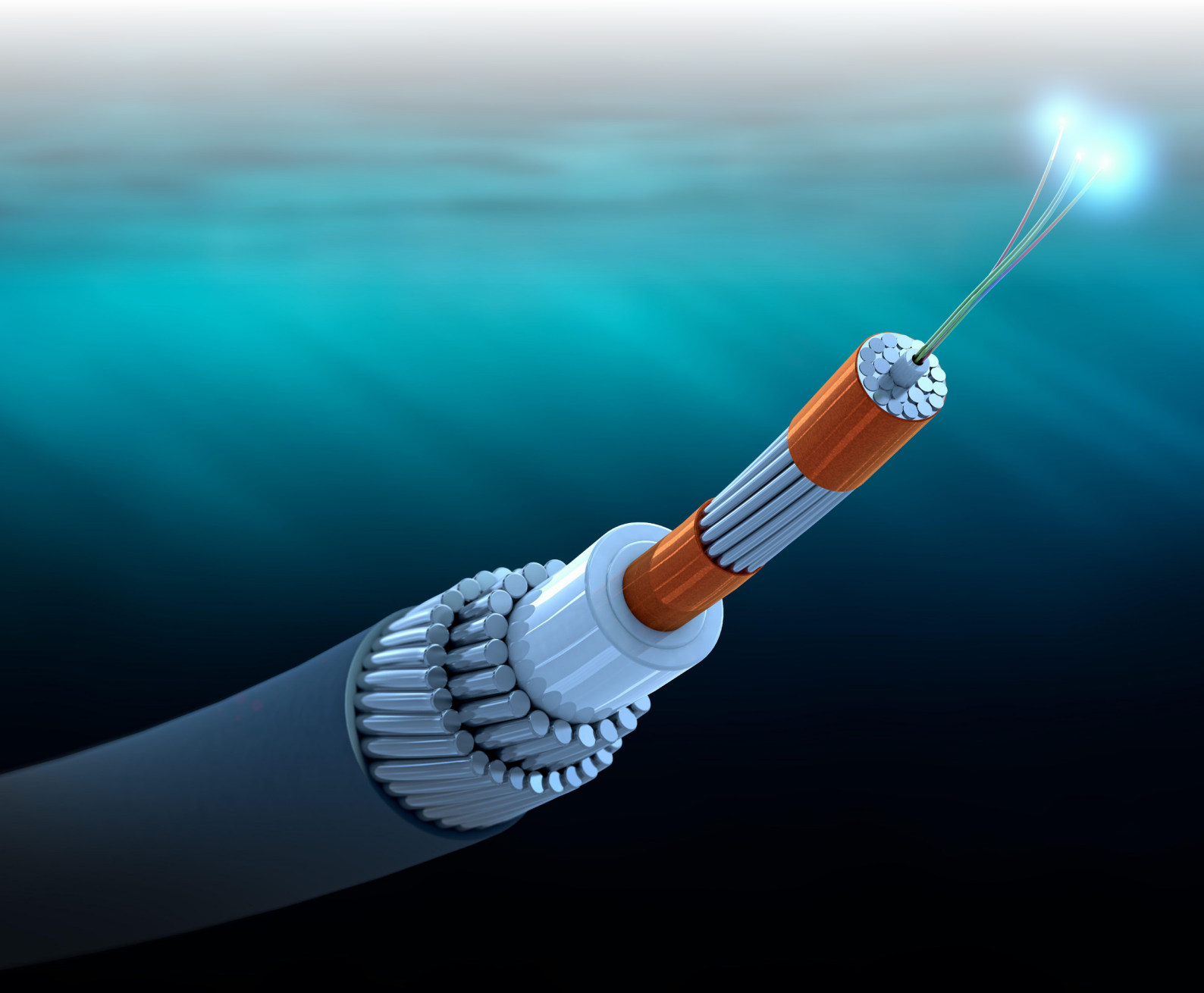
From space to seabed

Protecting the UK's undersea cables from hostile actors

Marcus Solarz Hendriks and Harry Halem

Foreword by Air Chief Marshal Lord Peach GBE KCB DL



From space to seabed

Protecting the UK's undersea cables from hostile actors

Marcus Solarz Hendriks and Harry Halem

Foreword by Air Chief Marshal Lord Peach GBE KCB DL

Policy Exchange

About the Authors

Marcus Solarz Hendriks, Research Fellow, Foreign Policy and Defence
Marcus joined Policy Exchange in September 2023 as a Research Fellow in Foreign Policy and Defence. He holds both a Master's Degree (Politics and International Relations) and a BA (Arabic, Persian and Middle Eastern Studies) from the University of Cambridge.

Harry Halem, Research Fellow, Foreign Policy and Defence
Harry specialises in grand and maritime strategy, defence industrial issues, and strategic history, particularly of British strategy from 1890 to 1945. He is an experienced strategic analyst who is thoroughly familiar with defence industrial and operational questions in modern conflict. Prior to Policy Exchange he was an operational analyst for a macroeconomic consultancy thoroughly engaged in Ukraine coverage, giving him an understanding of the role modern production and dual-use technologies play in contemporary combat.

Harry holds an undergraduate degree in Philosophy and International Relations from the University of St Andrews, and a postgraduate degree in Political Theory from the London School of Economics, where he specialised in comparative intellectual history. Prior to joining Policy Exchange, Harry was a researcher with the Hudson Institute and the Middle East and North Africa Forum.

Published by
Policy Exchange, 1 Old Queen Street, Westminster, London SW1H 9JA

www.policyexchange.org.uk

ISBN: 978-1-910812

Contents

Endorsements

"The protection of undersea cables is a truly collective endeavour. The efforts of all relevant government bodies and private sector stakeholders must be coordinated, and then joined to those of our partners and allies. At present, the Royal Navy and agencies tasked with maritime security do not receive the data and support they need from private companies. Policy Exchange's report pinpoints where this collaboration is still lacking, and demonstrates how the Government can offer greater leadership – and indeed, why it must do so."

Lord (Menzies) Campbell of Pittenweem CH CBE KC FRSE, former Leader of the Liberal Democrats

"Undersea cables are now as important to the international economy as open trade routes. They underpin our financial systems, data exchanges and energy supplies. Britain's economy and security are heavily dependent on its subsea connections with North America, Europe and the Middle and Far East. These are valuable targets for our global competitors: we have already seen Russian attempts to interfere with Atlantic cables. Countries like China are ahead of us in using sensors and unmanned vessels to protect their own networks By sounding the alarm over our extreme vulnerability, this compelling report demands that the government urgently adopt a robust strategic response across multiple theatres."

Rt Hon Sir Michael Fallon KCB, former Secretary of State for Defence

"While Undersea cables may be out of sight, we can never allow them to be out of mind. At a time of rising tensions in Europe this is a very timely report. In 'Indispensable, insecure' Policy Exchange highlighted the need to do more to protect what was then up to 97 per cent of global communications and is now even higher. Progress has been made but the authors are right to highlight what more needs to be done to protect these critical assets."

Rt Hon Sir Jeremy Quin MP, Chair of the Defence Select Committee

"Policy Exchange's second report on undersea cable security is as timely and insightful as the first I endorsed in 2017. The era of seabed warfare has arrived in the Euro-Atlantic, and other contested regions may soon follow suit. The authors offer invaluable proposals for developing a comprehensive strategy to meet these proliferating undersea threats."

Admiral James Stavridis, USN (Ret), former NATO Supreme Allied Commander Europe

"This report is a vital step in the debate on national and international 'whole of system strategy'. Protecting the integrity of subsea data infrastructure will require technical capabilities, skilled personnel and a holistic view of supply chain risk - ensuring a truly whole force approach to the maritime threat."

Sally Walker, former Director Cyber of GCHQ

"Policy Exchange's latest report details in irrefutable evidence that the UK's vast web of undersea cables, interconnectors and pipelines are under a "very real and present threat" from Russia. Increasingly frequent sightings of Russian vessels around this infrastructure, and numerous suspicious cable-cutting incidents in recent years, all illustrate the immediacy of this threat. The actions and statements of President Putin would seem to indicate that he already considers that he is in conflict with NATO, and unattributable attacks on undersea assets play into his use of the grey zone of warfare. Our nation must respond across government with appropriate urgency, and the authors provide vital and actionable measures for how to do so."

Admiral Lord West of Spithead GCB DSC PC, former First Sea Lord and Security Minister

Foreword

Air Chief Marshal Lord Peach GBE KCB DL
Former Chief of the Defence Staff and former Chairman, NATO Military Committee

Undersea fibre-optic cables are the unseen arteries of global communication. Their significance extends far beyond digital connectivity, underpinning the resilience of our economic systems, the efficacy of our defensive frameworks, and the cohesion of our modern societies. Unsurprisingly, they have now become a critical asset – and valuable target – in an era of rising geopolitical tensions.

When then backbencher Rishi Sunak wrote about the insecurity of the UK's undersea cables in his 2017 Policy Exchange report, and I spoke on the same issue in my RUSI Annual Chief of the Defence Staff Lecture that year, this national security risk was scarcely mentioned. Seven years later, however, regular sightings of suspicious Russian activity in nearby waters, mysterious cable-cutting incidents, and the growing concern amongst our allies about undersea infrastructure vulnerabilities, all signal that we have arrived in a new era of undersea warfare.

This new threat landscape demands an urgent assessment of the UK's undersea defences, and the further measures needed to bolster their resilience. Policy Exchange's new report offers just that, comprising a timely update on the state of our national undersea cable security, and proposing a new 'space to seabed' strategic doctrine for protecting our critical subsea infrastructure.

As the report shows, British interests depend on the stability of undersea cable networks the world over. As we are connected to our close Allies by our geography, our history and prosperity it is time – with our Allies – to act.

Moscow has already begun probing Atlantic undersea infrastructure as the weak underbelly of our national security. Targeting critical infrastructure to distract and degrade its enemies is far from an unexpected strategy, but is an essential pillar of Russia's military doctrine.

Further east, China is fortifying its undersea defences as part of its wider aspiration to become a great military power. Beijing's 'Undersea Great Wall' defensive system, and its attempts to finance and establish its own regional cable networks independent of the West, risk fracturing global digital communications in unprecedented and disruptive ways. And, as this report shows, the Supply Chain is taut, cable layers are in short supply, so the industrial angle needs close attention. As the war in Ukraine has shown us with the difficulties in the Black Sea, maritime geography matters.

In the Middle Eastern littoral waters act as the bottleneck of the major Europe-Africa-Asia cable highway. The proximity of the narrow and shallow waters to Iranian shores lays bare the extreme vulnerability of cables passing through this volatile region. The Iran-backed Houthi's assault on global maritime shipping has already demonstrated the ease with which our adversaries can wreak havoc on the water's surface; there are growing concerns that they might also start doing so below it.

The borders between competition, confrontation and conflict are becoming ever closer. The potential for deliberate ambiguity as to 'whodunit' adds to international friction.

Policy Exchange's new report makes targeted policy recommendations – ranging across the tactical, technical, operational and strategic domains – aimed at equipping the UK to protect its assets below the water's surface. Our friends – be they in NATO or the UK-led Joint Expeditionary Force – are reaching the same conclusion.

Novel strategic thinking is required, not least on how we conceptualise maritime defence in the modern day. I firmly believe that Policy Exchange's latest report provides a practical roadmap to formulating a 'whole of system' approach to defending undersea cables across the globe, and against the full array of threats.

Executive Summary

Technological and operational developments have brought geopolitical competition to the seabed. As the ability to manoeuvre, map and operate at greater depths increases, critical maritime infrastructure along the seabed resembles the exposed underbelly of national security in a new age of undersea warfare.

Undersea fibre-optic cables constitute the most vulnerable component of this infrastructure system. 99% of the UK's digital communications with the outside world depend on this cable network. Our social, economic, political and military systems are therefore entirely reliant upon our ability to police and protect the cables which run in and beyond our territorial waters.

Heavy congestion in digital and energy interconnector cable supply chains means that rapidly accelerating demand is set to outpace supply throughout the 2030s. As the global green transition necessitates new subsea infrastructure, cable manufacturing capacity is now over-stretched. Without rapid expansion of cable-making facilities, existing networks are set to come under increasing strain – and with that, their protection becomes all the more essential.

Protection of our undersea cable network poses a unique strategic challenge which distinguishes it from other 'new-age' domains. The current tactical, operational and technological landscape affords outsized advantages to the aggressor over the defender. Ease of access, and the near-impossibility of attributing intentional interference, combines with the difficulty of monitoring and policing such a vast area to an extent unparalleled by other infrastructure targets. The strategic benefits of disrupting these transnational digital connective systems makes hostile action, both below and above the conflict threshold, an immediate and future threat in emergent seabed warfare.

Rishi Sunak's 2017 Policy Exchange report on the insecurity of our cables kick-started the national debate on this critical area of vulnerability. Since then, government and departmental strategic documents have exhibited a stronger focus on the importance of protecting national digital infrastructure, including the 2021 *Integrated Review*, 2023 *Integrated Review Refresh*, and 2022 *National Strategy for Maritime Security*.

Since 2020, there has been a strategic step-change in our approach to the defence of critical maritime infrastructure. Alongside the strategic frameworks mentioned above, the government launched the Joint Maritime Security Centre (JMSC) in 2020, which coordinates the numerous departments and agencies involved in maritime security.

The MoD is investing more in procuring the equipment to deter threats along the seabed, most notably RFA Proteus, the first vessel of the Multi-Role Surveillance Ship programme. The UK has also partaken in a slew of new multilateral initiatives, including NATO's new Critical Undersea Infrastructure Coordination Cell, and the Joint Expeditionary Force's first seabed warfare deployment across the North Atlantic this year.

However, future progress depends on the establishment of a whole of system strategy. The UK must build on these tactical and operational initiatives by formulating a whole of system seabed warfare strategy, which marshals relevant government departments and agencies, as well as the private sector.

Seabed warfare is no longer a futuristic scenario, but a contemporary form of conflict in the era of increasing geopolitical competition. As a belligerent Russia, and disruptive China and Iran, develop the capabilities to conduct subthreshold undersea warfare, the UK and its allies must not be caught flat-footed, and unable to deter and disrupt aggression against our critical maritime infrastructure along the seabed.

Since 2021, there have been eight unattributed yet suspicious cable-cutting incidents in the Euro-Atlantic, and over 70 publicised sightings of Russian vessels behaving abnormally near critical maritime infrastructure. On numerous occasions, such as during the Shetland Islands cable-cutting in 2022, Russian ships have been spotted at the time, and in the vicinity, of the incident. The frequency of incidents and sightings involving critical maritime infrastructure is increasing. As the Ukrainian War is set to lock conventional forces for years to come, Russia is looking to achieve asymmetric advantages in the new-age frontier of the undersea domain.

The Irish and North Seas constitute the weakest point in the UK's maritime defence. Irish neutrality compounds the ease of access of Russian vessels to nearby waters, leaving the UK's western cables vulnerable both at sea and on shore.

Chinese undersea offensive and defensive capabilities are fast improving, posing growing risks to cable networks in the Indo-Pacific. The PRC is rapidly building its undersea arsenal of attack and defence capabilities, which is certain to play a significant role in future contestation in the region. Last year's suspicious cutting of two cables connecting mainland Taiwan to the Matsu Islands illustrated the likelihood of critical maritime infrastructure forming a primary target in a Chinese invasion, blockade or grey zone conflict of Taiwan. The PRC is also developing its own regional cable network independent of western control. This heralds a bifurcated cable system in the Indo-Pacific, which would immunise China from the impact of future disruption to existing networks.

The waters around the Arabian Peninsula are the major, congested cables crossroad running between Europe, Africa and Asia – and highly vulnerable to sabotage by Iran and its regional partners. The only factor restraining Iranian disruption of these cables is Tehran's own dependence on them. Should a war arise which threatens the regime's survival,

internecine Iranian attacks on cables would become entirely plausible. Meanwhile, fears are growing that the Houthis might begin targeting Red Sea cables as part of their disruption to global maritime systems.

In order to continue developing a robust defensive system to meet these threats, more operational capacity and strategic clarity is needed. The recent acceleration in acquiring undersea capabilities has established the UK as a frontrunner in this domain. That said, the sub-surface and seabed warfare domains are still insufficiently integrated into broad maritime and security doctrine. As a result, the Royal Navy and MoD are responding to mounting threats without a coherent whole of system framework. The JMSC, tasked with intelligence-gathering and responding to maritime threats, is department agnostic and lacks a legislated basis to conduct its own prescribed tasks. Whilst the JMSC convenes the panoply of agencies engaged in its work, it therefore lacks the authority to commission its own intelligence-gathering and analytical tasks, and is reliant upon joint, short-cycle funding from multiple departments.

The MROSS programme is an important step towards greater operational capability in the undersea domain, but more ships are needed to police our waters adequately. The first of the MROSS programme's two surface vessels, RFA Proteus, is still yet to complete its Operational Sea Training. Furthermore, despite the impressive technical and tactical showing, the operational and strategic benefit of two additional surveillance ships is limited, given the existence of multiple high-threat areas requiring constant monitoring in our waters and further afield.

New multilateral initiatives with our partners signal promising intent, but closer capability enhancement and regular joint operations are needed to provide collective deterrence in the present threat landscape. Whilst NATO and the EU have launched commissions and new agencies tasked with undersea defence, they mostly still remain limited to establishing definitions and formulating strategic concepts. More capability development coordination, and regularised joint operations towards clear strategic aims, are needed to create an interconnected defensive system to ward of hostile sub-surface activities.

The UK can benefit greatly from ad hoc partnerships with likeminded partners. Closer collaboration with other nations at the vanguard of maritime capabilities, such as France, and those with whom we enjoy close strategic alignment, such as the Baltic states, should be pursued when strategically beneficial.

There is insufficient clarity over where private sector responsibility for cable protection ends, and where the MoD's begins. Clearer legal and operational guidance must be given to the private entities which own and maintain cables over where their obligations lie, and where it becomes the task of the MoD to respond to suspicious activity and cable damage.

Full protection of cables will be impossible without closer public-private cooperation and data-sharing. Air-based data and satellite imagery are integral components of a robust maritime defence system, as undersea acoustic signals must be cross-checked with satellite imagery for

maximum surveillance and identification precision. Commercial data can also be used to develop evidence bases to attribute blame publicly when military intelligence cannot. This calls for expanded cooperation between government agencies tasked with seabed surveillance and private satellite-owning companies, under the umbrella of a comprehensive 'space-to-seabed' strategic doctrine.

The United Convention on the Law of the Sea, and its ancillary legal frameworks, are entirely inadequate for regulating activity along the seabed. As it stands, hostile first-movers will continue to act with impunity and alter the undersea strategic landscape through *fait accompli* actions. The UK cannot idly await an international effort to update UNCLOS, and must make use of its sovereign prerogative to pass laws to better protect its territorial waters.

In the absence of an up-to-date and robust international legal framework governing 21st century activities under the water's surface, a technological and operational arms race is underway between offensive and defensive capabilities. Resource-rich and technologically advanced first-movers are likely to acquire critical and durable advantages to achieve strategic objectives in this vast domain. The seabed can thus be characterised as in an interim phase between an era of competition and one of contestation. During the Cold War, the US-led underwater monitoring and policing Sound and Surveillance System (SOSUS) secured strategically significant, sub-surface dominance across the Pacific, Atlantic and Mediterranean. This constrained Russian submarines' ability to manoeuvre and threaten NATO territorial waters. The West must learn the lessons from the SOSUS to achieve similar dominance in the 21st century across the Euro-Atlantic and Indo-Pacific.

