey Till *is the S. Rajaratnam Professor of Strategic Studies and Advisor to the Maritime Security Programme at the S. Rajaratnam School of International Studies (RSIS).*