Introduction

The seabed remains distant and overwhelmingly unknown – to date, only 20% has been mapped at high resolution.[1] To those tasked with ensuring national security however, it has never felt closer, nor more in-focus.

Increasingly frequent warnings from our allies highlight the chronic vulnerability of our undersea critical maritime infrastructure, and the ease with which adversaries might target these weaknesses. The surging state interest in the exploration – and exploitation – of global seabed systems signals the ongoing transition from an era of underwater competition to one of contestation, heralding a new age of seabed warfare.[2]

In recent years, the UK has responded to these growing threats with a strategic step-change towards the undersea maritime domain. Successive government and departmental strategic concepts – including the 2021 *Integrated Review*, the 2022 *National Strategy for Maritime Security*, and the 2023 *Integrated Review Refresh* – have exhibited a newfound appreciation for the need to protect our critical undersea infrastructure. Meanwhile, the Joint Maritime Security Centre (JMSC), established in 2020, pools the agencies and departments involved in maritime security into an operational centre of excellence. The MoD has also invested heavily in procuring surface and sub-surface manned and unmanned vessels, as well as monitoring devices, to bolster our national defensive system. The number of joint initiatives with our allies for building collective resilience into critical undersea infrastructure has proliferated, as we increasingly shift our focus below the water's surface.

The UK's ability to police and protect this domain has therefore vastly improved rapidly in recent years. Yet, we still risk not keeping pace with the rapidly growing array of threats. This endangers the undersea infrastructure which undergirds our national prosperity and security.

Since Rishi Sunak first exposed the UK's undersea cable vulnerabilities in a paper for Policy Exchange in 2017,[3] future threats have swiftly become those of the present. In 2022, Chief of the UK Defence Staff Admiral Sir Tony Radakin rang alarm bells over Russia's increasing underwater activity, which seeks to "exploit the world's real information system… the undersea cables that go all around the world".[4] He continued by asserting that any intentional disruption to these networks could be taken as an act of war. Meanwhile, a NATO report last year warned that seabed warfare is no longer a distant concept: it represents an immediate threat to Allies".[5]

Whilst Sunak prudently identified Russia as the main geopolitical threat in the undersea domain, escalating tensions with China have pushed the question of cable security beyond European waters. The UK's contested

1. National History Museum, https://www.nhm.ac.uk/discover/news/2022/february/two-thirds-life-seabed-unknown-science.html#:~:text=Despite%20covering%2071%25%20of%20the,are%20yet%20to%20be%20described.
2. Seabed Warfare Strategy, French Ministry of Armed Forces, February 2022, https://www.archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf.
3. Rishi Sunak, Undersea Cables: Indispensable, insecure, *Policy Exchange*, 2017.
4. Larisa Brown and Catherine Philp, Admiral Sir Tony Radakin warns of Russian threat at sea, *The Times*, 7 January 2022, www.thetimes.co.uk/article/admiral-sir-tony-radakin-warns-of-russian-threat-at-sea-kx-7vf5sxv.
5. Protecting Critical Maritime Infrastructure – The Role of Technology, NATO Parliamentary Assembly, executive summary, 6 April 2023, https://www.nato-pa.int/download-file?filename=/sites/default/files/2023-04/032%20STC%2023%20E%20-%20CRITICAL%20MARITIME%20INFRASTRUCTURE%20-%20FRIDBERTSSON%20REPORT.pdf.

strategic environment now extends beyond the Euro-Atlantic to the economically vital Indo-Pacific region. The epicentre of Sino-American competition is the South and East China Sea, both major nodes of maritime activity and critical maritime infrastructure.[6] With China rapidly expanding its naval surface- and sub-surface capabilities, the likelihood of the deep-sea domain entering the contested Indo-Pacific theatre in the near-future is high.

Fears are also mounting that the cables which pass around the Arabian Peninsula will be targeted by Iran and its regional partners. The Red Sea and Persian Gulf constitute one of the three major global cable chokepoints, transmitting data between Europe, Africa and Asia. Whilst Iran depends on this infrastructure for its own connectivity, any conflagration which threatens the regime's survival may lead it to calculate that the cables have become a strategic target. Meanwhile, posts on the official social media channels of Iran-backed groups across the region, including the Houthis[7] and Hezbollah[8], have raised the alarm that they may broaden their response to the Hamas-Israel War to the subsea domain.

This interconnected strategic matrix is simultaneously extending the UK's maritime security parameters down towards the seabed, and outwards to far-flung waters. The result is the UK's increasing positioning in the midst of a hotly contested, intercontinental geopolitical environment, combining land and sea in what Policy Exchange has previously called the battle over Eurasian heartlands.[9] Hybrid warfare is flourishing within this context, which enables competing nuclear states to degrade one another's capabilities below the threshold of war, and with high degrees of deniability.

Despite this mounting concern over disruption to undersea infrastructure, the threat has been a reality for generations. Britain was the first nation to demonstrate the strategic sensitivity of undersea cables, when it cut all but one of Germany's at the beginning of World War I. This forced Berlin to re-direct all its sensitive digital communications along the remaining line. Britain tapped this line with a bugging device, thereby enabling vital military communications to be decoded.

As technology has developed, the ability to strike sub-surface maritime targets has increased. In 2014, an American strategic assessment anticipated a futuristic strategic landscape of sea warfare, coined a mature maritime precision-strike regime (MMPSR).[10] As land-based strike range extends into adversarial maritime bastions, large ocean swathes will become vulnerable overlap zones between offensive and defensive systems. This environment would pose significant risks to all surface operations, leading the report to predict the increased likelihood of competitors targeting one another's undersea infrastructure as a potentially devastating "cost-imposing strategy".[11] The assessment thus impelled the US and its allies to prepare defensively with urgency for, even with the most comprehensive and sophisticated defence systems, preventing such acts would be achieved with great difficulty.[12]

As an island nation, and the acting fulcrum of the Euro-Atlantic

6. Joe Brock, US and China wage war beneath the waves – over internet cables, *Reuters*, 24 March 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/.
7. Telegram Post, 24 December 2023, in *MEMRI*, In Veiled Threat, Telegram Channels Linked to Houthi Ansar Allah Movement Point to Submarine Internet Cables Off Yemeni Coast, 26 December 2023, https://www.memri.org/jttm/veiled-threat-telegram-channels-linked-houthi-ansar-allah-movement-point-submarine-internet#_edn1.
8. Telegram Post, 24 December 2023, Ibid.
9. Sir John Jenkins *et al*., The Iran Question and British Strategy, *Policy Exchange*, 17 July 2023, https://policyexchange.org.uk/publication/the-iran-question-and-british-strategy/.
10. Defined as a state of global military affairs when great powers have developed a maritime battle network incorporating advanced ISR, and precision-strike capabilities.
11. Andrew Krepinevich, Maritime Competition in a Mature-Precision-Strike Regime, *CSBA*, 2014, 101.
12. Ibid., 101.

alliance, the UK is especially reliant on the maritime domain for its trade, energy and communication. Undersea cables constitute the bedrock of the undersea dimension of this maritime infrastructure system. Approximately 60 cables make up the British network, carrying 99% of the digital data which powers all communication with the outside world.[13] With cables owned and operated by private entities, these transnational networks provide the architecture for all digital traffic, from WhatsApp messages between friends, to government emails, to sensitive military intelligence. In other words, the 1.4mn kilometres of undersea cables worldwide constitute the connective tissue of the entire global community.[14]

The transnational nature of this cable network renders it at significant risk in the current, increasingly contested geopolitical landscape. Both Russia and China stand as revisionist states seeking to undermine the post-World War II international systems, established and upheld by political liberal states with open economies. The linkage between economic prosperity and national security has therefore come under renewed scrutiny and peril. Whilst Russia's invasion of Ukraine is a clear menace to European security, it has also demonstrated the highly exposed nature of the continent's economic foundations, evinced most patently by the subsequent energy crisis. The Nord Stream pipeline incident of September 2022 illustrated how the undersea connectivity network represents the confluence of European infrastructural and economic security risk. In the aftermath, NATO's intelligence chief David Cattler raised the alarm that Russia may seek similar strategic goals by targeting undersea cables "to gain leverage against those nations that are providing security to Ukraine".[15]

The undersea domain's sheer size and inaccessibility makes it particularly suitable to the strategic grammar of hybrid warfare, further raising the probability of our critical maritime infrastructure being the target of future hostile acts. Dual-use scientific and technological developments are arriving at a pace which is outstripping the legal framework encompassing the seabed, enlarging the grey zone of hybrid warfare tactical options. The undersea domain therefore joins space and cyberspace as the new-age frontiers of competition. Its ill-defined and ungovernable nature has led it to be characterised as the 'undersea Far West'.[16]

This paper aims to set out how the UK can guarantee its national security against hostile states within this new-age undersea Wild West, which tethers our metropoles, shorelines and territorial waters to those of our allies and partners. The Russian, Chinese and Iranian threats to British critical maritime infrastructure share commonalities but also points of divergence. Only a clear-eyed assessment of the strategic landscape adumbrated above can diagnose the natures of these respective threats, and so pave the way to targeted and effective policy responses.

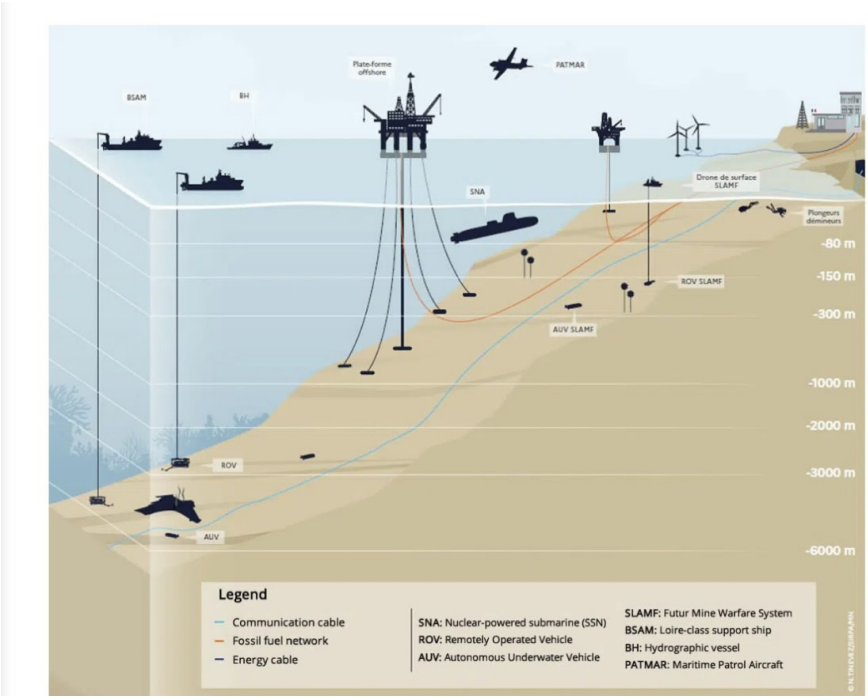
The sheer vastness of the undersea domain, its transnational nature, and its combination of physical and digital facets, all compel close partnership with allies in a format structured to meet these challenges. Presently, neither the UK's unilateral measures and technical capabilities, nor the urgency and coordination of fledgling multilateral responses, suffice.

13. Unseen but vital: Britain and undersea security, *The Council on Geostrategy*, 8 March 2023, https://www.geostrategy.org.uk/britains-world/unseen-but-vital-britain-and-undersea-security/.
14. TeleGeography, Submarine Cable 101, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions
15. Sabine Siebold, NATO says Moscow may sabotage undersea cables as part of war on Ukraine, *Reuters*, 3 May 2023, https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/.
16. French *Seabed Warfare Strategy*, 26.

The systematised public-private partnerships needed to develop a whole of system framework for ensuring maritime security are also absent. At this rate, undefended undersea cable networks will remain an exposed western underbelly, presenting adversaries with an enormous target to inflict immense damage, at relatively low cost and risk.

A strategic step-change is needed which integrates seabed strategy into the heart of wider national security. This may only be achieved by assessing the interstate competition taking hold in the undersea domain, analysing the strategic rationale of ongoing adversarial surface and sub-surface activities, exposing current national and allied defensive shortcomings, and identifying concrete, actionable measures to bolster the UK's maritime defences. In doing so, this paper takes the first step towards formulating a **seabed warfare strategy which conceptualises a 'space-to-seabed' maritime doctrine to meet our security needs**. Defence of all depths of the sea cannot just happen at sea, as air-based surveillance and satellite imagery are integral to 21st century monitoring and precision operations.

Chapter I: The Seabed as a Strategic Domain



Source: ***Marine Nationale, France (translated by Naval News)*** https://www.naval-news.com/naval-news/2022/02/france-unveils-new-seabed-warfare-strategy/.

Policy Exchange's first deep dive to the seabed, 2017

Policy Exchange's 2017 paper on the UK's undersea cables problem, *Indispensable, insecure*, authored by now-Prime Minister Rishi Sunak, was described as "groundbreaking" upon its publication.[17] It shed light on the strategic negligence of the UK and its allies in permitting its digital connectivity infrastructure to become so vulnerable to accidental and intentional damage alike. Whilst the most frequent cause of damage may be the snag of a trawler's net, the report called for greater focus on threats of human design – whether by lone saboteurs, terrorists or hostile states. Whatever the motivation, the stark revelation was the disproportionally large disruption to international digital channels which could be caused by a single, minor act of either physical or cyber nature.

The paper cited the Luzon Strait crisis of 2006 as a powerful illustrator

17. Unseen but vital: Britain and undersea security, *The Council on Geostrategy*.

of this reality, when an earthquake in the western Pacific Ocean severed six out of seven undersea cables, causing a widespread digital communication breakdown for 49 days between Taiwan, China and South Korea. That such incidents are not freak outliers was demonstrated by the report's appendix, which documents nine major disruptions to undersea cables networks since 2003.

Continuing the theme of the disproportionate relationship between system resilience and threat, the paper contrasted the flimsy and outdated international legal framework governing the undersea domain with the opportunity for sophisticated interstate conflict. At the time of writing, the greatest threat came from Russia. *Indispensable, insecure* details the Russian Navy's two decades-long transition from conventional surface power to sub-surface mapping and targeting capabilities, with the undeniable strategic objective of developing novel ways of waging asymmetric, below-threshold war on NATO. Russia's successful exploitation of Crimea's internet infrastructure in 2014 demonstrated the Kremlin's proclivity for exploiting information channels in its hybrid warfare doctrine.[18] Sunak's paper noted the convergence of Russia's undersea mapping and targeting programme with its wider strategic aims, testified by the numerous subsequent reports of Russian activity along the North and Baltic Seas' critical maritime infrastructure hotspots. The ability to couple (dis) information campaigns with offensive disruptions to financial, social, military and governance communication channels would constitute a significant mode of incapacitating western civil and military systems, offering clear strategic advantages at low risk of escalation.

The Russian Navy's oceanographic ship, Admiral Vladimirsky, part of its 'spy ship' fleet which has been caught acting suspiciously around British and European critical maritime infrastructure in recent years. *Source:* ***https://syria.mil.ru/en/syria/***

18. Keir Giles, Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power, *Chatham House*, 21 March 2016, https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power.

bulletins/bulletin/more.htm?id=12067960@egNews.

As mentioned, the existing international legal framework is ill-equipped to interdict such actions. Now, as in 2017, only three international conventions cover the sub-surface maritime domain: the 1884 Convention for the Protection of Submarine Telegraph Cables; the 1958 Geneva Convention on the High Seas; and the 1982 United Convention on the Law of the Sea (UNCLOS). As the dates would immediately suggest, none of these provide meaningful dissuasion again modern hostile tactics in the 21st century; the 1884 Convention even makes explicit that its injunctions are not meant to "in any way restrict the freedom of action of belligerents".[19] Most importantly, these legal parameters all have pre-Information Age origins, long before the internet emerged as the global nervous system. They are therefore "far more suited to the comparatively peripheral role the [undersea] infrastructure played in the '70s and '80s",[20] and so entirely inadequate to govern the ongoing advances in artificial intelligence, cyberspace and advanced robotics which herald the Fourth Industrial Revolution.

With the strategic and technological landscape thus articulated, as well as the inability to rely on legal deterrence to arrest hostile sub-surface acts, the paper proposed unilateral and multilateral steps for the UK and its allies to defend their undersea cable networks. Some of its recommendations have been acted upon, such as its call for more NATO naval exercises with specific attention on the sub-surface domain. Last year's formation of NATO's Critical Undersea Infrastructure Coordination Cell (CUICC), located in Brussels, was an important first step at establishing greater coordination at the strategic level. There are also signs[21] of the EU and NATO recognising the imperative of building greater redundancy into their shared critical maritime infrastructure (such as by employing 'dark cables' which switch on when main cables are damaged), as per Sunak's policy proposals.

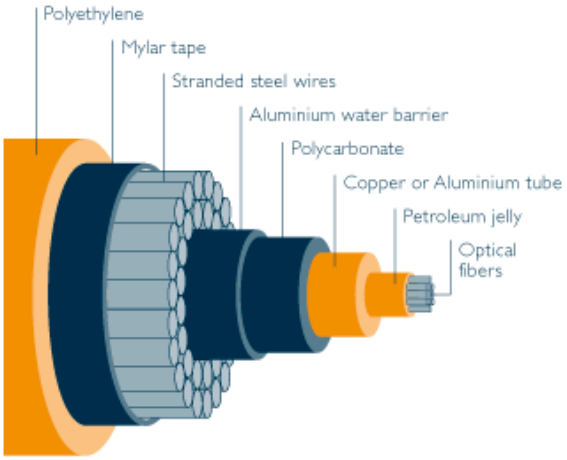
Other recommendations, however, have moved at a slower speed, notably in the deployment of monitoring equipment around cable hotspot zones, and standing up a dedicated naval fleet tasked with critical maritime infrastructure protection and including surface ships, submarines, and state-of-the-art UUVs and AUVs. Most concerningly, a final tranche of recommendations has not been acted upon at all: the UK and its allies have not led a drive to update international maritime conventions; global cable networks remain over-concentrated and undiversified; and the UK is yet to produce a strategic document which sufficiently integrates critical maritime infrastructure and the undersea domain into wider maritime doctrine and overall national security.

The upshot is that, seven years on, the UK's undersea cable security remains inadequate for the threat landscape which existed in 2017. As the next section demonstrates, this landscape has become even more perilous in the intervening years.

19. Submarine Telegraph Act 1884, Chapter 49.
20. Rishi Sunak, Indispensable, insecure, 17.
21. EU-NATO Task Force on the Resilience of Critical Infrastructure, 3.

Why undersea cables matter

Despite the misnomer, digital data is not stored in the 'cloud', nor does it travel between satellites above us. Instead, it is stored in large data centres on land, and moves across the world via some 500 ocean-traversing fibre-optic cables. 99% of our digital communications – whether it be social media posts, financial transactions between banks, or commands between military control centres and autonomous vehicles hundreds of kilometres away – rely upon these cables to function. Apart from a handful of closed military networks, the rest are owned by commercial entities.



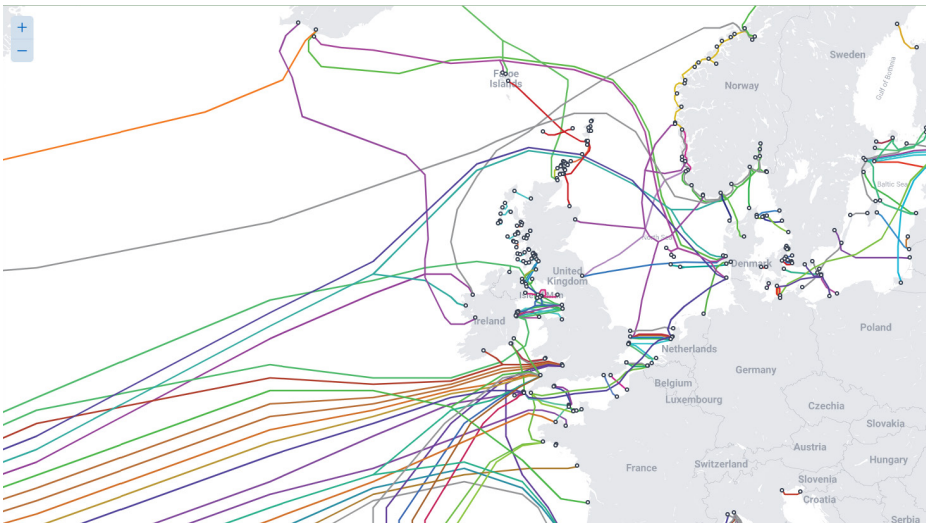
Source: https://blog.leaseweb.com/2013/09/16/scuba-dive-into-the-world-of-submarine-cables/

Put simply, without these cables, modern life as we know it would cease to function. The repercussions of cable damage can vary immensely in scale: those with high degrees of redundancy (meaning the presence of back-up 'dark cables', which activate if main routes are severed) can survive minor disruption. Failure of networks without these levels of in-built contingency, however, comes with massive consequences. In 2022, the Hunga Tonga-Hunga Ha'apai volcano erupted, severing the lone cable which connects Tonga to its neighbours. As a result, the island was cut off from the outside world for weeks. In 2008, the US Air Force lost communication with almost all its UAVs operating in Iraq and Pakistan, when a major cable running between Italy and Egypt was disrupted. When asked what would happen to the global financial system in the eventuality of widespread cable outage, the Former Federal Reserve chief of staff replied, "when communications networks go down, the financial services sector does not grind to a halt. It snaps to a halt".[22] It is therefore no exaggeration to say that undersea fibre-optic cables are as integral to the functioning of everyday life as the infrastructure which carries energy to our homes and offices.

22. Captain Douglas R. Burnett, Cable Vision, *Proceedings*, U.S. Naval Institute, 2011, 67.

The scenario today

The UK's transatlantic and European cable network



*Source: **https://www.submarinecablemap.com/***

The European Security Landscape

The UK's position within its European context today could not be more different to what many might have anticipated in 2017. The Brexit vote appeared to divert the UK from the bloc's ever-closer economic and security path: it would leave the single market at the end of 2020; whilst the referendum excluded the UK from the EU's 2016 Global Strategy aim to "enhance [its] credibility in security and defence".[23] Whilst the bloc progressed towards the establishment of a European security framework – later codified in its Strategic Compass of 2022 – the Brexit vote enshrined Britain's preference for the American security guarantees under the post-War Euro-Atlantic umbrella of NATO. Amongst the myriad socio-political rationales driving the campaign to leave the bloc, Brexit therefore manifested a rejection of structural integration into the EU's ever-closer economic and security union.

Russia's invasion of Ukraine in 2022 altered the trajectory of this calculus, reinforcing the inescapable link between the European security system and British national interests. The return of major war to Europe has seen the aggressor combine conventional warfare with the cyberspace and undersea domains in a 'new-age' strategic competition. Whilst Russia's tactical objective is the acquisition of Ukrainian territories, its strategic ambition amounts to subverting the continent's Euro-Atlantic security umbrella. In doing so, it seeks to displace the US from the security system which has defined European politics since the end of World War II.

Thus far, despite the difficulties, NATO's response has been characterised by its solidarity: the US has funnelled over $75bn into the Ukrainian War

23. A Global Strategy for the European Union's Foreign and Security Policy, 2016, https://www.coe-civ.eu/kh/a-global-strategy-for-the-european-unions-foreign-and-security-policy.

effort;[24] the UK moved decisively to offer European diplomatic leadership; with its *Zeitenwende*, Germany resiled from its decades-long policy of integrating Russia into the continent's economic and, eventually, political matrix; and Eastern and Central European nations have hardened their anti-Russian resolve.

The UK stands geographically remote from the physical destruction of mainland Europe, but is nonetheless threatened by four impacts cascading out of the war. First, the energy crisis instigated by the withdrawal of Russian gas caused a price hike biting domestic commercial and private consumers. Second, the provision of equipment and military assistance to sustain the Ukrainian war effort will inflict costs on the Treasury for years to come. Third, whilst the Ukrainian War has in many ways galvanised the West and injected renewed purpose into NATO, the strain of maintaining this accord is not insignificant. The need for constant allied vigilance in this regard is manifested in President Biden's iterative battle to appease mounting Republican reluctance to supply Kyiv with materiel, and the EU's crisis as Poland, Romania, Slovakia and Hungary challenged the Ukrainian grain export deal. As the war increasingly assumes an attritional nature, it is likely to drag on for years, continuing to disrupt the post-War economic, political and military status quo in deleterious ways.

The fourth impact on the UK concerns its undersea infrastructure, resulting from Russia's growing operational focus on this domain. The following section elaborates on this mounting threat to British maritime and national security.

Europe's undersea strategic landscape

Since the Cold War, the Eastern Atlantic, North Sea, Baltic littoral and High North have all been critical maritime regions of Russo-NATO competition, serving as they do as the essential highway of inter-Alliance communications, energy, commercial shipping and military naval traffic.

The existential imperative of protecting these waters during the Cold War motivated the creation of the SOSUS (later IUSS) system. This was a sophisticated undersea monitoring network, established by the US and its allies, comprising anti-submarine hydrographic and hydroacoustic sensors and patrolling surface vessels. The system's primary objective was twofold: to deny Russian targeting of NATO activity and maritime infrastructure; and to negate the USSR's second-strike system by detecting the presence of ballistic-missile submarines, thus enabling them to be neutralised before launching second-strike attacks. By the Cold War's conclusion, the SOSUS/IUSS system was thoroughly capable of tracking and targeting Soviet submarines that strayed beyond the Barents Sea into the GIUK Gap or North Sea, ultimately shifting the military balance in the West's favour.

Since then, the West has let its undersea monitoring network decline. There are numerous reasons for this – not least the cashing in of the post-1991 peace dividend – but the upshot is that these critical maritime domains are once again exposed to Russian manoeuvring. As Russia has

24. Jonathan Masters and Will Merrows, How Much Aid Has the U.S. Sent Ukraine? Here Are Six Charts, *Council on Foreign Relations*, last updated 8 December 2023, https://www.cfr.org/article/how-much-aid-has-us-sent-ukraine-here-are-six-charts.

been shown to lack the conventional warfare capabilities to overwhelm Europe on its eastern flank, unconventional methods of asymmetric manoeuvre in the maritime domain promise strategic advantage.

On top of the mounting evidence of Russian undersea activity and capability-development (see below), a solid strategic rationale for targeting NATO's undersea infrastructure importunes a greater western response to this undersea threat. Russia has long perceived the Baltic states not as genuine military targets nor irredentist goals, but rather both as a security challenge requiring offensive defence, and as a potential pressure point to weaken NATO.[25] This common strategic determinant underpins all aspects of Russian activity in the Baltics, from sophisticated cognitive warfare (e.g., disinformation campaigns), to covert intelligence operations, to borderland military build-up, and indeed to undersea intelligence-gathering missions.[26]

In order to desynchronise from Russian and Belarussian energy complexes, the Baltic states of Estonia, Sweden, Latvia and Lithuania have spent 20 years establishing a network of energy transmitting power cables with NATO allies: EstLink-1 and -2 connected Estonia and Finland in 2006 and 2014; NordBalt between Sweden and Lithuania in 2015; and the Poland-Lithuania Harmony Link is scheduled to go online in 2028.[27] This will enable the eventual decommissioning of Soviet-era land power cables linking the Baltic allies to Russia and Belarus, resulting in reduced energy dependence for the very calculus exemplified by Russia's weaponisation of its gas during the Ukrainian War.

However, as a NATO report foresaw, a situation would arise where "submarine power cables will play an even greater role in ensuring Baltic energy security",[28] bringing new vulnerabilities in exchange for those of old. Of particular concern is the likelihood of a hybrid Russian relational manoeuvre which coordinates physical and/or cyber operations against critical energy infrastructure and undersea cable networks.[29] Such an occurrence may have been realised last October, when an undersea gas pipeline and telecommunications cable linking Finland and Estonia was damaged by "external activity".[30] Whilst no attribution had been levelled at time of writing, such an attack is well within the strategic calculus of Russia.

Crucially to the UK, this evolving security dynamic brings the Russian threat more immediately to its territorial waters in the Irish and North Seas. For four structural and substantive reasons, we can be confident that the Kremlin will target the North Sea as a priority area for meddling in the West's strategic rear both in the near and longer-term future. This confidence stems from the emergent strategic geography of Russian-NATO relations, partly detailed above and fleshed out as follows.

Firstly, Russia's attempted expansion westward since 2022, coupled with the confirmed and pending NATO accessions of Finland and Sweden respectively, have modified the European security landscape and reasserted the North Sea's position as NATO's northeastern flank. The Ukrainian War jolted Russophobe Baltic states into closer union with NATO and the

25. Timothy Thomas, Russia's Reflexive Control Theory and the Military, *The Journal of Slavic Military Studies* 2004 17 (2).

26. Mark Galeotti, The Baltic States as Targets and Levers: The Role of the Region in Russian Strategy, 2019, https://www.marshallcenter.org/en/publications/security-insights/baltic-states-targets-and-levers-role-region-russian-strategy-0.

27. Lukas Trakimavicius, The Hidden Threat to Baltic Undersea Power Cables, NATO Energy Security Centre of Excellence, 21 December 2021, https://www.enseccoe.org/data/public/uploads/2021/12/the-hidden-threat-to-baltic-undersea-power-cables-final.pdf.

28. Ibid., 5

29. Ibid., 4.

30. Jari Tanner, Finish president says undersea gas and telecom cables damaged by 'external activity', *AP News*, 10 October 2023, https://apnews.com/article/finland-estonia-pipeline-24d6623cf2778464fdb4ef1d-85c70d91.

EU meaning that, in the words of a Nordic intelligence official, Russia's colourful array of operational tools "has only managed to give the Baltic security agencies experience, determination, and budgets".[31] The Kremlin is therefore likely to view the North Sea as a lower-risk area of operation moving forward. As climate change causes ice to melt in the High North, the southwards route along the western Baltic coastline will become increasingly navigable.

Secondly, returning to the terms of base strategic logic, Russia must find ways of confronting the West in a long-term military competition while at a clear disadvantage economically, a more moderate but still relevant disadvantage technologically, and all while under varying degrees of diplomatic isolation. In such a competition against an adversary with more overall resources, Russia as the weaker power must bide its time and pursue actions that are disruptive, imposing a greater relative cost on the West than it expends to conduct these disruptive operations.[32] The North Sea is an ideal spot for this disruption because it is economically and informationally relevant to the West but strategically exposed. The volume of trade, amount of energy investment and power generation, and the communications linkages within the North Sea make it an ideal target for pressure below the threshold of war.

Thirdly, pressure against the North Sea forces the West, both NATO and the European powers in general, to respond to even small threats with larger means. Considering Russia's materiel disadvantage, even the threat of disruption in the North Sea can be used to induce a state of tension in the West. Every sighting of drones and vessels near North Sea oil platforms has prompted a major panic, hacking major data providers has forced the UK to increase its data protection and general cyber capabilities, and most spectacularly, the destruction of the Nord Stream pipeline along with the Shetlands Cable incident indicates the threat to all North Sea critical infrastructure.[33] To this end, the UK's chronic issue during World War II in protecting maritime convoys in the Western Approaches to the North Sea has returned in reincarnated form in critical maritime infrastructure. An imprudent response that does not maximise effort will lead to over-expenditure of resources on domestic resilience that does not actually deter or prevent Russian probing and, worryingly, decreases the proportion of annual spending dedicated to concrete defence measures that will deter and defeat Russian pressure.

Fourthly, while Russia remains below the threshold of active conflict, pre-war cable mapping allows the Kremlin to build its intelligence picture of the UK's critical infrastructure and economic flows, thereby permitting disruption during a major war.[34] It is true that critical infrastructure in the North Sea remains well-known publicly, and that communications cable landing points, pipelines, and energy stations are mapped in the open-source. However, the precise path that different pipelines, and particularly fibre-optic cables or other energy cables take, is often unknown except to the provider that services them. This infrastructure is extremely small, and so can avoid detection by blending into the ocean floor. Conducting

31. Nordic intelligence official, from M Galeotti, The Baltic States as Targets and Levers.

32. Mason Clark, "Russian Hybrid War", *Institute for the Study of War* (Military Learning and the Future of War Series, September 2020), 15-19ff.

33. John Ainger and Michael Nienaber, "North Sea Nations to Work On Infrastructure Security Pact", *Bloomberg*, 24 April 2023, accessed via: https://www.bloomberg.com/news/articles/2023-04-24/north-sea-nations-to-work-on-security-pact-for-infrastructure.

34. "Heightened threat of state-aligned groups against western critical national infrastructure", *National Cyber Security Centre*, 19 April 2023, accessed via: https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups; Mark Scott, "UK warns Russian-aligned cyber groups targeting infrastructure across the West", *Politico*, 19 April 2023, accessed via: https://www.politico.eu/article/uk-warns-russian-aligned-cyber-groups-targeting-infrastructure-across-the-west/.

a large-scale mapping effort to identify and disrupt North Sea energy and communications infrastructure would therefore greatly improve Russian operational intelligence and enable future kinetic pressure against the UK and its allies.

These conditions are informing Russia's sub-threshold strategies vis-à-vis the West. In the case of a major conflict with NATO, the most natural spot to undermine NATO's northeastern line in Scandinavia would be the North Sea. Considering that the ammunition and materiel involved must be moved by ship beyond the first days of a major crisis, the North Sea will serve as the crucial supply link between Scandinavia and transatlantic NATO. It will also provide the Scandinavian powers even greater strategic depth if they, alongside the UK, can leverage their naval forces and operate from this area, at some remove from the most potent short and medium range Russian anti-ship missiles. Pressuring the North Sea during wartime by destroying physical port infrastructure, disrupting British and allied energy supplies, and cutting major communications cables would force the UK and NATO to refocus on homeland and near seas defence, thereby dividing attention and resources desperately needed for high-intensity warfare elsewhere.

Meanwhile, the race towards clean energy production and transmission is placing severe strain on digital and energy interconnector cable supply chains. Manufactures have reached over-capacity with existing orders, which is both causing delays to ongoing projects, and preventing further network expansion. For example, the NeuConnect electricity cable – a 700kmn long line set to open electricity channels between the UK and Germany – is currently four years behind schedule (initially 2024, now expected in 2028).[35] Planned projects linking Denmark and the UK, and France and Spain, are now similarly delayed due to cable market congestion.[36]

With cable supply chains already taut – as demand outstrips supply – costs are soaring, further applying the brakes on future efforts to expand and diversify subsea cable systems. In response, there has been a flurry of planned projects in the UK to reverse the plant closures over the preceding decades.[37] Significant challenges face each of these endeavours, however: the relative lack of process standardisation in the industry prohibits economies of scale from kicking in to drive down manufacturing costs; whilst the global nature of the market engenders stiff competition. It is therefore unclear whether British manufacturing will succeed in rising up to help plug the growing demand gap over the coming years, without greater financial support from the government.

As network diversification is set to prove a decisive factor in mitigating against worsening cable insecurity – and, as a corollary, the insecurity of the systems which depend on it – issues around Euro-Atlantic expansion projects directly compromise our efforts to insulate this critical infrastructure from the Russian threat.

35. OfGem, NeuConnect Britain Limited – Decision on a request for a later regime start date for the NeuConnect interconnector project, 21 March 2022, https://www.ofgem.gov.uk/publications/neuconnect-britain-limited-decision-request-later-regime-start-date-neuconnect-interconnector-project-0.

36. Rachel Millard, Will there be enough cables for the clean energy transition?, *FT*, 30 July 2023, https://www.ft.com/content/c88c0c6d-c4b2-4c16-9b51-7b8beed88d75.

37. XLCC is building an HVDC factory in Scotland by 2027; Sumitomo Electric Industries also in Scotland; Global Interconnection Group is considering a new plant in the Port of Tyne; and Manufacturer JDR Cables is building one in Northumberland.

Russian undersea doctrine and activity

The undersea domain is integral both to Russian maritime doctrine and the structure of its military and intelligence naval operations. The Kremlin's maritime special operations are housed at the intersection of the navy-intelligence domain, combining the Intelligence Directorate of the Main Staff of the Russian Navy, the GUGI (the Deep-Sea Research Group), and the GRU. Cross-pollination of personnel between these units provides a highly-specialised hybrid force with naval and intelligence experience.[38] Whilst the Russian Navy performs a broad operational role, it is the Russian MoD and the GRU which, through the GUGI, control everyday activity, both the defensively-minded protection of Russia's critical maritime infrastructure and waters, and the nefarious mapping and tapping of NATO assets. This is informed by the sub-threshold remit of Russia's military strategy, SODCIT, whose stated aim is to degrade western capabilities in the grey zone by targeting critical infrastructure.[39] By probing the military-economic capacities of adversaries through their infrastructure, SODCIT seeks to inflict material and psychological damage with no risk to life, thus reducing the risk of unintended escalation.[40]

As the key functionary in SODCIT's maritime purview, the GUGI is responsible for expeditionary exploration and exploitation. Its remit has expanded in recent years, now including laying Russia's own submarine-assisting sensor networks (the Harmony network), policing Russian territorial waters, and testing the Poseidon nuclear torpedo. These sizeable operational demands on a force which is difficult to expand rapidly,, due to the high bar placed on expertise and naval experience, may constrain the GUGI's expeditionary capacities in the near-term. That said, it still possesses a suite of sophisticated equipment which can interfere and damage exposed maritime infrastructure at great depths, which should guard the UK from relying upon Russia's internal constraints to action. In any case, the expedited purchase and development of the British Royal Navy's RFA Proteus (see below), and the establishment of a new NATO undersea centre with full-time personnel – both on the back of increased Russian activity – demonstrates that Moscow is already effectively imposing costs on the West in the undersea domain.

Russia's Maritime Doctrine of 2022 offers further guidance on the Federation's wider undersea objectives. The document openly states the national ambition of becoming "a great maritime power", leveraging its geographical advantage of occupying more than half of the Arctic coastline.[41] The grand strategy rationale behind this ambition is to sustain Russia's socio-economic development in the 21st century,[42] necessitating an expanded forward presence in the Arctic, Baltic and Atlantic seas, in order of priority. Throughout the Doctrine, NATO – particular its northern member states – is articulated as a direct strategic threat, owing to the proximity of each sides' maritime bastions, naval stations and maritime and energy routes. This doctrinal rationale explains Russia's "dose damage" tactic,[43] where seemingly random and unpredictable exploration and exploitation of high-threat NATO areas signals its offensive capabilities.

38. Sidharth Kaushal, Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure, *RUSI*, 25 May 2023, https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.

39. Michael Kofman et al., Russia Military Strategy: Core Tenets and Operational Concepts, *CAN*, August 2021, https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf, 68.

40. Ibid., 70.

41. Gonzalo Vázquez, 2022 Russian Maritime Doctrine: Implications for NATO & the Future of Great Power Competition in the Arctic, *The Arctic Institute*, 11 April 2023, https://www.thearcticinstitute.org/2022-russian-maritime-doctrine-implications-nato-future-great-power-.-arctic/.

42. Maritime Doctrine of the Russian Federation, translated by Anna Davis and Ryan Vest, accessed *US Russia Maritime Studies Institute*, 31 July 2022, https://dnnlgwick.blob.core.windows.net/portals/0/NWC-Departments/Russia%20Maritime%20Studies%20Institute/20220731_ENG_RUS_Maritime_Doctrine_FINALtxt.pdf?sv=2017-04-17&sr=b&si=DNNFileManagerPolicy&sig=2zUFSaTUSPcOpQDBk%2FuCtVnb%2FDoy06Cbh0EI5tGpl2Y%3D.

43. Dr Sidharth Kaushal, in Corrected oral evidence: The Arctic, International Relations and Defence Committee, *HMG*, 5 July 2023, 11.

This intends to deter states from participating in future conflict owing to Russia's projected ability to strike critical national infrastructure at will.

Recent Russian subsea activity in these regions therefore conforms to the diktats of its maritime doctrine and the characteristics of the strategic environment. This convergence of stated intention, strategic merit, and the recent uptick in confirmed acts, is what distinguishes the threat of the last few years from previous eras of Russian sub-surface activity. Norwegian Rear Admiral Rune Andersen commented last year on an escalation in Russian submarine patrols around his nation's Arctic coast, which are both "more unpredictabl[e]" and "more aggressive" than before.[44] In January 2022, multiple sections of fibre-optic cables in Norwegian waters were severed. In the Baltic, over 50 Russian vessels have been observed in unusual operational patterns around high-density cable areas in recent years.[45] Most recently, suspicious damage was caused on the same day in October to two Baltic cables linking Finland and Estonia,[46] and Sweden and Estonia,[47] with allegations levelled at Russian sabotage following sightings of Russian vessels at the same time near the incident. Climate change is destined to drive further activity in these northern extremities, by opening up shorter routes to Europe which will soon be navigable for six months of the year.[48]

Most directly threatening to the UK is the rise in activity further south in the North Sea. The GUGI's special purpose intelligence-collection ship, *Yantar*, was identified near a major fibre-optic cable in the Irish Sea in August 2021, before entering the English Channel the following month. In 2022, Russia's oceanographic research vessel, the Admiral Vladimirsky – which is fitted with equipment for underwater surveillance, as well as electronic (ELINT and signals (SIGINT) intelligence – sailed between the Scottish northeast coast and the Baltic Sea.[49] During the journey, the vessel remained in the Moray Firth for three days, raising concerns that it may have been attempting to intercept communications from RAF Lossiemouth.

Meanwhile, the still-unattributed cutting of two subsea cables near the Shetland Islands in 2022 coincided with the sighting of a Russian scientific research ship in the vicinity. Also that year, the Royal Navy reported that one of its submarine hunters had tracked two Russian submarines along their southward journey from the Arctic.[50] Russian activity came even closer last August, as a group of surface and sub-surface vessels were tracked in the English Channel.[51]

That such missions are almost-undoubtedly cable-mapping exercises was confirmed by Norwegian intelligence service sources and analysts earlier last year.[52] The North Sea is the fundamental backbone of the Euro-Atlantic fibre-optic cable system, the necessary junction through which all cables must pass which connect America to Europe (e.g., AC-1), and the GIUK, the UK, and the southern continent to northern Europe (e.g., DANICE, NSC, and Tampnet respectively).

44. Tom Costello et al., Norway watches warily as Russian subs and aircraft step up Arctic patrols, *NBC*, 23 March 2023, https://www.nbcnews.com/news/world/norway-russian-submarines-planes-military-ukraine-arctic-rcna76368.
45. Russian spy ships mapping undersea infrastructure in the North Sea, *Navy Lookout*, 20 April 2023, https://www.navylookout.com/russian-spy-ships-mapping-undersea-infrastructure-in-the-north-sea/.
46. Jon Henley, Nato vows to respond if Finland-Estonia gas pipeline is deliberate, *The Guardian*, 11 October 2023, https://www.theguardian.com/world/2023/oct/11/nato-vows-to-respond-if-finland-estonia-gas-pipeline-damage-is-deliberate.
47. Ido Vock, Sweden investigating damage to Baltic undersea cable, *BBC News*, 18 October 2023, https://www.bbc.co.uk/news/world-europe-67138269.
48. Arctic Council, Navigating the Future of Arctic Shipping, 10 May 2021, https://arctic-council.org/news/navigating-the-future-of-arctic-shipping/.
49. Russian spy ships mapping undersea infrastructure in the North Sea, *Navy Lookout*.
50. Royal Navy tracks movements of Russian submarines into the North Sea, *Royal Navy*, 22 July 2022.
51. Royal Navy and RAF track Russian vessels in waters close to the UK, *Royal Navy*, 31 August 2023, https://www.royalnavy.mod.uk/news-and-latest-activity/news/2023/august/31/230831-portland-and-tyne-track-russian-ships.
52. Niels Fastrup et al., Disclosure: Russian spy ships are preparing possible sabotage against offshore wind turbines, gas pipes and power cables in Denmark and the Nordics, *DR*, 19 April 2023, https://www.dr.dk/nyheder/indland/moerklagt/afsloering-russiske-spionskibe-forbereder-mulig-sabotage-mod.

Source: https://www.submarinecablemap.com/

The high cable density, relative ease of access, and strategic vulnerability of NATO all combine to incentivise Russia into targeting the North Sea and GIUK Gap in both the sub-threshold and above-threshold domain. Ongoing mapping – and, most likely, occasional sabotaging – missions afford four strategic benefits to Russia in their current level of frequency and depth: valuable intelligence-collection on western infrastructural systems and their weak-points; capability signalling to encourage the West to divert attention and resources from the ongoing Ukrainian War to the maritime domain; technical and operational trial runs at low escalatory risk to lend guiding experience for any future major conflict; and general confusion of overall assessments of Russian strategy and domain prioritisation.

This threat is compounded by concerns that British capabilities stationed in Scotland are already over-stretched, and likely to become more so given Russia's strategic re-focus on the Arctic and Atlantic, and ice melt in the High North freeing up the northern passages.[53] The House of Commons Scottish Affairs Committee expressed repeated concerns that HMNB Clyde and RAF Lossiemouth do not have the naval and air capacity to increase maritime patrolling in the increasingly exposed North Sea and GIUK Gap.[54] Air Vice-Marshal Andrew Roberts claimed in 2018 that the UK's fleet of nine P-8A Poseidon Maritime Patrol Aircraft is insufficient to fulfil the range of existing tasks, arguing the need for 16 to achieve necessary coverage.[55]

As well as more equipment, there will be a need for more deployment capacity from Scotland, which would necessitate the development of other bases. Scapa Flow has been touted as a prime candidate for enabling enhanced GIUK Gap deployment.[56] In addition to shoring up our own defences, enhanced forward presence would enable the UK – alongside its partners – to launch expeditionary missions nearer Russian waters. As the GUGI's vast operational remit already places strain on its capacities, this could tip the balance of its offensive-defensive balance in favour of the latter, thereby further reducing the threat it poses to our critical maritime infrastructure.

53. For example, James Heappey MP, oral evidence given to the House of Lords International Relations and Defence Committee, 5 June 2023 (Session 2022-23), 37, https://committees.parliament.uk/publications/42335/documents/210453/default/.

54. House of Commons Scottish Affairs Committee, *Defence in Scotland: the North Atlantic and the High North*, 21 July 2023, 32-33.

55. Air Vice-Marshal Andrew Roberts (Retd), Written evidence submitted to Defence Committee 'Beyond 2 per cent: A preliminary report on the Modernising Defence Programme Contents', 18 June 2018, accessed https://publications.parliament.uk/pa/cm201719/cmselect/cmdfence/818/81806.htm#footnote-067-backlink.

56. Dr Marc DeVore, Ibid., 32.

Allied responses in the Euro-Atlantic

The EU, NATO and its ancillary Framework Nations Concept blocs have in recent years begun to respond multilaterally to this Euro-Atlantic threat landscape.

NATO

Recent sightings and probable incidents involving Russian undersea activities have spurred a swift security refocus from NATO to integrate the sub-surface domain into its maritime purview. Its *Protecting Critical Maritime Infrastructure* report last year identified the bloc's sizeable surface and sub-surface exposure to hostile acts, primordially by Russia (but also Iran and China), which "has a motive to conduct such operations given the Russian Federation's stated aims to undermine Allies' security".[57] David Cattler elaborated on the immediacy of the threat, where:

> *"Allied critical infrastructure could be targeted by Russia as part of its war against Ukraine or in any future conflict. Russia is actively monitoring Allied critical infrastructure, recognising that the ability to compromise the security of energy, information and financial systems provides a significant strategic advantage".*[58]

The report proceeds with an assessment of current defence capabilities. It concludes with a list of the missing key technical and tactical ingredients of an effective operational effort to deter such acts by denial, including bolstering the Alliance's sensor network, AUV and UUV fleet, and coordinated allied patrolling of the North and Baltic seas.

In conjunction with this report, NATO launched the CUICC in Brussels, a unit which coordinates the strategies of member states in the undersea cable domain. This cell joined the existing MARCOM centre in Northwood, which serves as the command centre for multilateral operations. Whilst it might be useful to stand up a specific diplomatic centre – and the increased attention on the undersea domain is always welcome – the existence of two coordinating centres risks bifurcating the chain of command, thereby sapping the clarity out of the NATO approach. Great care must be taken to sustain the Organisation's strategic efficiency.

EU-NATO Cooperation

In line with the broad scale of the critical maritime infrastructure threat, the EU and NATO have become cognisant of their mutual security imperatives, and the resultant need for inter-bloc strategic partnership. The launch of the EU-NATO task force on resilience of critical infrastructure last year – which now comprises the sixth spoke of the EU-NATO joint dialogue wheel, launched in 2016 –[59] seeks to coordinate capability-building and operational command between the blocs. Whilst stressing that critical maritime infrastructure resilience remains primarily a national responsibility for member states,[60] the task force's report confirmed the blocs' shared threat perception in four critical sectors: energy, transport, digital infrastructure and space.[61] Policy recommendations were offered to

57. NATO, 2023, https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.
58. Lee Willet, NATO Steps Up Response To Clear and Present Undersea Infrastructure Risk, 16 May 2023, https://www.navalnews.com/naval-news/2023/05/nato-steps-up-response-to-clear-and-present-undersea-infrastructure-risk/.
59. EU-NATO Cooperation, *EEAS*, March 2022, https://www.eeas.europa.eu/sites/default/files/documents/2022-03-24-EU-NATO-COOPERATION-NewLayout.pdf.
60. EU-NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report, June 2023, 3.
61. Ibid., 8.

foster a cooperative response which involves the exchange of best practice between civilian and military actors.

The document's largely diagnostic and conceptual nature, however, meant that it fell short of offering a clear, actionable roadmap. Without a rapid follow-up in the vein of strategically-orientated defensive capability-building measures – such as launching a centralised inter-bloc command centre, or creating an integrated equipment-sharing platform – the taskforce is unlikely to bolster the Euro-Atlantic alliance's resilience to hostile acts against its critical maritime infrastructure.

Following the suspected Russian interference in Baltic cables in October, the EU announced a plan to boost investment in diversifying its cable network, beginning in 2024.[62] Nonetheless, an initial draft reveals that the policy is likely to be confined to a non-binding recommendation for member states, falling short of the necessary impetus required by this critical immediate strategic challenge.

The fundamental question which arises from the burgeoning EU-NATO cooperation asks what the strategic merits of pooling the blocs' strategic thinking, resources and operations are. Bringing Austria, Cyprus, the Republic of Ireland (the ROI), Malta and Sweden (whose NATO accession is imminent anyway) ostensibly expands the multilateral defensive framework, but there are limits to their operational and tactical contributions: Austria is landlocked; Cyprus is plagued by political division; Malta's stance on Russia is nebulous; and the ROI maintains its post-World War II military neutrality doctrine. Nonetheless, any multilateral endeavour which aligns partners more closely from the strategic and, eventually, operational angle has the potential to be strategically advantageous, as long as it elicits a high degree of commitment from each and every participant.

One aspect of this fledgling multilateral framework with critical strategic implications for the UK's undersea cable defence is the ROI's participation in NATO efforts through EU collaboration. The ROI has hitherto maintained a doctrine of neutrality since World War II. As well as limiting its contribution to UN peacekeeping missions with the strict 'triple lock' criteria, this doctrine has kept the ROI out of NATO. As Policy Exchange's recent paper, *Closing the Back Door*,[63] demonstrates, decades of underinvestment in the Irish Defence Forces and intelligence apparatus has left the ROI without the equipment, nor operational and technical capacity, to protect the transatlantic critical maritime infrastructure which passes through its waters.

In recent years, the dial has gradually shifted on the ROI's defence calculus. This has above all been catalysed by a growing awareness of the vulnerability of undersea infrastructure in its waters, including three quarters of all cables running throughout the northern hemisphere. As a result, the government has embarked upon a wholesale reform of its military and security apparatus, and is slowly engaging more in the EU's mutual security and defence initiative, the Permanent Structured Cooperation (PESCO).

Between joining in 2017 and 2021, the ROI played a minimal role in

62. Mathieu Pollet, EU looks to boost secure submarine internet cables in 2024, *Politico*, 11 October 2023, https://www.politico.eu/article/eu-looks-to-boost-secure-submarine-internet-cables-in-2024/.

63. Marcus Solarz Hendriks and Harry Halem, *Closing the Back Door: Rediscovering Northern Ireland's Role in British National Security*, *Policy Exchange*, 5 February 2024.

the initiative, participating in only one of PESCO's first 60 missions. Since the recent increase in Russian activity in the Atlantic, however, the ROI has observed 19, and participated in four, PESCO joint exercises, with domestic media noting that escalating Russian sub-surface activity around its waters "has jolted the Irish system out of a long slumber".[64] That said, the ROI inexplicably still does not participate in PESCO's critical seabed infrastructure protection project (CSIP),[65] likely a result of the Naval Services' deficiency in undersea equipment and expertise.

The ROI has also veered away from its aversion to NATO engagement in the field of maritime security. Last February, Dublin partook in a NATO REP(MUS) naval exercise involving unmanned submersibles and testing the interoperability of member states for the first time. On the back of this exercise, NATO's Deputy Secretary General Mircea Geoană encouraged Dublin to partner with NATO's new CUICC.[66] This month, NATO and the ROI signed a new agreement, the Individually Tailored Partnership Programme (IPTT), to boost cooperation against threats to undersea infrastructure and cybersecurity.[67]

The transnational nature of undersea cable security confirms the clear strategic rationale behind converging the ROI's defensive system with its partners, for no one state can unilaterally protect its sub-surface fibre-optic architecture. It is no secret that the ROI's economic reliance on the financial, and increasing tech, sectors are entirely reliant upon the undersea cables which connect it to the outside world. With the Irish government stating its future ambition "to position Ireland as a central hub in an East-West corridor",[68] the need to contribute more to an integrated allied defensive system will become more urgent than ever. This therefore represents a politico-security opportunity for multilateral western cooperation of critical importance for the present and future, and one which must be encouraged. Without significant progress in upgrading the Irish Defence Forces, however, the ROI will remain incapable of contributing sufficiently to multilateral initiatives aimed at defending undersea infrastructure.

To reiterate, without full integration of the Irish Sea and Western Approaches to the North Sea into the West's maritime comprehensive defence framework, these regions shall remain the UK, and its allies', weak point against Russian maritime hostility. This state of affairs endangers the collective security of allies and partners.

UK Joint Expeditionary Force (JEF)

As part of the NATO Framework Nations Concept, JEF marshals the forces of the UK, Denmark, Finland, Estonia, Iceland, Latvia, Lithuania, the Netherlands, Sweden, and Norway into an ad hoc military partnership. The JEF partnership has configured the High North, Baltic and North Sea into the essential linking tissue between member states. Initially, this collaboration was limited to its military nature, but recent Russian activity has begun to expand the JEF's remit into the realm of critical maritime infrastructure. The JEF's June 2023 meeting in Amsterdam resulted in a joint statement pledging renewed focus on undersea capabilities to combat

64. Tony Connelly, Crossed Wires: Irish neutrality and undersea cables, *RTE*, 19 June 2023, https://www.rte.ie/news/ireland/2023/0617/1389644-neutrality/.

65. EU Permanent Structured Cooperation (PESCO), Critical Seabed Infrastructure Protection (CSIP), https://www.pesco.europa.eu/project/critical-seabed-infrastructure-protection-csip/.

66. Tony Connelly, Crossed Wires.

67. The Journal, Ireland in new agreement with Nato to counter potential threats to undersea infrastructure, 9 February 2024, https://www.thejournal.ie/ireland-nato-agreement-cyber-threats-undersea-infrastructure-6295188-Feb2024/.

68. International Connectivity for Telecommunications Consultation – Key Findings 2021, Irish Dept of the Environment, Climate and Communications, 2021, 15.

Russian acts in this domain, involving further sharing of ISR (Intelligence, Surveillance and Reconnaissance) to promote common situational awareness.[69] Importantly, the statement asserted JEF's integration into wider NATO efforts, indicating an appropriate eye on the need to develop a broad multilateral system to defend the undersea domain.

As it is understood that the JEF was always conceived to operate in all domains,[70] and indeed has done so, it has great potential to be a vital component of a multilateral critical maritime infrastructure defence system. In acknowledgement of this, the JEF conducted its first seabed warfare deployment at the beginning of this year – under the leadership of the UK – across North Atlantic waters.[71]

The JEF has great potential in this domain, if it can convert ad hoc initiatives into a concerted strategy. Sweden and Norway bring leading shallow water expertise and capabilities, as they routinely cope with overt and covert Russia incursions in littoral regions. As the British Royal Navy has greater experience in oceanic, blue water operations, the two skill sets can be combined to generate effective comprehensive defence in the region. The JEF could also grant the UK increased operational access to the High North through allied cooperation, projecting its power to police the northward approach and enforce UNCLOS in this region. Crucially, JEF's status as a NATO Framework Nations Concept also eases its integration into the organisation's overall maritime security architecture, and so presents the UK with another opportunity to establish itself as a driver of this overarching multilateral endeavour.

Unilateral and Bilateral Steps

Some member states have made important inroads in the pursuit of greater undersea security. As nations at the vanguard of strategic thinking and operational capabilities in the full extent of the maritime domain, France and Italy are prime candidates for expanded bilateral collaboration with the UK.

France stands out in this regard due to the 2021 *Seabed Warfare Strategy* developed by its Ministry of Armed Forces. The document is the first attempt by a western ally to position the seabed as integral to national security, reasoning that its clear relevance to the state's fundamental civil and military systems demands a whole-of-state strategy orchestrated by the government's military department. The *Strategy* exhibits an astute grasp of the strategic logic of the sub-surface domain, from its attractiveness to hostile actors seeking asymmetric advantage in hybrid warfare paradigms, to the trifurcated nature of competition into 'knowledge of the seabed', 'monitoring capacity', and 'military action'. What distinguishes France from its western counterparts is its success in generating targeted, actionable responses to its assessed security frailties (in contrast to the EU-NATO task force, for example), ultimately providing the government with a task-list of capability enhancement to overcome them.

The UK and France face similar strategic landscapes in the undersea domain, which encourages stronger bilateral collaboration on the

69. Joint statement by Joint Expeditionary Force Ministers, June 2023, *HMG*, 13 June 2023, https://www.gov.uk/government/news/joint-statement-by-joint-expeditionary-force-ministers-june-2023.

70. Air Chief Marshal Lord Peach et al., Stretching the Joint Expeditionary Force: An Idea for Our Times, *RUSI*, 8 September 2023, https://www.rusi.org/explore-our-research/publications/commentary/stretching-joint-expeditionary-force-idea-our-times.

71. Dr Lee Willett, UK-Led JEF Task Force Conducts First Seabed Warfare Deployment, *Naval News*, 3 January 2024, https://www.navalnews.com/naval-news/2024/01/uk-led-jef-task-force-conducts-first-seabed-warfare-deployment/.

operational and strategic levels. Both are exposed on the western side to oceanic Atlantic approaches, and northwards through the North Sea, representing mutual structural vulnerabilities which could be exploited by Russian vessels travelling from the Arctic. Both nations also have extensive interests in the Pacific, which should form the foundational basis of collaboration in that theatre as well. The Royal Navy has already started cooperating closely with France in the sub-surface maritime domain, through the joint minehunting programme, Artemis Trident (see below).

The ongoing strengthening of ties between London and Paris, following a cooler period after Brexit, presents a window of opportunity to synthesise mutual commitment to undersea cable security. The protection of critical maritime infrastructure upon which both states depend could, for example, be incorporated into the existing Anglo-French maritime and port security treaty.[72] Alternatively, the bilateral Combined Joint Expeditionary Force (CJEF) could be expanded to these ends, such as by developing undersea interoperability and platforms for deploying task forces to respond to critical maritime infrastructure incidents. France has already signalled its capability acquisition and operational objectives in its *Seabed Warfare* strategy, particularly in the development of deep-sea ROV and AUV vehicles fitted with ultra-low frequency acoustic propagation. The UK should bear these emerging strengths in mind when developing its own R&D and technical enhancement programmes, in order to add complementary material value to its burgeoning allied defensive framework.

As for Italy, its creation of the National Subsea Hub in La Spezia in 2022 warrants attention. Under the supervision and control of the Navy, the centre has been allocated €2mn/year to develop knowledge of the seabed through scientific exploration and mapping.[73] Housing the Hub within the Italian Navy demonstrates an equally strategic mindset towards the seabed similar to that of France, and indeed the Italian government has since defined the subsea world as a military, rather than maritime, domain.[74] Appropriately, Italy has offered the Hub's research and operational capacities to NATO, again to harness multilateral resilience in the sub-surface domain. The Italian Navy has also signed an information-sharing contract with the nation's largest internet provider. On top of providing the much-needed commercial data to military operations at sea, this provides the military with an unclassified evidence base which can be shared and disclosed, crucial to attributing blame for intentional exploitation. This provides a blueprint for the public-private partnership which the UK must establish to defend its critical maritime infrastructure.

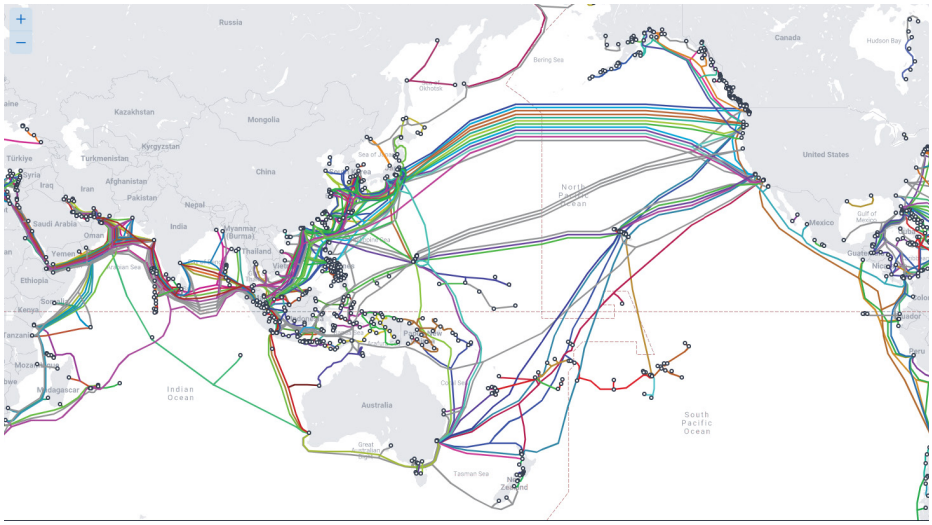
72. FCDO, UK/France: Agreement on Cooperation in Matters relating to Maritime and Port Security, 11 May 2022, https://www.gov.uk/government/publications/ukfrance-agreement-on-cooperation-in-matters-relating-to-maritime-and-port-security-and-specifically-in-relation-to-passenger-vessels-in-the-chann.

73. Gabriele Carrer, The National Subsea Hub is Born, *Drass*, 21 December 2022, https://www.drass.tech/2022/12/22/national-subsea-hub-is-born/.

74. Elio Calcagno and Alessandro Marrone (ed.), The Underwater Environment and Europe's Defence and Security, *Istituto Affari Internazionali*, https://www.iai.it/sites/default/files/iai2313.pdf.

The Indo-Pacific security landscape

The Indo-Pacific cable network



Source: https://www.submarinecablemap.com/

The Indo-Pacific has, due to Sino-American competition, quickly emerged as the globe's geopolitical fulcrum. Although the UK is over 6,000 miles away from the South China Sea, the impact of this theatre on our strategic and diplomatic interests was stated indefatigably by the *Integrated Review* of 2021, which implemented the strategic rationale prescribed by Policy Exchange's 2020 paper, *A Very British Tilt*.[75] The *Integrated Review Refresh* of 2023 bolstered its predecessor's strategic step change with a coherent, well-argued analytical framework for British foreign and defence policy's eastward pivot. As the global maritime hub – with $3.5tn in trade passing through the South China Sea each year,[76] East-Asia Pacific trade consistently accounting for 30% of total global trade,[77] and generates almost half of the global manufacturing output[78] - the UK's economy and national security is closely tethered to its enduring stability. This therefore came as a welcome reassessment of the UK's grand strategy, and how to pursue our strategic objectives across multiple theatres.

The West orchestrated the development of the region's economic-security system following World War II for strictly defensive purposes: namely to cultivate an open international trade ecosystem which served the West's prosperity and isolated the Soviet Union.[79] Following the collapse of the USSR, the West pursued an open-access policy in its Eurasian system under the neoliberal assumption that economic integration would generate convergent state interests, thereby deterring would-be aggressive powers. It was this strategy which enabled – and indeed encouraged – China's entry into the global economic system, joining the WTO in 2001 and quickly supplanting the West as the 'factory of the world'. The success of this Asia-Pacific integration is attested by the concept of 'Chimerica', a neologism coined for the symbiotic economic relationship established

75. Policy Exchange, A Very British Tilt, 22 November 2020.

76. Shannon O'Neil, *The Globalisation Myth: Why Regions Matter*, 2022, 6.

77. Ibid., 7.

78. Combining date from East Asia & Pacific Manufacturing Output 2004-2023, https://www.macrotrends.net/countries/EAS/east-asia-pacific/manufacturing-output#:~:text=East%20Asia%20%26%20Pacific%20manufacturing%20output%20for%202022%20was%20%247%2C595.08B,a%2020.13%25%20increase%20from%202020, and World Manufacturing Output 1997-2023, https://www.macrotrends.net/countries/WLD/world/manufacturing-output#:~:text=Data%20are%20in%20current%20U.S.,a%202.88%25%20decline%20from%202019.

79. Marc Trachtenberg, Assessing Soviet Economic Performance During the Cold War: A Failure of Intelligence?, *Texas National Security Review*, 1:2 (March 2018), 77-80.

between China and the US in these years.

As Sino-American tensions mount, the foundations of this intercontinental system are at stake, and so too is the stability of the global economic system which it underpins writ large. It is far beyond the remit of this paper to assess the full implications of these developments, but those pertaining to undersea cable security in the region are detailed as follows.

Defensive and offensive cable postures

In the absence of conflict between China and the US, the same strategic rationale applies to the Indo-Pacific as to the Euro-Atlantic. Offensive actions by an economically and technologically capable hostile actor – China, as opposed to Russia – would endanger the digital communications passing between western-allied states. In the present sub-threshold context, Beijing will continue to gather information on adversaries' cable networks which, as in the Euro-Atlantic, are currently poorly defended.[80] This would engender tactical and operational options suited to asymmetric hybrid warfare, seeking to disrupt the US' burgeoning mosaic of regional security partnerships. The unattributed yet highly suspicious attack on two cables linking Taiwan and Matsu Islands last February indicates the likely direction of travel in this regard.[81] Cognisant of this threat, the Quad alliance (the US, Japan, Australia and India) launched a Quad Partnership for Cable Connectivity and Resilience initiative last July, pooling technical expertise and operational coordination to counter future Chinese sub-surface activity.

A key point of departure from Russia's undersea strategy is China's focus on its own cable resilience system. There are two components to this: the formation of a sophisticated A2/AD system in Chinese territorial waters around its own maritime bastion to neutralise hostile offensive capabilities; and the development of an alternative, insulated cable network in case of a future need to de-couple from the region's incumbent western-owned one. These measures are constituent parts of the CCP's emerging operational concept, Multi-Domain Precision Warfare, which seeks to align its forces and capabilities from cyber to space to compete with the US across all domains.[82]

As part of its wider effort to bolster its land and sea defensive framework, the CCP has been developing cable monitoring technology since the 1990s. As early as 2002, the PLA launched a self-developed undersea cable-laying system, and has regularly supplemented this with new monitoring ships and cutting-edge sensor devices.[83] China's endeavours to this end have been compared to the US SOSUS system of undersea detection which, as noted above, essentially single-handedly transformed the strategic balance in the Euro-Atlantic maritime domain during the Cold War.[84]

What is more, the CCP's regional strategic aims blur the lines between defensive and offensive sub-surface capacities in the South China Sea. China is now believed to be nearing the completion of an 'underwater great wall' in the contested waters of the South China Sea.[85] Fitted with

80. Joe Brock, U.S. and China wage war beneath the waves – over internet cables, *Reuters*, 24 March 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

81. Huizhong Wu and Johnson Lai, Taiwan suspects Chinese ships cut islands' internet cables, *AP*, 18 April 2023, https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70.

82. US Department of Defence, Military and Security Developments Involving the People's Republic of China, Annual Report to Congress, 2023, 10-11; 59.

83. Eli Huang, China's Cable Strategy: Exploring Global Undersea Dominance, *Real Clear Defence*, 4 December 2017, https://www.realcleardefense.com/articles/2017/12/04/chinas_cable_strategy_exploring_global_undersea_dominance_112720.html.

84. Carl Thayer, quoted in James Griffiths, Beijing plans underwater observation system in South China Sea, *CNN*, 30 May 2017, https://edition.cnn.com/2017/05/29/asia/south-china-sea-underwater-observation-system/index.html.

85. Catherine Wong, 'Underwater Great Wall': Chinese firm proposes building network of submarine detectors to boost nation's defence, *South China Morning Post*, 19 May 2016, https://www.scmp.com/news/china/diplomacy-defence/article/1947212/underwater-great-wall-chinese-firm-proposes-building.

a comprehensive ocean-floor acoustic sensing system around China's coastline, it will firstly serve to deter covert sub-surface operations in the Chinese maritime bastion in the advent of a Sino-American Air-Sea Battle. Secondly, enhanced knowledge of the region's seabed via defensive mapping would concomitantly provide the intelligence necessary to conduct offensive operations, not least towards Taiwan, which serves as the on-site centre of ten cables passing on to other Asia-Pacific countries. Diminishing the scope for offensive US actions generates an asymmetric advantage in the same theatre for China to conduct its own aggressive acts. Furthermore, threatening a robust Chinese defensive framework would necessitate the US spending more time and money on the development of increasingly sophisticated offensive capabilities, diverting resources from its own defence and thus leaving them vulnerable. The undersea cable dimension thus promises to offer China a potentially devasting offensive avenue in the case of contestation over and around Taiwan.

Looming cable network bifurcation

Another essential development in the Indo-Pacific's undersea domain is China's quest to establish an alternative cable network owned, controlled and maintained by itself. This ambitious programme began in earnest in 2015 with the launch of the Digital Silk Road which – in addition to fostering telecommunication and technological partnerships built upon a new inter-continental infrastructure system across Asia, Europe and Africa – is constructing a Chinese-owned undersea cable network beyond the reach of the US and its allies. The latest instalment of mass investment arrived last April, as Chinese state-owned telecom firms pledged $500mn to develop one of the most far-reaching cable systems in the globe.[86] This came on top of rapid previous success in upending the incumbent, decades-old monopolisation of international networks by French, American and Japanese companies, when Huawei Marine captured one fifth of the global undersea cables market by 2019.[87]

As the US woke up to China's intention of subverting the post-World War II western economic and digital superstructures, it moved to restrict Beijing's infrastructural manoeuvring. The Trump administration created the Clean Network initiative to restrain the participation of Chinese entities in cable-laying, with early successes in blocking HMN Tech (which absorbed Huawei Marine following western sanctions against the telecom conglomerate) out of numerous projects, notably the Pacific Light Cable Network linking the Philippines and Taiwan.[88]

Nevertheless, the bifurcation of global cable networks along geopolitical fault lines remains a distinct future possibility. China is having success in leveraging the reluctance of regional powers to pick sides in Sino-American rivalry, in order to enforce the participation of HMN Tech and other Chinese companies in new cable projects. This tenacity is unsurprising given the strategic imperative of insulating itself from hostile acts, as an unnamed Chinese official noted how "the South China Sea is one of the most critical sea areas in China's military strategy. Every link

86. Joe Brock, Exclusive: China plans $500 million subsea internet cable to rival US-backed project, *Reuters*, 6 April 2023, https://www.reuters.com/world/china/china-plans-500-mln-subsea-internet-cable-rival-us-backed-project-2023-04-06/.

87. Anna Gross et al., How the US is pushing China out of the internet's plumbing, *FT*, 13 June 2023, https://ig.ft.com/subsea-cables/#:~:text=There%20are%20more%20than%20500,landing%20stations%20around%20the%20world.

88. Ibid.

and component of the infrastructure must be controllable".[89]

Thus, China poses a distinct, greater strategic challenge to Russia. The latter's undersea objectives are twofold: to secure the digital channels on which it relies; and to exploit and undermine those of the West. The former, on top of developing capabilities on these fronts, is also establishing a means of monitoring and controlling the digital communications of other states which use these new Chinese cable networks. This will afford Beijing effective means of surveilling sensitive information, which could be used for a wide array of strategic ends.

Further complicating this ongoing quest for cable autonomy and defensive resilience is the operational reality of maintenance. There are only 60 cable-repairing ships worldwide, owned predominantly by private entities.[90] The issue of access to damaged cables is thus likely to become hostage to geopolitical competition, as states could either withdraw the repair services of their nationally domiciled companies, or block access to cables in their vicinity to missions from other nations. Such considerations render the insulation of cables immensely difficult, exposing them further to the strategic posturing of warring powers.

Unlike the Euro-Atlantic, this landscape does not concern British territorial waters or domiciled critical infrastructure. Nonetheless, the UK has specific interests in Indo-Pacific cable security, which are at stake in rising competition with China. Firstly, the interconnected nature of the global financial system prevents any disruption from remaining localised, as severed digital channels impede transactions between banks in the affected region and elsewhere. Thus, no state can insulate its economy and financial sector entirely from destabilising developments in other regions.

More importantly, the Indo-Pacific is an area of high trade growth for the UK. The UK's trading relationship with the Indo-Pacific reached over £250bn in 2022.[91] Meanwhile, the combined GDP of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) bloc amounted to £12tn in 2022.[92] As Britain's accession to the CPTPP – enabled by its departure from the EU – is an economic pillar of the Indo-Pacific tilt, strengthening ties with these states will breed vested strategic interests in regional stability and critical infrastructure security.

The second category of British interests in the Indo-Pacific is its security and intelligence pacts. As island nations, Australia, Japan and New Zealand share the UK's total reliance on ocean-crossing fibre-optic cables in the absence of overland routes. Partnerships with these nations therefore do not differ in any way from other modern connectivity structures in the way that their constituent digital modes of communication depend on undersea cables. They are therefore equally exposed to China's various endeavours in the sub-surface maritime domain, whether that be crude cable damage – as may have been exemplified in the Matsu incident this year – or covert interference through tapping and surveillance. The transfer of digital data which underpins the Hiroshima Accords' cooperation on economic and IP security, and AUKUS' fledgling Pillar II techno-economic partnership on advanced technologies, would therefore be compromised

89. Unnamed Chinese official, quoted in ibid.

90. Dan Swinhoe, The cable ship capacity crunch, *DCD*, 6 December 2022, https://www.datacenterdynamics.com/en/analysis/the-cable-ship-capacity-crunch/#:~:text=These%20cables%20are%20the%20lifeblood,small%3A%20just%2060%20ships%20worldwide.

91. UK Defence Committee, UK Defence and the Indo-Pacific: Eleventh Report of Session 2022-23, 24 October 2023, https://publications.parliament.uk/pa/cm5803/cmselect/cmdfence/183/report.html#:~:text=The%20UK's%20trading%20relationship%20with,on%20households%20in%20the%20UK.

92. IMF World Economic Outlook Database, April 2023, https://www.imf.org/en/Publications/WEO/weo-database/2022/October.

by Indo-Pacific undersea cable disruption.

There are positive signs that the UK and its AUKUS allies have grasped the imperative need to defend the undersea critical infrastructure upon which the alliance depends: joint exercises utilising UUVs and surface surveillance vessels were conducted in Australia in November,[93] and the development of a new space radar system (DARC) was unveiled last December, which will enhance future maritime monitoring capabilities.[94] It is essential that these do not remain sporadic measures, but are packaged into a fully coordinated multilateral strategy for defending the critical undersea infrastructure which undergirds our allied economic, defensive and intelligence systems.

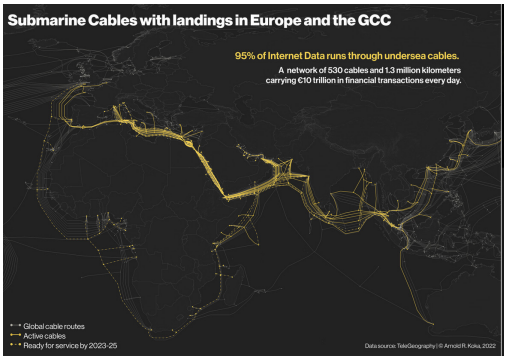
The Five Eyes constitutes an integral component of the UK's global intelligence framework. China's offensive capabilities below the water's surface could enable it to disrupt, breach, and even manipulate intelligence and sensitive military information passing between the UK and its regional allies. Beijing's attempt to bifurcate regional cable networks also poses strategic risks to the Five Eyes. By incentivising other states to opt out of existing western-owned networks with low-cost bandwidth and lower latency, the PRC would harm the Five Eyes' own monitoring capabilities. As it has been characterised elsewhere, the effect would be to give the Five Eyes cataracts.[95]

93. UK Government, New undersea capability to strengthen AUKUS partnership, 13 November 2023, https://www.gov.uk/government/news/new-undersea-capability-to-strengthen-aukus-partnership.

94. UK Government, New deep space radar will transform UK security, 2 December 2023, https://www.gov.uk/government/news/new-deep-space-radar-will-transform-uk-security.

95. Kieren McCarthy, China's undersea cable plan targets US and British intelligence, *The Telegraph*, 9 May 2023, https://www.telegraph.co.uk/news/2023/05/09/china-undersea-cable-us-intelligence-nsa-gc-hq-five-eyes/.

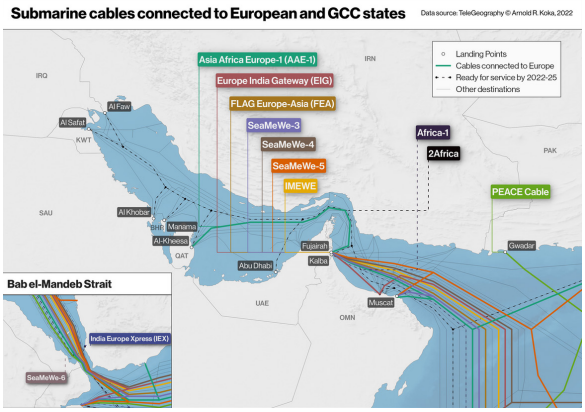
The Arabian Peninsula



Source: https://www.egic.info/gulf-submarine-network-amid-sabotage-mine-warfare

Whilst China does not factor into the UK's strategic considerations in the Persian Gulf, another threat looms in this peripheral region of the Indo-Pacific: the Islamic Republic of Iran. The narrow waters around the Arabian Peninsula are a notoriously precarious choke-point of global oil trade, but they are equally important due to the cable highway running below the water's surface. Major cables passing from Europe, through Africa and towards Asia run down the Red Sea, before bending round eastwards through the Gulf to its myriad on-shore sites. The FLAG Europe Asia cable, for example, carries data through the Persian Gulf as part of its 28,000km journey from Cornwall via 16 countries, and three continents, to Miura in southern Japan. The region thus constitutes the major digital maritime route between Europe and the eastern side of the Eurasian heartland.

Iran does not possess Russia's high-end sub-surface naval capabilities necessary to engage in sophisticated cable disruption at depth. However, the structural characteristics of the Persian Gulf's narrowness and shallowness, and constant cable proximity to Iran's numerous naval bases, affords Tehran the capacity to conduct cheaper – yet equally devastating – forms of attack. The IRGC Navy is equipped with numerous small platforms catered to laying mines, maritime improvised explosive devices, and to carrying out swift hit-and-run operations.[93] These tactical capabilities have all been developed in a concerted effort to pose a constant, asymmetric threat to maritime stability in the Gulf, deterring adversaries from wider strategic objectives against Iran in the region. Iran's heavy mining of the Persian Gulf presents a ubiquitous risk to regional cables which – due to the blunt, imprecise impact of explosives – would cause collateral damage which would be impossible to predict and control, making crisis escalation management very difficult. Cable redundancy levels are poor in the region, and so if numerous main lines are severed, a major rupture of digital communications would occur.



Source: https://www.egic.info/gulf-submarine-network-amid-sabotage-mine-warfare

96. Arnold Koka, The Gulf Submarine Network amid Sabotage and Mine Warfare Threats, *Euro-Gulf Information Centre*, 25 October 2022, https://www.egic.info/gulf-submarine-network-amid-sabotage-mine-warfare.

One point of distinction from the Russian threat in the Atlantic – and, in turn, a similarity with the strategic landscape in the South and East China Sea vis-à-vis China – is that Iran also relies on Gulf cable network for its own digital communications. Whilst this acts as a restraining force on Iranian calculus below the threshold of conflict, the Islamic Republic may conclude that such internecine acts are strategically meritorious in the case of an existential conflict.

Tehran could also command its regional allies to sabotage equally congested cables running in the Red Sea to distance itself from the immediate fallout. Indeed, fears of such proliferation have risen in recent months, after posts on Telegram channels affiliated with the Houthis and Hezbollah appeared to threaten attacks on cables in the region.[97] Whilst these groups are not thought to possess the equipment necessary to conduct sophisticated subsea warfare, Iran could provide such capabilities.[98] In any case, cables passing through the shallower waters of the Red Sea are exposed to far more rudimentary methods, such as cutting and mines. The Houthis have already received combat diver training,[99] and have an array of naval mines which could damage cables at shallower depths.[100]

Whilst the West currently operates two maritime policing missions in the region – the US-led International Maritime Security Construct, and the EU's European Maritime Awareness in the Strait of Hormuz – these would be entirely overwhelmed if Iran opted to escalate considerably in the undersea domain. As a result, the UK and its allies currently rely entirely on the deterrence of mutual consequence to ward off the dormant Iranian threat to undersea cables in the Persian Gulf. In the event of a future major conflict, in which the Islamic Republic perceives its existence to be at stake, this deterrent may no longer hold. At this point, it must be made explicit that the concerted targeting of cables linking Europe to Africa and Asia would be treated as an act of war. Before this point – and hopefully in order that it is never reached – the UK and its allies must bolster their undersea warfare capabilities in the region to act as a necessary deterrence.

Cables as a Unique Strategic Challenge

In order to devise a roadmap for responding to these threats, the distinct strategic nature of undersea cables must first be properly understood. As with all other military targets, undersea cable security is determined by the relationship between offence and defence. However, structural and technological idiosyncrasies afford cables a distinctly specific strategic grammar.

The French *Seabed Warfare Strategy* offers the first genuine acknowledgement of this fact in western government-level doctrine, and so serves as a useful blueprint for applying these principles to UK strategy. The document formulates a "new grammar of [seabed] strategy" in which the domain's intrinsic nature sets it apart in terms of strategic calculus.[101] The two determinant factors of this grammar are *ambiguity* and *the notion of thresholds*, both of which afford outsized advantages to the aggressor, owing to geographical and technological features, which are unique in the warfare continuum.

The pro-aggressor balance of ambiguity, the *Strategy* says: "stems here from both the difficulty of keeping an immense, unknown, opaque and barely accessible submarine area under surveillance, and the complexity, heightened by the exercise of a right that is still too weak and shaken up".[102] This rightly identifies the combination of the seabed's geographical and bathymetric inaccessibility, the resultant technical and operational challenges of defence and attribution, and the flimsy international legal framework offering weak deterrence and restitution. The implications of this feature are far-reaching and severely complicate the formation of effective defensive systems of deterrence by denial and punishment.

The question of thresholds arises from ambiguity as a dependent factor, and the *Strategy* states that:

101. French *Seabed Warfare Strategy*, 21.

102. Ibid.

97. MEMRI, In Veiled Threat, Telegram Channels Linked To Houthi Ansar Allah Movement Point To Submarine Internet Cables Off Yemeni Coast, 26 December 2023, https://www.memri.org/jttm/veiled-threat-telegram-channels-linked-houthi-ansar-allah-movement-point-submarine-internet.

98. Emily Milliken, The Next Casualty of the Red Sea Attacks: Undersea Cables, *Gulf International Forum*, 29 January 2024, https://gulfif.org/the-next-casualty-of-the-red-sea-attacks-undersea-cables/.

99. Michael Knights, The Houthi War Machine: From Guerrilla War to State Capture, *CTC Sentinel*, September 2018, 11 (8), 20.

100. Farzin Nadimi, Under Fire in the Bab al-Mandab: Houthi Military Capabilities and U.S. Response Options, *The Washington Institute for Near East Policy*, 8 December 2023,https://www.washingtoninstitute.org/policy-analysis/under-fire-bab-al-mandab-houthi-military-capabilities-and-us-response-options.

> *"Although there is practically no risk of losing human lives in such a theatre of operations, which is uninhabited in essence and highly robotised, the opacity of the seabed carries the risk of unrestrained actions being undertaken by automated systems that are difficult to control due to the nature of the environment".*[103]

The most significant consequence of this facet of the undersea domain is to muddle the escalation chain. In the post-heroic era –[104] when the loss of human life in war is deemed less acceptable in democracies than ever before in history - the capacity to inflict grave damage to the enemy's economic, social and political systems at diminished risk of escalation offers an unparalleled strategic opportunity. Combined, these core features of the undersea domain, and cables as its primary target, demand wholesale change in strategic doctrine in order to recognise sufficiently our critical vulnerabilities in this area.

CASE STUDIES: Cable-cutting concerns

As argued, the challenge of protecting undersea cables is complicated by the difficulty of ascribing definitive attribution. Two recent, highly suspicious episodes – one in the Euro-Atlantic in 2021, the other in the Indo-Pacific in 2023 – exemplify how hostile states may already be perpetrating aggressive acts against cables in both theatres, and getting away with it.

Norway 2021

In April 2021, 4.2km of fibre-optic cables completely vanished in the Arctic Ocean. The cable, connecting the Svalbard archipelago to the Norwegian mainland, transmits oceanographic monitoring data to the central authorities, and carries hydrophone sensors crucial for monitoring underwater activity. The damage caused information flow to halt completely, and will still not be fully operational until 2024, at the cost of €5.6mn.[102]

For seven months, the piece remained missing, until it was discovered more than 11km out of position. The mystery developed further after Norway's public broadcaster, NRK, revealed that a Russian trawler had been identified at the very location of the incident when the authorities received the cable's last signal. However, analysis of the recovered segment could not confirm whether the causation was natural, accidental or intentional. The incident nonetheless joins a growing list of critical maritime infrastructure incidents occurring in the Euro-Atlantic in the suspicious proximity of Russian naval vessels.

There are other reasons why Svalbard would pose an attractive strategic target for Russia. The Global Seed Vault is stationed on the island, where blueprints and duplicates of every type of seed are stored in genebanks to mitigate against future apocalyptic catastrophe. Its security is therefore a task of incredibly high stakes for the Norwegian government, meaning that any relatively minor Russian incursion or interference is likely to impose significant protective costs on Oslo in response. Svalbard is also home to SvalSat, a major satellite station, and one of only two capable of communicating with low altitude polar orbiting satellites upon every Earth rotation. SvalSat is used for a plethora of satellite and cyber purposes by international entities, including the European Space Agency, NASA, and other governments. The fact that such critical infrastructure is stationed on an island linked to the mainland by just two fibre-optic cables, and located so close to Russia, makes it an unrivalled strategic vulnerability for the West in the coming age of Arctic contestation.

Source: https://icepeople.net/2022/01/10/one-of-svalbards-two-undersea-fiber-cables-severed-officials-say-communications-capability-still-normal-emergency-repair-and-contingency-operations-underway/

103. Ibid.

104. See Edward N. Luttwak, Toward Post-Heroic Warfare, *Foreign Affairs*, May/June 1995, https://www.foreignaffairs.com/articles/yugoslavia/1995-05-01/toward-post-heroic-warfare.

105. Lisbeth Kirk, Mysterious Atlantic cable cuts linked to Russian fishing vessels, *EU Observer*, 26 October 2022, https://euobserver.com/nordics/156342.

Taiwan 2023

Two years later, two fibre-optic cables running between Taiwan and its Matsu islands were cut. As with the Norwegian incident, the consequences were grave, as the 14,000 Matsu islanders lost complete internet access for several days, and then only received 5% of full bandwidth from the backup microwave system during the two month-long process of repairing the cables.[103]

Unlike Norway's reticence, the Taiwanese government was quick to blame China, announcing that a Chinese fishing vessel and freighter had been spotted near the cable. The near-impossibility of proving intent in the undersea domain was once again apparent, however, as Taipei fell short of accusing the CCP of foul play. Whether intentional or not, the episode illustrated Taiwan's immense critical maritime infrastructure weakness, as its digital communications with the surrounding world rely on only 14 cables. In the event of a Chinese blockade or invasion, this would prove a potentially critical strategic vulnerability for Taiwan.

Source: https://www.stuff.co.nz/world/asia/300825910/taiwan-suspects-chinese-ships-cut-islands-internet-cables

The lack of analogy for undersea cables as a strategic target

A comparison with other new-age frontiers further attests to the unique advantages afforded to aggressors in the undersea domain, and thus the concomitant defensive disadvantages.

The space age shares some structural similarities with the sub-surface maritime landscape: as with critical maritime infrastructure, space architecture houses the digital transmissions which underpin transnational social, economic and military networks; great geographical distance which renders access difficult; and a rate of technological progression which is outstripping the governing legal parameters.

However, three key differences exist which distinguish the strategic conundrum posed by the two respective domains. Firstly, whilst seabed mapping and physical interference operations require cutting-edge equipment, the ability to do so is already a technological reality more so than in space, as demonstrated extensively in the previous chapter's assessment of Chinese and Russian capabilities. Secondly, the global space architecture – satellites, spacecraft and space stations – constitutes a civil-military permutation.[107] Often, equipment can serve a dual-use purpose, with government initiatives and personnel using equipment owned and maintained by private entities. The upshot of this is to complicate the insulation of offensive operations from state-targets, carrying far

107. The Space Report, Infrastructure, https://www.thespacereport.org/topics/infrastructure/.

106. Sarah Wu and Yimou Lee, Analysis: Fear of the dark: Taiwan sees wartime frailty in the communications links with world, *Reuters*, 16 March 2023, https://www.reuters.com/world/asia-pacific/fear-dark-taiwan-sees-wartime-frailty-communication-links-with-world-2023-03-15/.

greater risks of escalation than in the undersea domain. Thirdly, and most importantly, the satellite network lacks the physical connectivity of undersea cables travelling through vulnerable territorial and international waters, which offers a critical potential target as explained above.

Undersea gas pipelines are another infrastructure which might at first appear analogous. They too are located deep below the surface, pass through all categories of maritime territories, are owned by private entities, and transfer essential goods (energy rather than digital) between states. Again, however, their intrinsic features render them less attractive targets of geopolitical machination than cables. Gas pipelines lie on average 2,500m below the water's surface,[108] compared with the frequent >5,000m depth of fibre-optic cables, making the former easier to access for exploration and exploitation purposes.[109] Furthermore, the framework of the global energy market ensures that any disruption to supply routes reverberates internationally, precluding the targeted impact of, say, severing the AC-2/Yellow cable between the US and UK. Whilst the unifying interconnectedness of global energy markets may be a strategic boon in some instances, such as Russia's weaponisation of its gas reserves during the Ukrainian War to damage Europe's economic system, it would deter China from similar acts due to its status as a vast energy importer. The cable network's immanent capacity for precision operations, as opposed to the blunt mechanism of energy pipeline targeting, therefore offers the great strategic merit of optionality.

Supply chain globalisation, an exponential trend since the logistical transition to steel container shipment in the 1950s, has attracted significant attention as an international vulnerability amidst escalating Sino-American competition. The consequence has been a political jolt towards onshoring, friend-shoring and near-shoring policies, driven by new state capitalistic dogma and energised by industrial subsidy programmes pursuing economic insulation. In reality these developments amount to a reassertion of the implicit tendency towards regionalisation since the mid-20th century, which created three intra-continental manufacturing and trade hubs in Europe, Asia and, to a lesser degree, North America.[110] Nonetheless, as raw materials, components and manufactured goods travel above the water beneath whose surface fibre-optic cables lie, their exposure to destabilising geopolitical competition is similar.

However, once again, the implausibility of insulating one's maritime trade entirely from global disruption makes offensive operations to these ends a less versatile strategic tool. Russia's decision to resume its blockade of Ukrainian Black Sea grain exports to suffocate the latter's economy has not come without cost. Soaring shipping insurance costs in the region have collapsed Moscow's own access to export ships, forcing the Kremlin to turn to older vessels which are slower and have less capacity. The Russian agriculture ministry forecasts an 8% drop in grain exports for the year 2023/2024, a likely secondary effect of this trade warfare.[111] This dilemma has also injured Russian grand strategy horizontally, as the global energy security crisis threatens to weaken its diplomatic courting of the

108. Medgaz, Construction of a submarine gas pipeline, 1, https://www.medgaz.com/medgaz/doc/informacion-eng.pdf.

109. Geoff Huston, At the bottom of the sea: a short history of submarine cables, *APNIC*, 12 Feb 2020, https://blog.apnic.net/2020/02/12/at-the-bottom-of-the-sea-a-short-history-of-submarine-cables/.

110. Shannon O'Neil, *The Globalisation Myth*, 20.

111. Jonathan Saul and Nigel Hunt, After attacking Ukraine wheat exports, Russia faces own shipping challenge, *Reuters*, 8 August 2023, https://www.reuters.com/world/europe/after-attacking-ukraine-wheat-exports-russia-faces-own-shipping-challenge-2023-08-08/.

Global South.

In the Indo-Pacific, the perilous scenario of the US and its allies countering a Chinese blockade or invasion of Taiwan by closing off the Strait of Malacca has earned the title 'the Malacca Dilemma' in Beijing's strategic thought. Three quarters of the PRC's petroleum and LNG exports, and 60% of its overall trade flow, pass through the Strait,[112] meaning that any first-strike action in the theatre is destined to become internecine conflict. Again, this may well serve overall strategic calculus, which it is beyond the remit of this paper to consider. The fact remains, however, that undersea cables permit a degree of precision and versatility at sub-threshold level which offers distinct strategic value.

The unique strategic grammar of undersea cables therefore presents inordinate advantages to the aggressor over the defender. This dynamic poses defensive challenges to both deterrence by denial and deterrence by punishment. In the case of the former, the relative ease of access and engagement combines with the difficulties of monitoring and policing such a vast target, thereby diminishing the potency of deterrence. In the case of the latter, obstacles to the attribution of damage causation – and the near-impossibility of proving intent – complicates the management of escalation via proportionate response. As the two case studies demonstrate, the result is impunity of hostile action towards a vulnerable and strategically vital target in a manner which is distinct from other new-age military domains.

112. Pawel Paszak, China and the "Malacca Dilemma", *Warsaw Institute*, 28 February 2021, https://warsawinstitute.org/china-malacca-dilemma/.

UC Chapter II: A British 'Space-to-Seabed' Maritime Strategy

The strategic case for a space-to-seabed doctrine

The pace of scientific and technological development, alongside dawning recognition of the competitive advantages available below the water's surface, are extending the maritime domain downwards as a strategic theatre. For this and all the reasons above, the UK needs to formulate a comprehensive strategy which incorporates the entirety of the water's depths, whilst integrating the full technological capabilities of the air and space domain in a space-to-seabed maritime doctrine to secure our interests at sea. Recent progress in capability enhancement and multilateral cooperation is welcome, but must be integrated into a robust whole of system approach to defence of the undersea domain.

As the French *Seabed Warfare Strategy* rightly notes, the seabed is currently in a liminal era between that of competition and of contestation.[113] The *Strategy* identifies three critical trends which will determine the nature and outcome of this transition: increasing economic exploitation of sub-surface resources by public and private actors; rising state dominance of this competition through predatory actions; and a 'might equals right' scenario, where early movers outpace both their rivals and international legal parameters through *fait accompli* actions. Alarmingly, the UK's lack of strategic clarity regarding the seabed, previous insufficient attention, and disjointed capability-enhancement programmes put it on the back foot in the emerging contested phase, which is defined by strategic complexity, expensive R&D demands and costly cutting-edge technological offensive and defensive systems.

Although these three trends characterise total global seabed competition, the features of each theatre raise distinct strategic imperatives – and demand specific responses – for the UK. As seen, Russia poses a threat in both the sub- and above-threshold Euro-Atlantic context to the British-owned and non-British owned critical infrastructure which constitutes the vital connective tissues of the UK's digital channels. These immediate exigencies urge the UK to contribute to the formation of a multilateral framework of deterrence by denial and punishment.

In the Indo-Pacific theatre, the UK has contiguous security concerns. Here, the Chinese threat is not directly towards British infrastructural systems, but rather the functioning of the global maritime landscape. It also risks weakening the UK's intelligence alliances by compromising

113.French *Seabed Warfare Strategy*, 24-26.

and disrupting the transmission of vital digital communication. Whilst geographical distance, and realism over the material and operational capacity of a middle power, combine to constrain the UK's ability to meaningfully alter the balance of power in the Indo-Pacific, it must nonetheless develop means of mitigating these strategic vulnerabilities. This calls for full UK collaboration with its regional partners' efforts to meet these challenges, as well as support of measures taken at the international diplomatic and legal levels to attenuate the risk of escalation in the undersea domain.

The following section lays out the UK's existing strategic and undersea capability landscape, as well as the international legal framework in which it operates. This permits an assessment of the extent to which the UK is ill-equipped to meet its security requirements in the current military balance. The final section offers recommendations aimed at bridging these gaps.

The porous international legal framework

As Sunak noted in 2017, legal protection of undersea cables "seem[s] far more suited to the comparatively peripheral role the infrastructure played in the '70s and '80s, than to the indispensable status they now hold in the internet age".[114] The seabed is governed by three international conventions. The most recent of which, UNCLOS, is 41 years old. Whilst the 1884 Convention provided early recognition that the seabed is a public good needing mutual protection and regulation,[115] law and enforcement mechanisms have not kept pace with the growing room for manoeuvre for state and non-state actors alike in this domain.

The criminalisation of global activities does not stop perpetrators entirely. The illegal invasion of Ukraine is the clearest testament to this reality today, as too are the innumerable cases of illicit financial activity which occur on a daily basis. Whereas the former exemplifies how insufficient deterrence welcomes the perpetration of international crimes, the latter's appeal relies on its covert and unenforceable nature.

Without a strong legal framework governing the seabed, it will therefore remain a domain in which actors can pursue sub-threshold advantages free from both forceful deterrence, and indeed devoid of a clearly defined border between licit and illicit activity. UNCLOS is not fit for purpose to uphold national security in the undersea domain: it does not prohibit states from targeting undersea cables via physical or cyber means as legitimate military targets in times of war; it does not permit warships policing territorial waters to board vessels engaging in suspicious behaviour around national infrastructure; and it entirely overlooks cables at the point they make landfall at landing sites.[116]

Even the Tallinn Manual, a guide provided by the NATO Cooperative Cyber Defence Centre of Excellence which offers non-binding best-of-practice guidance on international law principles in the realm of cyber warfare, attests to the legal lacunae complicating jurisdiction of the undersea domain. Not only does it confirm that the targeting of cables carrying military and civilian traffic is a legitimate operation under the law of armed conflict,[117] it notes that peacetime cyber espionage does

114. Rishi Sunak, Indispensable, insecure, 17.

115. United Nations Documents on the Development and Codification of International Law, 41 AM. J. INT'L L. SUPP. 29, 33-34 (1947)

116. Rishi Sunak, Indispensable, insecure, 17.

117. Michael Schmitt, Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum, *Harvard National Security Journal*, May 2017, 246.

not *per se* violate international law, as long as the actual methodology does not contravene UNCLOS.[118] Any update is going to require greater definitional clarity based on a thorough assessment of contemporary technological capabilities throughout the maritime domain – and how they impact national and commercial interests – must be provided so that the convention can meaningfully regulate activities both above and below the conflict threshold.

As states grapple with the inadequacies of international legal frameworks governing other new-age frontiers, such as cyber and space, the seabed is also in urgent need of reappraisal. The united international effort to redraft the Convention will not happen quickly, however. In the meantime, the UK cannot accept a situation in which hostile actors can freely target its undersea maritime interests, whether by contravening existing but unenforced restrictions or, more likely, exploiting loopholes and lacunae in outdated laws.

The UK must therefore make better use of its sovereign right to enact national laws to protect assets in its territorial waters better. UNCLOS contains carve outs which enable nations to adopt laws and regulations to protect cables and pipelines in their territorial waters.[119] Article 113 also makes it incumbent upon states to punish perpetrators of intentional attacks against critical maritime infrastructure.[120] Even in UNCLOS' current state, therefore, the UK has bilateral legal avenues for better protecting its cables.

To this end, the UK should follow the lead of Australia and New Zealand by establishing unilateral legal frameworks, Coastal Protection Zones, which impose more stringent restrictions on activities in territorial waters. Measures such as fines for anchoring and bottom trawling, and ordering ships to broadcast their positions to Coast Guard upon entry, greatly enhance the ability to monitor activity in these waters. Ultimately, it is the sovereign right of the state to control what happens in its waters, and the UK should explore unilateral avenues for protecting its critical maritime infrastructure and national security.

Assessment of current undersea defensive capabilities

As has been intimated throughout, the UK lacks a clear-eyed strategic doctrine guiding policy towards the seabed. Presently, the UK's national and maritime security doctrines are defined by a constellation of various strategic frameworks.

As mentioned, the *Integrated Review Refresh* is Britain's most up-to-date strategic concept, marshalling a whole-of-government collective effort towards core national objectives. Whilst undersea cables do not receive individual treatment, the *Refresh* identifies the profound security risks associated with critical infrastructure in the contemporary technological age. The respondent strategy incorporates close multilateral cooperation with allies and partners across Eurasia and the Indo-Pacific, and public-private partnership to guarantee digital and cyber security.[121] The document thus stands up the National Protective Security Authority to

118. Michael Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press: 2017, 168.

119. UNCLOS, 1982, Article 21, 31.

120. Ibid., 64.

121. *Integrated Review Refresh*, 6, 48.

provide intelligence agency-led advice to firms operating in sensitive sectors of the economy, including critical infrastructure. Such measures reveal an ongoing rejuvenation of British strategic thought, lending a clear direction of travel which has been entirely absent since the end of the Cold War. The failure to treat in earnest undersea cables, however, leaves this fundamental component of maritime security a strategic blind-spot which must be fully integrated into subsequent strategic concepts.

The House of Commons Library has a research briefing on undersea infrastructure, *Seabed warfare: Protecting the UK's undersea infrastructure*,[122] published last year. Despite the title's promising similarities to the French *Seabed Warfare Strategy*, it amounts to a one-page primer detailing the importance of the seabed, and the MoD's Multi-Role Ocean Surveillance (MROS) development programme. The section on the Russian threat is confined to four sentences containing quotes from British and ally officials on the matter. The government's sole treatment of critical maritime infrastructure, therefore, is significantly cursory.

The government's maritime strategy is comprised of various policy papers, all of which gloss over the sub-surface and seabed. The 2022 *National Strategy for Maritime Security* assigns 2 out of 115 pages to the protection of subsea infrastructure, again limited to explaining the strategic importance of cables without providing a subsequent roadmap of actionable measures.[123] Tangible steps are limited to boosting collaboration with cable-owning and -operating private entities, re-hashing the 2021 announcement of MROS, and pledging to "re-evaluate its regulatory framework to support the continued security, resilience, and integrity of critical UK communications".[124] One year on, there is no sign of progress on the third commitment.

Oddly, but indeed illustratively, the most comprehensive government-level consideration of undersea cables is found in the Department for Transport's (DfT) 2019 *Maritime 2050: Navigating the Future*. The paper notes specifics related to the issue, such as the importance of defending interconnector cables as well as fibre-optics, the need to build contingency into the system, and – crucially – the need for "total MDA" (maritime domain awareness), synonymous with this paper's 'space-to-seabed' parameter.[125] That the best example of government thinking on the subject is five years old – before the recent uptick in Russian incidents in the Atlantic Sea – and a siloed paper produced by the DfT without participation from the MoD, FCDO or Home Office, attests to the dire need for an updated integrated appraisal of seabed security.

With the UK's incomplete maritime strategic framework outlined, it is time to turn to an assessment of our existing defensive capabilities in the undersea domain. The institution tasked with this function is the Royal Navy.[126] As identified in the House of Commons Library's *Seabed Warfare*, the Navy's flagship seabed defence operation in the North Atlantic is the MROS programme, launched by the MoD in 2021.[127] This mission was spurred by Russia's investment in underwater capabilities "which can threaten undersea cables".[128] The MROS provides surveillance assistance

122. Louisa Brooke-Holland, Seabed warfare: Protecting the UK's undersea infrastructure, House of Commons Library, 24 May 2023, https://commonslibrary.parliament.uk/seabed-warfare-protecting-the-uks-undersea-infrastructure/.

123. *National Strategy for Maritime Security*, HMG, August 2022, 66-67.

124. Ibid., 67.

125. *Maritime 2050: Navigating the Future*, Department for Transport, January 2019, 268-269.

126. "We're going to need a bigger Navy", *House of Commons Defence Committee*, Third Report of Session 2021-22, HMG, December 2021, 13.

127. Defence in a competitive age, Ministry of Defence, March 2021, 48-50.

128. Ibid., 9.

to the Navy's seven Astute class submarines alongside the single Trafalgar class, whose service was extended to bridge the transition period. These submarines are fitted with the Sonar 2076, UK-manufactured non-acoustic sensors enabling navigation and detection below the surface.[129]

As part of the MROS operation, the UK is partnering with France in the development of a new autonomous minehunting system, which will concomitantly see the Navy's extant Mine Counter Measures Vessels retired.[130] Last April, the two European allies completed successful anti-mining exercises with the US in the Gulf, operation Artemis Trident. The autonomous minehunting system is not set to replace completely traditional ships for over ten years.[131]

After a near year-long delay, the first of the two scheduled MROS ships, RFA Proteus, came into service last October.[132] RFA Proteus is a re-purposed platform supply vessel from the oil and gas industry, and required the personal intervention of then-Defence Secretary Ben Wallace to expedite the initial procurement process in 2022, on the back of reports of Russian mapping missions in the Atlantic. Despite this, the UK's enduring difficulties in reaching operational readiness in the undersea domain is exemplified by the fact that RFA Proteus has still not yet completed its Operational Sea Training programme as of this year.[133] It was therefore unable to participate in the JEF seabed warfare exercise earlier this year.

Furthermore, whilst the vessel's highly publicised introduction has sent a clear deterrence signal to hostile actors seeking to exploit the undersea maritime domain, its material operational and strategic value is limited. Furthermore, for context, platform supply vessels travel at approximately 12-18 knots, or 20-30km/hr. The UK's EEZ is 6.8mn km^2. The AC-1 trans-Atlantic cable linking the US, UK, the Netherlands, and Germany is 14,000km long. This is one of the c.60 cables which directly pass through British territorial waters. The operational limitations are clear.

As for the UK's cable monitoring and sensing equipment pool, public sources suggest that a relatively systematised procurement process is underway. It appears that the MoD's principal supplier of sonobuoys is Ultra Electronics Command & Sonar Systems. In 2017, the MoD purchased sonobuoys for the Navy's Merlin MK2 maritime patrol helicopter fleet.[134] The same company received another contract in 2018 for Sonar Type 2150s to be installed on the Type 26 Frigate.[135] In April2 2019, the MoD awarded the company a three-year contract to supply sonobuoys, with the potential of another three years.[136] Last June, the MoD purchased a further five 2150 sonars from Ultra Electronics.[137] These contracts amounted to in excess of £100mn across their lifespans. Due to the surge in state focus on the undersea domain, forecasters estimate the submarine sensor market to grow 40%, from $290mn in 2023 to $420mn by 2033.[138] The Royal Navy's sonar suite is stationed at HMNB Clyde, where training and seabed monitoring operations take place.

Finally, the Royal Navy is acquiring a fleet of UUVs and AUVs to police the seabed. These vehicles operate under Project Hecla, established to optimise the collection and exploitation of hydrographic and

129. Royal Navy submarines and non-acoustic sensor technology, Navy Lookout, 12 February 2021, https://www.navylookout.com/royal-navy-submarines-and-non-acoustic-sensor-technology/.

130. Ibid., 48.

131. Royal, US and French Navies complete major minehunting workout in Gulf, *Royal Navy*, 20 April 2023, https://www.royalnavy.mod.uk/news-and-latest-activity/news/2023/april/20/20220420-royal-us-and-french-navies-complete-major-minehunting-workout-in-gulf.

132. Twitter, Defence Equipment & Support, @DefenceES, 10/10/23, https://twitter.com/DefenceES/status/1711791077819121995.

133. Analysis: Royal Navy deploys seven ships on underwater infrastructure patrols, *Navy Lookout*, 3 December 2023, https://www.navylookout.com/analysis-royal-navy-deploys-seven-ships-on-underwater-infrastructure-patrols/.

134. Lopamudra Roy, Ultra Electronics receives contract extension to supply sonobuoys for UK Navy, *Naval Technology*, 4 January 2017, https://www.naval-technology.com/news/newsultra-electronics-receives-contract-extension-to-supply-sonobuoys-for-uk-navy-5709339/?cf-view

135. Ultra, Ultra Electronics Command & Sonar Systems Awarded Contract to Supply Sonar Type 2150 to the First Three of Eight Planned UK Royal Navy Type 26 Frigates, 23 October 2018, https://www.ultra.group/fr/media-centre/ultra-news/ultra-electronics-command-sonar-systems-awarded-contract-to-supply-sonar-type-2150-to-the-first-three-of-eight-planned-uk-royal-navy-type-26-frigates/.

136. Ultra, Ultra Electronics Command & Sonar Systems to supply new sonobuoys to UK MoD, 16 April 2019, https://www.ultra.group/fr/media-centre/ultra-news/ultra-css-to-supply-new-sonobuoys-to-uk-mod/

137. https://bidstats.uk/tenders/2023/W25/801243516.

138. Future Market Insights, Submarine Sensors Market Outlook from 2023 to 2033, https://www.futuremarketinsights.com/reports/submarine-sensors-market.

oceanographic information in high-threat areas to protect ships navigating British waters. Another operational value is to provide identification and locational assistance to Type 23 Frigates and P-8 Maritime Patrol Aircraft fleets responding to underwater threats. Last February, £6mn-worth of orders were made for three Iver 4 580 AUVs and two Gavia underwater drones.[139] These join the Navy's fleet of Slocum Gliders, which have been utilised in hydrographic-oceanographic surveillance missions in the North Atlantic since June 2019.

To support the Royal Navy on the operations side, in 2019 the government established the Joint Maritime Security Centre (JMSC). The JMSC is jointly governed by the Depart for Transport, the Home Office, and the MoD, and is supported by these departments as well as Border Force, the Navy, Counter Terrorism Police, the FCDO, HM Coastguard, HM Revenue and Customs, the National Crime Agency and Marine Scotland. The JMSC is thus tasked to act as the central node of a whole system response to maritime security threats,[140] and does so by cohering the responses of its constituent agencies to respond to maritime incidents in British territorial waters. In addition, the JMSC routinely cooperates with allies, including NATO, largely through intelligence-sharing and crisis response.

As mentioned, the UK lacks the public-private partnerships needed to support the agencies which provide ISR for maritime defence. The JMSC currently purchases satellite imagery from private companies on an ad hoc, expensive basis. Given the integral role which air- and space-based surveillance must play in a 'space-to-seabed' maritime system, this leaves the UK under-equipped for its surface and sub-surface monitoring needs, reducing its capacity to intervene in hostile acts and, more critically, to attribute blame after they have occurred.

As well as these vulnerabilities at sea, the cable on-shoring sites dispersed across the UK in remote locations are largely under-protected. There are approximately 100 of these centres, which are mostly found in remote peninsula regions of the western coastline of the British Isles. The majority traverse the ocean-facing southwestern and northwestern approaches of the Bristol Channel, St George's Channel, and North Channel, even extending as far north as The Minch before docking around the Hebrides. This presents critical security concerns for two structural reasons: they are difficult to access by land, connected to major settlements exclusively by slow transport routes; and they are easily accessible by sea routes through the open seas.

There are also serious question marks over the on-site security arrangements at these centres. In 2018, a reporter from *The Times* simply strolled into two Cornish cable facilities in daylight, entirely unchallenged.[141] The two centres house multiple cables, including several transatlantic ones and the Europe-India Gateway cable. It was also claimed that British security agencies had been warned about the lax security of these Cornish sites 12 years prior.

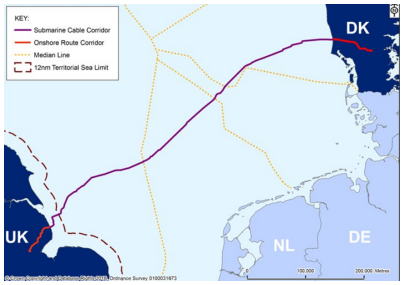
139. George Allison, Britain orders new Autonomous Underwater Vehicles, *UK Defence Journal*, 20 February 2023, https://ukdefencejournal.org.uk/britain-orders-new-autonomous-underwater-vehicles/.

140. HMG, National Strategy for Maritime Security, 18.

141. Mark Hookham and Gabriel Pogrund, Revealed: how reporter strolled into UK's 'secure' data-cable sites, *The Times*, 4 February 2018, https://www.thetimes.co.uk/article/revealed-how-reporter-strolled-into-uks-secure-data-cable-sites-f6fx2hndv.

Insufficient On-shore Cable Security

It is unclear that future cable projects are set to bolster on-shore security adequately on the back of these breaches and concerns. By way of example, the planned security measures of the VikingLink – a new clean energy and 1,250km submarine cable channel running between the UK and Denmark, expected to be completed this year – were published in 2017.[142] These include security fencing, CCTV ("where determined necessary"), and restricted access to approved personnel only.[143] All security responsibilities are to fall within the remit of a lone Land Officer, who is the point of contact for all individuals and bodies with interests in the cable network. Whilst further security arrangements – including the number of on-site personnel – may not be in the public domain, the reliance on restrictive infrastructure and remote surveillance equipment seems unlikely to ensure the higher level of protection required to deter and deny hostile interference at this on-shore cable site.



Source:https://www.offshorewind.biz/2019/12/18/balfour-beatty-secures-viking-link-onshore-contract/

The VikingLink on-shore station, Bicker Fen, Lincolnshire

Source: https://www.power-technology.com/projects/viking-link-interconnector-project-denmark-uk/?cf-view

To what extent, then, is the UK's undersea defensive system – incorporated into the integrated framework of its alliances and partnerships – sufficient to meet the needs of national security? In other words, is the existing balance of military power in the British seabed domain loaded in favour of the aggressor or the defender?

A useful starting point for guidance is historical analogy with the last, highly successful Euro-Atlantic submarine and seabed detection system: the US-led SOSUS (later SURTASS) of the Cold War. SOSUS was launched in the US 1954, with $10mn of annual state funding,[144] to counter the Soviet submarine threat.[145] The novel system harnessed the sub-surface detection technologies developed by the SOFAR channel of World War II. American scientists ascertained that hydrophones deployed at scale on strategic submersible routes along the ocean floor could detect the noisy

144. Approximately $115mn today.

145. Integrated Undersea Surveillance System (IUSS) History 1950 – 2010, IUSS/CAESAR Alumni Association.

142. National Grid, VikingLink UK Onshore Scheme: Outline Construction Environmental Management Plan, August 2017, https://www.viking-link.com/media/1462/outline-cemp_-proposed-dc-cable-route-revfinal.pdf.

143. Ibid., 14.

diesel engines powering Soviet submarines and, by triangulating their signals, could then locate the vessels accurately from hundreds of miles away.

A rapid capability development programme ensued – combining feats in scientific, engineering, logistical, strategic and multilateral cooperative terms – to pave extensively high-threat areas in the Atlantic, Pacific and Caribbean seas with hydrophones, policed by surface and submersible surveillance vehicles.[146] At its peak, SOSUS employed 4,000 allied personnel stationed at 20 on-shore NAVFAC sites. Operational command resided in the two US Ocean Systems commands, COMOCEANSYSLANT and COMOCEANSYSPAC, housing 3,500 personnel between them. The US government ensured its access to cutting-edge technology by entering into systematised, long-lasting partnerships with leading private sector technology companies – notably WECo and Bell Laboratories – and eased government contracting processes to facilitate equipment acquisition.[147]

Whilst the Warsaw Pact nations countered with their own system of towed array platforms, the technical and operational advantage was firmly with the Euro-Atlantic allies, sustaining a critical strategic victory in the wider Cold War conflict.

The SOSUS (now called the IUSS – the Integrated Undersea Surveillance System) was eventually re-purposed for primarily civilian oceanographic research at the end of the Cold War. However, in the context of Indo-Pacific contestation – as well as escalating Russian sub-surface activity – the US has recently re-launched the IUSS for military purposes. This incarnation's key mechanism is the Deep Reliable Acoustic Path Exploitation System (DRAPES), which relies less on seabed cables than its predecessors, undergirded instead by a cutting-edge wireless network transmitting data via acoustic modems. The ongoing development of the IUSS will be returned to later.

It should be immediately apparent that the UK and its allies' current approach to developing its undersea detection system – piecemeal, relatively uncoordinated, and outside of any orchestrated multilateral framework – falls far below the bar set by SOSUS. By all metrics – funding levels, technological ascendance, multilateral collaboration, and indeed strategic clarity – we are dramatically ill-equipped to meet the undersea threats in both the Euro-Atlantic and Indo-Pacific theatres.

Aside from these capability, tactical and strategic shortcomings, the UK's unilateral operational capacity is also inadequate. Whilst a promising endeavour, the JMSC is currently ill-equipped to fulfil its sizeable brief to its full potential. Without a remit prescribed by legislation, the Centre is confined to the extent that it is limited to receiving orders on an ad hoc 'Ask' basis, rather than having the authority to 'Task' its own research and analysis. Its ability to contribute to an integrated maritime security system is therefore institutionally limited. Existing models in the US and Australia, in which counterpart maritime security agencies have a legislated basis to perform tasks with a degree of impartiality, should be considered as a basis for reforming the JMSC.

146. The Cold War: History of the SOund SUrveillance System (SOSUS), Discovery of Sound in the Sea, accessed 10 October 2023, https://dosits.org/people-and-sound/history-of-underwater-acoustics/the-cold-war-history-of-the-sound-surveillance-system-sosus/.

147. Origins of SOSUS, *Commander Submarine Force US Pacific Fleet*, accessed 10 October 2023, https://www.csp.navy.mil/cus/About-IUSS/Origins-of-SOSUS/.

Furthermore, the Centre largely relies on purchasing costly satellite data from commercial entities to complete its intelligence-gathering missions. Satellite imagery is essential for investigating sub-surface incidents, particularly to corroborate radar scanning when searching for black targets. Without an expanded budget and a more systematised process for acquiring this satellite imagery, the JMSC's critical intelligence-gathering role in the maritime domain will remain impeded.

The second way that further utilisation of commercial data would bring further important benefits to maritime defence is by enlarging the scope to provide publicisable evidence bases to support allegations of hostile acts. Aside from insufficient information, one of the main obstacles blocking attribution is that military intelligence cannot be disclosed in order to develop an evidence base for the public domain. If private sector-sourced information were more accessible, hostile activity around critical maritime infrastructure would be easier to prosecute or – more likely – deter altogether by the ability to present evidence publicly.

The third reason for establishing stronger partnerships with commercial satellite companies is that it would help to overcome barriers to information-sharing between allies. As the constellation of bilateral and multilateral undersea defence frameworks grows, states must be able to share surveillance and identification data seamlessly. At present, legal and operational sensitivities impede the sharing of maritime intelligence.[148] As with the above point, harnessing commercial data more would solve this problem, significantly increasing the effectiveness of existing and future cooperation in the maritime domain.

As shown, the private sector also has a crucial industrial role to play in cable security. The present inability of manufacturers to supply existing projects is only going to worsen, barring concerted public-private cooperation to expand this capacity. Greater incentivisation for domestic cable manufacturing expansion must therefore constitute a core component of the UK's new strategy for undersea warfare. As this covers both digital cables and clean electricity interconnectors, the industry should be included in government green funding initiatives.

Returning to the threat landscape, in the face of Russian aggression in the Euro-Atlantic, the UK must support the accelerated development and operationalisation of NATO's seabed defence system. National capability enhancement must be coordinated with allies to achieve the necessary scale of knowledge-acquisition, monitoring, and deterrent action-taking in the seabed domain. As with SOSUS, efforts must be concentrated in identified threat areas according to the cable choke-points and Russian high-activity zones detailed above. A clear and efficient chain of command, embedding the CUICC and MARCOM centres symbiotically, must be established so that member states' strategies, procurement programmes and capabilities enhancement are orchestrated under a suitable, strategically-orientated umbrella.

Due to the need to prioritise the Euro-Atlantic landscape which endangers our own critical maritime infrastructure, the UK will play a

148. Dr Sidharth Kaushal, in Corrected oral evidence: The Artic, International Relations and Defence Committee, 5 July 2023, 15.

supportive role in undersea competition with China in the Indo-Pacific. Nonetheless, it must lean its full support into the protection of the regional undersea infrastructure systems from which it benefits. As the era of contestation materialises, this means providing diplomatic – and, when practical, logistical and operational – assistance to the emerging endeavours of regional allies and partners. The UK must also work with its regional partners and allies in the Middle East to sustain a lasting deterrence against Iranian targeting of cables in the Persian Gulf and Red Sea. In the eventuality that conflict escalates, it would be important to make clear that attacks on cables linking Europe to Africa and Asia would aggravate a serious response.

The unbreakable link between the various maritime theatres of the UK's Eurasian context was exemplified by the role of IUSS sensors in detecting recent Russian submarine activity around Scotland and the GIUK.[149] This underscores the potential for cross-theatre capability sharing between the UK and its various alliance frameworks which, returning to the three components of an effective undersea strategy, can guarantee the cross-pollination of best-of-practice methods in knowledge-acquisition, monitoring, and responsive action. As it did during the Cold War, the UK must therefore insert itself as a key player in the US' re-energised IUSS. To ensure that we continue to play a central role in multilateral resistance to increasing Russian incursions from the High North into the GIUK Gap, Baltic and North Seas, the UK must adequately increase its patrolling and deterrence capabilities in Scottish naval and air bases.

The following policy recommendations arise as corollaries of these immediate and long-term strategic exigencies. They are categorised into those at the conceptual and grand strategy level, those at the operational level, and those at the technical and capability-acquisition level.

149. Listening to the ocean – the secretive enablers in the underwater battle, *Navy Lookout*, accessed 8 October 2023, https://www.navylookout.com/listening-to-the-ocean-the-secretive-enablers-in-the-underwater-battle/.

Policy Recommendations

1. Strategic

The UK has made genuine improvements to its ability to defend against hostile actors in seabed warfare. That said, the current approach to protecting sub-surface infrastructure is a case of the cart leading the horse. In the absence of a clearly-define strategic framework for how the seabed fits into wider maritime security, and then national security and grand strategy, impressive progress in operational and capability-enhancement will remain reactive, and not part of a concerted strategic approach to the subsea domain.

The government must therefore produce an intelligence-driven, 'space-to-seabed' strategic doctrine, which articulates a coherent 'whole of system' approach to guarding cables and other subsea infrastructure. This must be incorporated into the Royal Navy's current maritime doctrine at the highest order of priority, and then serve as a pillar of future strategic updates. The strategy should address the geographical regions presented by this paper, offering clarity on the variegated national objectives and operational capacity in the Euro-Atlantic and Indo-Pacific regions, whilst retaining the *Integrated Review Refresh*'s acknowledgement of the two theatres' interaction in wider Eurasian competition. The strategy must also acknowledge and incorporate closer engagement with relevant private sector stakeholders, namely satellite imagery providing companies, and British cable manufacturers. As electricity interconnectors assume increasing importance in the green transition, the government should consider assisting their manufacturers with early-stage, green public investment schemes. This would de-risk the projects in their crucial nascent phase, thereby incentivising subsequent private investment.

The doctrine must demonstrate a clear grasp of how the air and space domains are essential to maritime security at all depths. Modern offensive and defensive capabilities below the water's surface, and intelligence-gathering missions, depend upon air-based ISR data and satellite imagery for locating and precision purposes. The government must produce a truly 'space-to-seabed' strategy which guides and codifies closer collaboration between the MoD, other engaged public bodies, and the satellite-owning private sector (see *Capability acquisition* recommendations below for more on public-private collaboration).

In order for this doctrine to be necessarily strategically-orientated, the Office for Net Assessment and Challenge (SONAC) must first produce an analysis of existing capabilities within the strategic environment. Recent events across the globe have proven the critical limitations in western intelligence-gathering and strategic assessment

capacity. Without immediate refinement, the seabed's uniquely challenging strategic grammar promises to leave us highly exposed in this new-age domain. Only a rigorous analysis of the balance of military power between aggressor and defender, produced by SONAC, can guide a British space-to-seabed maritime strategy for effective capability enhancement.

The government must also define with greater clarity responsibilities in the critical maritime infrastructure domain. The MoD is currently legislated to protect defence infrastructure but not commercial, although it de facto covers both areas. Clearer delineation between public and private sector obligations is needed from both the legal and operational perspective. This feeds into the general need to devise a clearer chain of command and ownership framework for the undersea domain.

The UK must make critical undersea infrastructure protection a key pillar of its multilateral security arrangements across the globe. The implications for British security of critical infrastructure being targeted and damaged in these theatres would be devastating for our economic, communication and security arrangements. The government should therefore make protecting the infrastructure upon which these relationships depend a central component. For example, the AUKUS partners must build upon their nascent attention to cable security by devising a coherent joint strategy. These strategies will necessarily involve resource coordination, and collective campaigns to fortify the international laws governing the maritime domain.

The UK should therefore support any international movement to update UNCLOS to regulate the rapidly advancing undersea warfare landscape. UNCLOS and its counterpart conventions are entirely archaic and ill-equipped to govern new-age action along the seabed. The UK should offer its support to any emergent attempts to address this. International legal frameworks have a crucial role to play in preventing the proliferation of undersea warfare into the Indo-Pacific, which cannot be accomplished by military means alone.

Before such international collective efforts materialise, the government should make use of UNCLOS Article 21, which permits states to adopt tighter regulation of its own territorial waters. The UK can learn from the examples of New Zealand and Australia in this regard, which have exercised their rights to implement Coastal Protection Zones.

Alongside this, the UK should press for stronger international oversight of the undersea domain, by campaigning for the International Cable Protection Committee (ICPC) to be granted enhanced regulatory capacities. The self-titled "Guardian of Subsea Cable Infrastructure", the ICPC brings together governments and 98% of the world's subsea cable providers, making it uniquely equipped to convene multilateral efforts to police the complex public-private nature of cable security. The ICPC could be integrated more formally into the UNCLOS framework to empower it to become a lead agency for issues pertaining to cable monitoring and security.

2. Operational

With this national strategic framework in place, the UK will be placed to engage fully with its allies in the emerging undersea multilateral defence framework. The aspiration in this regard is the resounding success of the SOSUS, whose degree of multilateral coordination, strategic insight and capability-enhancement vastly outstrip ongoing efforts.

The JMSC's authority and governance models should be addressed, so as to enable it to fulfil its operational potential in the newly formulated 'space-to-seabed' maritime doctrine. Whilst its 'department agnostic' status affords the Centre advantages in convening cross-agency personnel, its jointly-funded budget renders it beholden to short term political and financial cycles. A governance model should be established which both regularises the Centre's budget, whilst preserving its impartiality and autonomy to task its own intelligence-gathering and analysis tasks. Doing so would place the JMSC at the centre of a fully integrated whole of system approach to maritime security, which engages all relevant government and private sector stakeholders. As witnessed above, Russia and China have already structured their military-intelligence outfits to enable cross-agency, orchestrated undersea operations. The UK cannot outmanoeuvre these threats without likeminded strategic focus at governmental level.

Taking guidance from the SOSUS' strategic success, an extensive ISR assessment must be commissioned to identify the UK's undersea high-threat areas needing immediate attention. As stated above, we cannot, and do not need to, monitor and police all areas of our EEZ. Instead, cable choke-points in our territorial waters must be identified, researched, and protected, at highest priority. This ISR mission would drive subsidiary tasks related to intelligence-gathering, sensor-laying and, eventually, policing by surface and sub-surface deterrence vessels.

The government must launch an assessment of the undersea patrolling capabilities of Scottish bases, and increase these as necessary. Government officials have already warned of a capability over-stretch, as Russia's ability and intent to target critical infrastructure in the Arctic, Atlantic and Baltic Seas increases. To respond to this mounting threat, air and naval presence in Scotland must be enhanced, particularly as our P-8 fleet is already at maximum operational capacity. A permanently stationed MMROS vessel would also facilitate GIUK Gap and northern maritime policing, as would additional naval bases, such as at Scapa Flow. An additional strategic benefit would derive from greater capacity to launch expeditionary missions alongside partners towards Russian waters, which would divert the already-strained GUGI's resources towards a defensive posture, thereby reducing its offensive threat to our critical maritime infrastructure.

On the multilateral level, the UK should therefore take a leading role in NATO's CUICC and MARCOM undersea cable centres, using them as a platform to marshal allied cooperation on seabed security. MARCOM, which provides military and operational leadership, is located in Northwood, near London, offering the perfect opportunity to

leverage a newfound British focus on undersea infrastructure. MARCOM should retain overall oversight of the subsidiary bilateral and multilateral partnerships forming between NATO members. The British team in the CUICC and MARCOM should therefore work closely with the MoD and JMSC, to ensure that our national undersea defence system is closely coordinated with our allies.

Within this framework, the UK should push to formalise allied processes for the coordinated procurement of relevant technologies, and information and capability-sharing platforms. The breadth and multi-jurisdictional nature of the subsea domain renders unilateral efforts by definition incapable of ensuring national security. To avoid the waste of resources through R&D and equipment duplication, a coordinated inter-alliance sharing system is needed to achieve a robust and extensive defensive system.

Alongside this, the UK should offer its full support to, and participation in, the US' revitalised IUSS. Whilst this American endeavour is spurred by Chinese contestation in the Indo-Pacific, its benefit to nearer shores has already been proven by its detection of Russian activity around Scotland and the GIUK. British participation in the new IUSS would thus serve two critical strategic objectives: protecting our interests in the Indo-Pacific region endangered by China; and inculcating a symbiotic intelligence-sharing and operational relationship to assist in the Euro-Atlantic.

Where beneficial, the UK should supplement these multilateral efforts with further bilateral strategic partnerships in the North and Baltic seas, in the vein of the agreement reached with Norway last year. Due to Irish neutrality, and the exposure of the UK to Russian incursions into the ocean approaches to the North Sea, this region is the weak spot in critical maritime infrastructure defence. Where British security concerns elide closely with allies, bilateral cooperation may be necessary to ensure additionally-thick layers of defence. On top of Norway, key contenders for such security agreements in the future are the Republic of Ireland, Sweden and Iceland.

The UK should explore expanding existing Anglo-French military-security partnerships to the undersea domain. CJEF, or the UK-France Maritime Security Treaty, could both be extended in light of our strategic alignment, and renewed focus, on the undersea domain, and similarly cutting-edge operational and technological capabilities.

Under British leadership, the JEF should build on its recent patrol mission to regularise surveillance missions within a concerted strategic framework for undersea warfare. The JEF nations are situated in areas of critical strategic competition with Russia, and so would comprise a natural alliance in the undersea domain. This avenue should be explored, whereby deepening partnerships across the technical, tactical and operational levels could see the JEF lead the way in wider NATO collaboration on critical maritime infrastructure protection.

3. Capability acquisition

The final slew of actions the UK must take relates to unilateral capability enhancement of its seabed defence system. As stated, further fortification can only occur under the stewardship of a focused strategic doctrine, and close cooperation with allies.

Once this has been achieved, the UK should extend the Hecla programme to execute the sufficient deployment of seabed sensors around identified threat-areas in its sub-surface infrastructural lattice. The entirety of the 6.8mn km^2 EEZ cannot be paved with detection equipment, and nor must it be. Cable choke-points in the North and (British territorial waters of the) Irish seas should be prioritised, so that we no longer rely on the American IUSS to surveil our waters for us. As noted above, the first step of any effective undersea strategy is knowledge-acquisition. A comprehensive sensor network – not surface vessels and a handful of submarines – are the only means of achieving this.

To expedite this sensor-paving process, the MoD should establish long-term partnerships with relevant technology companies. The SOSUS' early, critical success in rapid capability development owed in part to the US military's close cooperation with Bell Laboratories, which provided oceanographic R&D and a steady supply of sensors via long-term contract procurement arrangements. The UK should learn from this public-private partnership and identify those companies with British-domiciled skills and manufacturing ecosystems which can, alongside pooled allied capabilities, build the national undersea defence system.

The MROSS programme should be expanded to a fleet of three ships, contributing to an expanded and persistent surveillance of undersea critical infrastructure in British waters. RFA Proteus must conclude its final training and preparation to attain sea readiness as soon as possible. With the operational and tactical lessons learned from its early deployments, efforts and resources should be channelled into developing two further surface surveillance vessels. This would ensure critical strategic fleet depth to sustain policing of British waters at all times, whilst keeping one available for deployment further afield, such as to the north alongside our regional partners.

The government should establish regularised partnerships with satellite-owning private sector entities to build a whole of government approach to maritime security. Satellite imagery serves three critical purposes in undersea security. Firstly, it enables intelligence agencies to monitor critical maritime infrastructure and identify suspicious vessels. Interdictions in cases of illicit maritime activity are reported to increase by 500% with the use of satellite imagery, providing clear deterrence benefits to the UK's security. Secondly, commercial data can also be used to build evidence bases necessary to attribute blame for maritime incidents. Thirdly, it would facilitate greater information-sharing between partners in multilateral defence frameworks, which is currently restricted by constraints around disclosing military intelligence. This whole of government approach would be entirely in the interests of the private

sector, which also depends on the security of undersea cables.

Finally, the UK must hold on-shore cable facility providers to higher security standards to ensure that they are adequately protected by sufficient personnel and constant surveillance. Whilst recent hostile activity has focused on cables at sea, the UK has just under 100 cable on-shore centres, many of which are located in remote peninsula regions which are difficult to reach by land, and easily accessible by landing at shore. As cable sabotage at these sites would be just as disruptive to networks – even more so, given that many sites house multiple cables – their security is paramount. Greater demands must be placed on facility providers so that they are adequately manned by security personnel and CCTV cameras.

£10.00
ISBN: 978-1-910812

Policy Exchange
1 Old Queen Street
Westminster
London SW1H 9JA

www.policyexchange.org.uk